

Enterprise SONiC Distribution by Dell Technologies

Management Framework CLI Reference Guide Release
4.4.1

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Chapter 1: CLI basics..... **29**

Chapter 2: A commands..... **34**

aaa authentication login console.....	35
aaa authentication login default.....	35
aaa authentication failthrough.....	36
aaa authorization default group tacacs+.....	36
aaa name-service group.....	37
aaa name-service netgroup.....	37
aaa name-service passwd.....	37
aaa name-service shadow.....	38
aaa name-service sudoers.....	38
aaa server radius dynamic-author.....	39
abort.....	39
access-list.....	39
activate.....	39
add-reason.....	40
addpath-tx-all-paths.....	41
addpath-tx-bestpath-per-as.....	41
address-family ipv4.....	42
address-family ipv6.....	42
address-family l2vpn.....	43
advertise ipv4 unicast.....	43
advertise ipv6 unicast.....	44
advertise-all-vni.....	44
advertise-default-gw.....	44
advertise-pip.....	45
advertise-svi-ip.....	45
advertisement-interval.....	46
aggregate-address.....	46
aging-interval.....	47
alarm acknowledge.....	47
alarm unacknowledge.....	48
algorithm.....	48
alias.....	48
allow high-wattage optics.....	48
allowas-in.....	49
always-compare-med.....	50
area.....	50
ars bind.....	51
ars bind profile.....	52
enable.....	52
ars object	52
ars port-profile.....	52

ars profile.....	53
as-notation.....	53
as-override.....	54
attribute-unchanged.....	54
auditd-system rules.....	55
auth-type	55
authentication command bounce-port ignore	56
authentication command disable-port ignore	56
authentication event fail action authorize.....	56
authentication event no-response.....	57
authentication host-mode.....	57
authentication max-users.....	58
authentication monitor.....	58
authentication open.....	58
authentication order.....	59
authentication periodic.....	59
authentication port-control.....	60
authentication priority.....	60
authentication rest.....	60
authentication telemetry.....	61
authentication timer reauthenticate.....	61
auto-breakout.....	62
auto-cost.....	62
autoneg.....	62
autort.....	63
autostate.....	63

Chapter 3: B commands..... **64**

banner login.....	64
banner motd.....	64
bestpath as-path confed.....	65
bestpath as-path ignore.....	65
bestpath as-path multipath-relax.....	66
bestpath compare-routerid.....	66
bestpath med.....	66
bfd.....	67
bgp as-path-list.....	67
bgp community-list.....	68
bgp extcommunity-list.....	69
binding.....	70
buffer default-lossless-buffer-profile.....	70
buffer init lossless.....	70
buffer pool.....	71
buffer priority-group.....	71
buffer profile.....	72
buffer queue.....	72

Chapter 4: C commands..... **74**

call.....	76
-----------	----

capability dynamic.....	76
capability extended-nexthop.....	76
capability orf prefix-list.....	77
channel-group.....	77
cir.....	78
class.....	78
class-map.....	78
classifier	79
clear ars nhg-statistics.....	79
clear audit-log.....	79
clear authentication history interface.....	80
clear authentication sessions.....	80
clear bfd peer.....	80
clear bgp all.....	81
clear bgp ipv4.....	81
clear bgp ipv6.....	82
clear bgp l2vpn evpn.....	83
clear buffer-pool.....	83
clear core-files.....	84
clear counters interface.....	84
clear counters service-policy.....	84
clear counters service-policy interface.....	85
clear counters service-policy policy-map.....	85
clear counters tam.....	86
clear counters vxlan.....	86
clear device.....	86
clear error-database.....	87
clear evpn dup-addr.....	87
clear ip access-list counters.....	88
clear ip arp.....	88
clear ip arp interface.....	89
clear ip dhcp snooping binding.....	89
clear ip dhcp snooping statistics.....	90
clear ip dhcp-relay.....	90
clear ip helper-address statistics.....	90
clear ip igmp interfaces.....	91
clear ip igmp vrf.....	91
clear ip mroute.....	91
clear ip ospf.....	92
clear ip pim.....	92
clear ip sla.....	92
clear ip sla all.....	93
clear ipv6 access-list counters.....	93
clear ipv6 dhcp snooping binding.....	93
clear ipv6 dhcp snooping statistics.....	94
clear ipv6 dhcp-relay.....	94
clear ipv6 nd.....	95
clear ipv6 neighbors.....	95
clear ipv6 neighbors interface.....	96
clear logging.....	96

clear mac access-list counters.....	96
clear mac address-table dynamic.....	97
clear mac dampening-disabled-ports.....	97
clear nat.....	97
clear poe counters.....	98
clear priority-group.....	98
clear queue.....	98
clear radius-server dynamic-author statistics	99
clear radius-server statistics.....	99
clear snmp counters.....	100
clear spanning-tree counters.....	100
clear threshold breach.....	100
client.....	101
client-to-client reflection.....	101
clock timezone.....	101
cluster-id.....	102
coalesce-time.....	102
collector.....	102
compatible.....	103
confederation.....	103
configure terminal.....	104
consistency-check start access-list.....	104
consistency-check start route.....	104
consistency-check stop.....	105
copp-action.....	105
copy.....	105
core enable.....	106
counter.....	106
counters.....	106
counters rif interval.....	107
crm.....	107
crm polling-interval.....	108
crm threshold.....	108
crm threshold type.....	109
crypto ca-cert delete.....	109
crypto ca-cert install	110
crypto ca-cert verify expiry.....	110
crypto cert delete.....	111
crypto cert generate request	111
crypto cert install cert-file key-file.....	112
crypto cert verify expiry.....	112
crypto fips enable.....	113
crypto security-profile.....	113
crypto security-profile certificate.....	114
crypto security-profile trust-store.....	114
crypto ssh-keygen.....	115
crypto trust-store.....	115
crypto trust-store ca-cert.....	115

dampening.....	118
debug shell.....	118
default interface.....	118
default ipv4-unicast.....	119
default local-preference.....	119
default show-hostname.....	120
default shutdown.....	120
default subgroup-pkt-queue-max	120
default-information.....	121
default-metric.....	121
default-originate.....	122
default-originate.....	122
delay-restore.....	123
delete.....	123
delete-reason.....	123
description.....	124
destination.....	124
destination CPU.....	125
destination erspan.....	125
detect-multiplier.....	126
deterministic-med.....	126
df-election-time.....	127
df-preference.....	127
diag-mode.....	127
dir.....	128
disable-connected-check.....	128
disable-ead-evi-rx.....	129
disable-ead-evi-tx.....	129
disable-ebgp-connected-route-check.....	129
distance.....	130
distance bgp.....	130
dont-capability-negotiate.....	131
dot1p.....	131
dot1x pae.....	132
dot1x system-auth-control.....	132
dot1x timeout.....	132
downstream all-mclag.....	133
downstream all-evpn-es.....	133
drop-monitor.....	133
dropcounters.....	134
dscp.....	134
duplex.....	135
dup-addr-detection.....	135
dup-addr-detection freeze.....	135
Chapter 6: E, F, and G commands.....	137
ebgp-multihop.....	138
echo-interval.....	138
echo-mode.....	138
ecn.....	139

enable.....	139
encapsulation dot1q vlan-id.....	140
end.....	141
enforce-first-as.....	141
enforce-multipoint.....	141
enterprise-id.....	142
entry.....	142
errdisable recovery cause.....	143
errdisable recovery interval.....	143
es-activation-delay.....	144
evpn esi-multihoming.....	144
evpn ethernet-segment.....	144
exit.....	145
external-ip.....	145
fabric-external.....	146
factory default profile.....	146
fast-convergence	147
fast-external-failover.....	147
fast-reboot.....	148
fec.....	148
filter-list.....	148
flow-group.....	149
forwarding-fbs.....	150
frequency.....	150
graceful-restart	151
graceful-restart enable.....	151
graceful-restart helper enable	151
graceful-restart helper strict-lsa-checking	152
graceful-restart helper supported-grace-time	152
graceful-restart helper planned-only	152
graceful-restart preserve-fw-state.....	152
graceful-restart restart-time.....	153
graceful-restart stalepath-time.....	153
graceful-shutdown (BGP).....	153
graceful-shutdown (Port Channel).....	154
green.....	154
group.....	155
Chapter 7: H and I commands.....	156
hardware.....	159
hostname.....	159
icmp-echo.....	159
idle-time.....	160
ifa.....	160
ignore server-key	160
ignore session-key	160
image firmware install.....	161
image gpg-key key-server key-id.....	161
image install.....	161
image patch install.....	162

image patch rollback.....	162
image remove.....	163
image set-default.....	163
image verify gpg signature.....	163
image verify pki signature.....	164
import vrf.....	164
instance.....	165
interface.....	165
interface CPU.....	166
interface breakout.....	166
interface Loopback.....	167
interface Management.....	167
interface media-fec.....	167
interface-naming.....	168
interface PortChannel.....	168
interface port-locator.....	169
interface range.....	169
interface transceiver diagnostics loopback.....	170
interface transceiver diagnostics pattern.....	170
interface vxlan.....	171
ip access-group.....	171
ip access-list.....	172
ip acl.....	172
ip address.....	172
ip anycast-address.....	173
ip anycast-address.....	173
ip anycast-mac-address.....	174
ip anycast-mac-address router-mac-for-forwarding.....	174
ip arp.....	174
ip dhcp-relay.....	175
ip dhcp-relay circuit-id.....	175
ip dhcp-relay link-select.....	176
ip dhcp-relay max-hop-count.....	176
ip dhcp-relay policy-action.....	176
ip dhcp-relay source-interface.....	177
ip dhcp-relay vrf-select.....	177
ip dhcp snooping.....	178
ip dhcp snooping trust.....	178
ip dhcp snooping verify mac-address.....	178
ip dhcp snooping vlan.....	179
ip drop-neighbor.....	179
ip drop-neighbor aging-time.....	180
ip forward-protocol udp enable.....	180
ip forward-protocol udp exclude.....	180
ip forward-protocol udp include.....	181
ip forward-protocol udp rate-limit.....	181
ip helper-address.....	181
ip igmp.....	182
ip igmp join.....	182
ip igmp last-member-query-count.....	183

ip igmp last-member-query-interval.....	183
ip igmp query-interval.....	183
ip igmp query-max-response-time.....	184
ip igmp snooping.....	184
ip igmp version.....	185
ip load-share hash algorithm.....	186
ip load-share hash ingress-port.....	186
ip load-share hash ipv4.....	186
ip load-share hash ipv6.....	187
ip load-share hash offset.....	187
ip load-share hash roce qpn.....	188
ip load-share hash seed.....	188
ip name-server.....	189
ip name-server source-interface.....	189
ip nht.....	189
ip ospf.....	190
ip ospf area.....	190
ip ospf authentication.....	190
ip ospf authentication-key.....	191
ip ospf bfd.....	191
ip ospf bfd profile.....	192
ip ospf cost.....	192
ip ospf dead-interval.....	192
ip ospf hello-interval.....	193
ip ospf message-digest-key.....	193
ip ospf mtu-ignore.....	194
ip ospf network.....	194
ip ospf priority.....	195
ip ospf retransmit-interval.....	195
ip ospf transmit-delay.....	196
ip pim.....	196
ip pim bfd.....	197
ip pim bfd profile.....	197
ip pim drpriority.....	198
ip pim hello.....	198
ip pim sparse-mode.....	199
ip prefix-list.....	199
ip protocol.....	199
ipv6 protocol.....	200
ip reserve local-neigh.....	200
ip rest	200
ip rest authentication.....	201
ip rest cipher-suite.....	201
ip rest security-profile.....	202
ip route.....	202
ip sla.....	203
ip source binding.....	203
ip ssh.....	203
ip ssh client ciphers.....	204
ip ssh client kexalgorithms.....	205

ip ssh client macs.....	205
ip telemetry	206
ip telemetry authentication	206
ip telemetry security-profile.....	207
ip unnumbered.....	207
ip vrf.....	207
ip vrf forwarding.....	208
ip vrf mgmt.....	208
ipv6 access-group.....	208
ipv6 access-list.....	209
ipv6-acl.....	209
ipv6 address.....	210
ipv6 anycast-address.....	210
ipv6 anycast-address enable.....	210
ipv6 dhcp snooping.....	211
ipv6 dhcp snooping trust.....	211
ipv6 dhcp snooping verify mac-address.....	211
ipv6 dhcp snooping vlan.....	212
ipv6 dhcp-relay.....	212
ipv6 dhcp-relay max-hop-count.....	213
ipv6 dhcp-relay source-interface.....	213
ipv6 dhcp-relay vrf-select.....	213
ipv6 drop-neighbor.....	214
ipv6 enable.....	214
ipv6 nd adv-interval-option.....	214
ipv6 nd cache.....	215
ipv6 nd dnssl.....	215
ipv6 nd home-agent-config-flag.....	216
ipv6 nd home-agent-lifetime.....	216
ipv6 nd home-agent-preference.....	216
ipv6 nd managed-config-flag.....	217
ipv6 nd mtu.....	217
ipv6 nd other-config-flag.....	217
ipv6 nd prefix.....	218
ipv6 nd ra-fast-retrans.....	218
ipv6 nd ra-hop-limit.....	219
ipv6 nd ra-interval.....	219
ipv6 nd ra-lifetime.....	220
ipv6 nd ra-retrans-interval.....	220
ipv6 nd rdnss.....	220
ipv6 nd reachable-time.....	221
ipv6 nd router-preference.....	221
ipv6 nd suppress-ra.....	222
ipv6 neighbor.....	222
ipv6 nht.....	223
ipv6 prefix-list.....	223
ipv6 route.....	223
ipv6 source binding.....	224

kdump enable.....	227
kdump memory.....	227
kdump num-dumps.....	227
keepalive-interval.....	228
key config-key password-encrypt.....	228
l2-nexthop-group.....	228
lacp individual	229
ldap-server.....	229
ldap-server host.....	232
ldap-server map.....	232
ldap-server nss.....	233
ldap-server pam.....	234
ldap-server security-profile.....	236
ldap-server source-interface.....	236
ldap-server sudo.....	236
ldap-server vrf.....	237
line vty.....	238
link state track.....	238
link-error-disable.....	239
listen limit.....	239
listen range.....	240
lldp.....	240
lldp enable.....	240
lldp med-tlv-select.....	241
lldp multiplier.....	241
lldp system-description.....	241
lldp system-name.....	242
lldp timer.....	242
lldp tlv-select.....	242
lldp tlv-set.....	244
lldp vlan-name-tlv allowed vlan.....	245
lldp vlan-name-tlv max-tlv-count.....	245
load-current-max-val.....	246
load-current-min-val.....	246
load-future-max-val.....	247
load-future-min-val.....	247
load-future-weight.....	248
load-past-max-val.....	248
load-past-min-val.....	249
load-past-weight.....	249
load-scaling-factor.....	249
local-as.....	250
locator-led chassis.....	251
log-adjacency-changes.....	251
log-neighbor-changes.....	252
logger.....	252
logging security-profile.....	252
logging server.....	253
login exec-timeout.....	254
login lockout.....	254

login password-attributes.....	254
mab	255
mab request format	256
mab timeout.....	256
mac access-group.....	256
mac access-list.....	257
mac address-table.....	257
mac address-table aging-time.....	257
mac address-table dampening-interval.....	258
mac address-table dampening-threshold.....	258
mac-holddate.....	258
map.....	259
match access-group.....	259
match as-path.....	260
match community.....	260
match dei.....	260
match destination-address.....	261
match dscp.....	261
match ethertype.....	261
match evpn.....	262
match ext-community.....	262
match interface.....	262
match ip protocol.....	263
match ip address prefix-list.....	263
match ip next-hop prefix-list.....	263
match ipv6 address prefix-list.....	264
match l4-port.....	264
match local-preference.....	264
match metric.....	265
match origin.....	265
match pcp.....	265
match peer.....	266
match protocol.....	266
match source-address.....	267
match source-protocol.....	267
match source-vrf.....	267
match tag.....	268
match tcp-flags.....	268
match vlan.....	269
max-flows.....	269
max-med.....	269
max-metric.....	270
maximum-paths.....	270
maximum-paths ibgp.....	270
maximum-prefix.....	271
mclag.....	271
mclag domain.....	271
mclag gateway-mac.....	272
mclag-peer-gateway.....	272
mclag-separate-ip.....	272

mclag-system-mac.....	273
meter-type.....	273
minimum-ttl.....	273
mirror.....	274
mirror-session.....	274
mode.....	275
monitoring-fbs.....	275
mtu.....	276
Chapter 9: N, O, and P commands.....	277
name.....	278
nat.....	279
nat-zone.....	279
neigh-holddown.....	279
neigh-suppress.....	280
neighbor.....	280
network.....	280
network import-check.....	281
network prefix.....	281
network-policy.....	282
network-policy.....	282
next-hop-self.....	282
no crm all.....	283
ntp authenticate.....	283
ntp authentication-key.....	284
ntp server.....	284
ntp source-interface.....	285
ntp trusted-key.....	285
ntp vrf.....	285
ospf abr-type.....	286
ospf router-id.....	286
override-capability.....	287
passive.....	287
passive-interface.....	288
passive-interface (for OSPFv2).....	288
passive-mode.....	288
password.....	289
pbf next-hop-group.....	289
pbf replication-group.....	290
pbs.....	290
peer.....	290
peer-group.....	291
peer-ip.....	292
peer-link.....	292
pfc-priority.....	292
pfc-priority pg.....	293
ping.....	293
ping vrf.....	295
ping vrf mgmt.....	295
ping6.....	296

ping6 vrf.....	297
ping6 vrf mgmt.....	297
pir.....	298
poe detection.....	298
poe disable.....	299
poe power management.....	299
poe priority.....	299
poe reset.....	300
police.....	300
police.....	301
policy-map.....	301
pool.....	302
port.....	302
port	302
port-group.....	303
portchannel graceful-shutdown.....	303
port-load-current.....	303
port-load-exponent.....	304
port-load-future.....	304
port-load-future-weight.....	304
port-load-past.....	304
port-load-past-weight.....	305
port-security enable.....	305
port-security maximum.....	305
port-security violation.....	306
preempt.....	306
prefix-list.....	307
primary-ip.....	307
priority.....	308
priority-flow-control.....	308
priority-flow-control watchdog action.....	309
priority-flow-control watchdog counter-poll.....	309
priority-flow-control watchdog off.....	309
priority-flow-control watchdog on.....	310
priority-flow-control watchdog polling-interval.....	310
priority-flow-control watchdog restore-time.....	310
profile.....	311

Chapter 10: Q and R commands.....	313
qos-fbs.....	314
qos map dot1p-tc.....	314
qos map dscp-tc.....	314
qos-map pfc-priority-pg.....	315
qos map pfc-priority-queue.....	315
qos map tc-dot1p.....	315
qos map tc-dscp.....	316
qos map tc-pg.....	316
qos map tc-queue.....	316
qos scheduler-policy.....	317
qos wred-policy.....	317

qos-map dot1p-tc.....	317
qos-map dscp-tc.....	318
qos-map pfc-priority-queue.....	318
qos-map tc-dot1p.....	318
qos-map tc-dscp.....	319
qos-map tc-pg.....	319
qos-map tc-queue.....	319
qos-mode.....	320
queue.....	320
radius-server auth-type.....	320
radius-server host.....	321
radius-server key.....	321
radius-server nas-ip.....	322
radius-server retransmit.....	322
radius-server statistics.....	322
radius-server timeout.....	323
radv enable.....	323
random-seed.....	323
rd.....	324
read-quanta.....	324
reboot.....	324
receive-interval.....	325
redirect security-profile.....	325
redistribute.....	325
redistribute.....	326
refresh.....	327
remark.....	327
remote-as.....	327
remove-private-as.....	328
renew dhcp-lease.....	328
request-data-size.....	329
revision.....	329
roce enable.....	329
route-map.....	330
route-map.....	330
route-map delay-timer.....	331
route-reflector allow-outbound-policy.....	331
route-reflector-client.....	332
route-scale routes.....	332
route-scale hosts.....	333
route-server-client.....	333
route-target.....	334
router bgp.....	334
router ospf.....	334
router-id.....	335
Chapter 11: S to show priority-group commands.....	336
sampler.....	341
sampling-interval	341
scheduler-policy.....	342

send-community.....	342
seq.....	343
seq.....	343
server-key	344
service-policy.....	344
session.....	345
session-timeout.....	345
session-vrf.....	346
set ars disable.....	346
set ars-object.....	346
set as-path.....	347
set comm-list delete.....	347
set community.....	348
set copp-action.....	349
set dscp.....	349
set extcommunity.....	349
set interface.....	350
set ip.....	350
set ip.....	350
set ipv6.....	351
set ipv6 next-hop.....	351
set local-preference.....	352
set metric.....	352
set mirror-session.....	353
set origin.....	353
set pcp.....	353
set traffic-class.....	354
set trap-action.....	354
set trap-priority.....	355
set trap-queue.....	355
set weight.....	355
sflow agent-id.....	356
sflow collector.....	356
sflow enable.....	356
sflow polling-interval.....	357
sflow sampling-rate.....	357
show aaa.....	358
show access-group.....	358
show alarm.....	358
show ars bind.....	360
set ars disable.....	361
show ars nhg-statistics.....	361
show ars object.....	361
show ars port-profile.....	362
show ars port-quality	362
show ars profile.....	363
show audit-log.....	363
show audited-system log.....	364
show audited-system rules.....	364
show authentication.....	364

show authentication authentication-history.....	365
show authentication clients.....	365
show authentication interface.....	367
show ip rest authentication.....	369
show ip telemetry authentication.....	369
show bfd peer.....	369
show bfd peer counters.....	370
show bfd peers.....	371
show bfd profile.....	372
show bgp all.....	373
show bgp as-path-access-list.....	374
show bgp community-list.....	374
show bgp ext-community-list.....	375
show bgp ipv4.....	375
show bgp ipv6.....	377
show bgp l2vpn evpn es.....	379
show bgp l2vpn evpn es-evi.....	380
show bgp l2vpn evpn es-vrf.....	380
show bgp l2vpn evpn next-hops.....	381
show bgp l2vpn evpn route.....	381
show bgp l2vpn evpn route detail type.....	382
show bgp l2vpn evpn route rd.....	383
show bgp l2vpn evpn route type.....	384
show bgp l2vpn evpn route vni.....	384
show bgp l2vpn evpn summary.....	385
show bgp l2vpn evpn vni.....	385
show buffer interface.....	386
show buffer-pool.....	386
show buffer profile.....	387
show ca-crypto cert.....	388
show cable-diagnostics.....	389
show class-map.....	390
show clock.....	390
show config-key password-encrypt.....	391
show configuration.....	391
show consistency-check status.....	392
show copp.....	393
show core config.....	394
show core info.....	394
show core list.....	395
show crm.....	396
show crm resources.....	396
show crm thresholds.....	398
show crypto ca-cert file.....	399
show crypto cert.....	400
show crypto cert file.....	401
show crypto security-profile.....	401
show crypto ssh-key.....	402
show crypto trust-store.....	402
show current.....	403

show database map.....	403
show device.....	404
show dot1x.....	404
show dot1x detail.....	404
show dropcounters capabilities.....	405
show dropcounters configuration.....	406
show dropcounters configuration detail.....	406
show errdisable link-flap.....	406
show errdisable recovery.....	407
show error-database.....	407
show event.....	408
show evpn.....	410
show evpn arp-cache vni.....	411
show evpn arp-cache vni all.....	411
show evpn es.....	412
show evpn es startup-delay.....	413
show evpn es-evi.....	413
show evpn l2-nh.....	414
show evpn mac vni.....	414
show evpn mac vni all.....	415
show evpn next-hops vni.....	416
show evpn next-hops vni all.....	416
show evpn rmac vni.....	416
show evpn rmac vni all.....	417
show evpn vni.....	417
show evpn vni detail.....	418
show fips status.....	418
show hardware tcam allocation.....	419
show hardware tcam key-profile.....	419
show histogram memory system.....	420
show hosts.....	420
show image firmware.....	421
show image firmware status.....	422
show image list.....	422
show image patch history.....	423
show image patch list.....	423
show image patch status.....	423
show image status.....	424
show in-memory-logging.....	425
show in-memory-logging count.....	425
show in-memory-logging lines.....	426
show interface.....	426
show interface advertise.....	429
show interface breakout.....	430
show interface counters.....	432
show interface description.....	432
show interface dropcounters.....	433
show interface Ethernet.....	433
show interface link-training.....	434
show interface loopback.....	435

show interface management.....	435
show interface-naming.....	436
show interface phy counters.....	436
show interface phy status.....	437
show interface portchannel.....	437
show interface port-locator.....	438
show interface status.....	439
show interface transceiver.....	440
show interface transceiver wattage.....	442
show interface transceiver summary.....	442
show interface unreliable-los status.....	443
show interface vlan-mappings.....	443
show interface vlan-mappings dot1q-tunnel.....	444
show ip access-group.....	444
show ip access-lists.....	445
show ip arp.....	445
show ip arp interface.....	446
show ip dhcp snooping.....	446
show ip dhcp snooping binding.....	447
show ip dhcp snooping statistics.....	447
show ip dhcp snooping statistics detail.....	448
show ip dhcp-relay.....	448
show ip forward-protocol.....	449
show ip helper-address.....	450
show ip helper-address statistics.....	450
show ip igmp snooping.....	451
show ip igmp groups.....	452
show ip igmp interface.....	452
show ip igmp join.....	453
show ip igmp sources.....	453
show ip igmp statistics.....	454
show ip igmp vrf.....	454
show ip interfaces.....	455
show ip load-share.....	455
show ip mroute.....	456
show ip ospf.....	457
show ip ospf graceful-restart helper.....	463
show ip ospf neighbor detail.....	464
show ip ospf route.....	464
show ip pim.....	465
show ip prefix-list.....	467
show ip rest.....	468
show ip rest authentication	468
show ip rest cipher-suite.....	468
show ip route.....	469
show ip sla.....	470
show ip static-anycast-gateway.....	471
show ip telemetry.....	471
show ip vrf.....	472
show ipv6 access-group.....	473

show ipv6 access-lists.....	473
show ipv6 dhcp snooping.....	473
show ipv6 dhcp snooping binding.....	474
show ipv6 dhcp snooping statistics.....	474
show ipv6 dhcp snooping statistics detail.....	475
show ipv6 dhcp-relay.....	475
show ipv6 interfaces.....	476
show ipv6 nd ra-interfaces.....	477
show ipv6 neighbors.....	478
show ipv6 neighbors interface.....	479
show ipv6 prefix-list.....	479
show ipv6 route.....	480
show ipv6 static-anycast-gateway.....	480
show kdump files.....	481
show kdump log.....	481
show kdump memory.....	482
show kdump num-dumps.....	482
show kdump status.....	482
show ldap-server.....	483
show link state tracking.....	484
show lldp neighbor.....	484
show lldp statistics.....	485
show lldp table.....	485
show locator-led chassis.....	485
show logging.....	486
show logging count.....	487
show logging filter.....	487
show logging lines.....	488
show logging servers.....	488
show mab.....	489
show mab interface.....	489
show mac access-group.....	489
show mac access-lists.....	490
show mac address-table.....	490
show mac address-table address.....	491
show mac address-table aging-time.....	491
show mac address-table count.....	491
show mac address-table dynamic.....	492
show mac address-table interface.....	493
show mac address-table static.....	493
show mac address-table Vlan.....	494
show mac dampening.....	495
show mac dampening-disabled-ports.....	495
show mclag brief.....	495
show mclag mac remote	496
show mclag interface.....	496
show mclag peer-gateway-interfaces.....	497
show mclag separate-ip-interfaces.....	497
show mirror-session.....	497
show nat.....	498

show neighbor-suppress-status.....	499
show ntp associations.....	500
show ntp global.....	501
show ntp server.....	501
show object-groups.....	501
show pbf next-hop-group.....	502
show pbf next-hop-group status interface.....	502
show pbf next-hop-group status Switch.....	503
show pbf replication-group.....	503
show pbf replication-group status interface.....	504
show pbf replication-group status Switch.....	504
show pending.....	505
show platform environment.....	505
show platform fanstatus.....	506
show platform firmware.....	507
show platform firmware detail.....	507
show platform psustatus.....	508
show platform psussummary.....	509
show platform sbstatus.....	510
show platform ssdhealth.....	510
show platform syseprom.....	510
show platform temperature.....	511
show platform temperature detail.....	511
show poe.....	512
show poe port configuration.....	512
show poe port info.....	513
show policy-map.....	514
show PortChannel summary.....	515
show port-group.....	515
show port-security.....	516
show port-security interface.....	516
show priority-flow-control.....	516
show priority-group.....	517

Chapter 12: show qos to switchport commands.....	518
show qos.....	522
show qos map dot1p-tc.....	523
show qos map dscp-tc.....	523
show qos map pfc-priority-pg.....	524
show qos map pfc-priority-queue.....	524
show qos map tc-dot1p.....	525
show qos map tc-dscp.....	525
show qos map tc-pg.....	526
show qos map tc-queue.....	526
show qos scheduler-policy.....	526
show qos wred-policy.....	527
show queue.....	528
show radius-server.....	529
show radius-server dynamic-author.....	529
show reboot-cause.....	531

show route-map.....	532
show running-configuration.....	532
show running-configuration bfd.....	533
show running-configuration bgp.....	533
show running-configuration bgp as-path-access-list.....	534
show running-configuration bgp community-list.....	534
show running-configuration bgp extcommunity-list.....	535
show running-configuration bgp neighbor.....	535
show running-configuration bgp peer-group.....	535
show running-configuration class-map.....	536
show running-configuration dropcounters.....	536
show running-configuration hardware.....	537
show running-configuration hardware access-list.....	537
show running-configuration hardware tcam.....	537
show running-configuration igmp.....	538
show running-configuration interface.....	538
show running-configuration interface Loopback.....	539
show running-configuration interface Management.....	539
show running-configuration interface PortChannel.....	540
show running-configuration interface Vlan.....	540
show running-configuration interface vxlan.....	541
show running-configuration ip access-list.....	542
show running-configuration ip prefix-list.....	542
show running-configuration ipv6 access-list.....	542
show running-configuration ipv6 prefix-list.....	543
show running-configuration line vty.....	543
show running-configuration link state tracking.....	543
show running-configuration mac access-list.....	544
show running-configuration mlag.....	544
show running-configuration mirror-session.....	544
show running-configuration nat.....	545
show running-configuration ospf.....	545
show running-configuration ospf interface.....	545
show running-configuration pbf next-hop-group.....	546
show running-configuration pbf replication-group.....	546
show running-configuration policy-map.....	547
show running-configuration route-map.....	547
show running-configuration spanning-tree.....	547
show running-configuration subinterface.....	548
show running-configuration tam.....	548
show running-configuration vrf.....	549
show service-policy.....	550
show service-policy interface.....	550
show service-policy policy-map.....	551
show service-policy summary.....	552
show sflow.....	552
show sflow interface.....	553
show snmp counters.....	553
show snmp-server.....	554
show snmp-server community.....	554

show snmp-server group.....	555
show snmp-server host.....	555
show snmp-server interface-traps.....	555
show snmp-server traps.....	556
show snmp-server user.....	556
show snmp-server view.....	557
show spanning-tree.....	557
show spanning-tree bpdu-guard.....	558
show spanning-tree counters.....	558
show spanning-tree inconsistentports.....	558
show spanning-tree mst.....	559
show spanning-tree mst configuration.....	559
show spanning-tree mst detail.....	560
show spanning-tree mst interface.....	560
show ssh-server vrf.....	561
show storm-control.....	561
show storm-control interface.....	561
show subinterfaces status.....	562
show switch-profiles.....	562
show switch-resource drop-monitor.....	562
show switch-resource route-scale.....	563
show switch-resource vlan-stacking.....	563
show switching-mode.....	564
show system.....	564
show system cpu.....	564
show system memory.....	565
show system processes.....	565
show system processes cpu.....	566
show system processes mem-usage.....	566
show system processes mem-util.....	567
show system processes pid.....	568
show system status.....	568
show system vlan.....	571
show tacacs-server.....	572
show tacacs-server global.....	572
show tacacs-server host.....	572
show tam collectors.....	573
show tam drop-monitor.....	573
show tam drop-monitor sessions.....	574
show tam features.....	574
show tam flowgroups.....	575
show tam ifa.....	575
show tam ifa sessions.....	576
show tam samplers.....	576
show tam switch.....	577
show tam tail-stamping.....	577
show tam tail-stamping sessions.....	577
show tech-support.....	578
show tech-support cancel.....	578
show techsupport-export.....	579

show tech-support status.....	579
show tech-support terminal.....	579
show threshold breaches.....	580
show threshold buffer-pool.....	581
show threshold device.....	581
show threshold priority-group.....	581
show threshold queue.....	582
show tpcm list.....	584
show tpcm name	584
show udld global.....	585
show udld interface.....	585
show udld neighbors.....	586
show udld statistics.....	586
show udld statistics interface.....	587
show uptime.....	587
show users.....	587
show users configured.....	588
show version.....	588
show Vlan.....	590
show vrrp.....	590
show vrrp6.....	591
show vxlan counters.....	591
show vxlan interface.....	592
show vxlan remote mac.....	592
show vxlan remote mac count.....	593
show vxlan remote nexthop-group.....	593
show vxlan remote vni.....	594
show vxlan remote vni count.....	594
show vxlan tunnel.....	594
show vxlan tunnel count.....	595
show vxlan vlanvnimap.....	595
show vxlan vlanvnimap count.....	596
show vxlan vrfvnimap.....	596
show vxlan vrfvnimap count.....	596
show warm-restart.....	597
show watermark interval.....	598
show watermark telemetry.....	598
show ztp-status.....	598
shutdown.....	600
snmp-server agentaddress.....	601
snmp-server community.....	601
snmp-server contact.....	602
snmp-server enable trap.....	602
snmp-server engine.....	602
snmp-server group.....	603
snmp-server host.....	603
snmp-server location.....	604
snmp-server user.....	604
snmp-server view.....	605
snmp trap enable.....	605

soft-reconfiguration.....	606
solo.....	607
source-address.....	607
source-interface.....	607
source-ip.....	608
source-port.....	609
source-vrf.....	609
spanning-tree bpdufilter.....	609
spanning-tree bpduguard.....	610
spanning-tree cost.....	610
spanning-tree edge-port.....	611
spanning-tree enable.....	611
spanning-tree forward-time.....	611
spanning-tree guard.....	612
spanning-tree guard.....	612
spanning-tree hello-time.....	613
spanning-tree link-type.....	613
spanning-tree loopguard.....	614
spanning-tree max-age.....	614
spanning-tree mode.....	614
spanning-tree mst configuration.....	615
spanning-tree mst forward-time.....	615
spanning-tree mst hello-time.....	615
spanning-tree mst max-age.....	616
spanning-tree mst max-hops.....	616
spanning-tree mst priority.....	616
spanning-tree port.....	617
spanning-tree portfast.....	617
spanning-tree port-priority.....	618
spanning-tree priority.....	618
spanning-tree uplinkfast.....	618
spanning-tree vlan.....	619
spanning-tree vlan.....	619
speed.....	620
speed auto.....	621
ssh-server vrf.....	622
standalone-link-training.....	622
startup-delay.....	622
static.....	623
storm-control broadcast.....	623
storm-control unknown-multicast.....	624
storm-control unknown-unicast.....	624
strict-capability-match.....	624
switch-id.....	625
switch-resource.....	625
switching-mode cut-through.....	625
switchport access.....	626
switchport trunk.....	626
switchport vlan-mapping.....	627
system-mac.....	628

system resource-stats-polling-interval	628
system vlan.....	629

Chapter 13: T, U, V, W, and Z commands..... 630

table-map.....	631
tacacs-server auth-type.....	631
tacacs-server host.....	632
tacacs-server key.....	633
tacacs-server source-interface.....	633
tacacs-server timeout.....	633
tail-stamping.....	634
tam.....	634
tcam.....	634
tcp-connect.....	635
tcp-timeout.....	635
techsupport-export enable.....	635
techsupport-export interval.....	636
techsupport-export remote-server.....	636
terminal length.....	636
terminal timeout.....	637
test cable-diagnostics.....	637
threshold.....	637
threshold (IP SLA).....	638
threshold buffer-pool.....	638
threshold device.....	639
threshold priority-group.....	639
threshold queue.....	639
timeout.....	640
timeout (IP-SLA).....	640
timeout (NAT).....	640
timers.....	641
timers.....	641
tos.....	642
tpcm install.....	642
tpcm uninstall.....	643
tpcm update.....	644
tpcm update disk-limit.....	644
tpcm upgrade.....	645
traceroute.....	645
traceroute6.....	646
track-interface.....	646
traffic-class.....	646
transmit-interval.....	647
ttl.....	648
ttl-security hops.....	648
type.....	648
udld aggressive.....	649
udld enable.....	649
udld message-time.....	650
udld multiplier.....	650

udp-timeout.....	650
unreliable-los.....	651
unsuppress-map.....	651
update-delay.....	651
update-source.....	652
usb enable.....	653
usb mount.....	653
username password role.....	653
use-v2-checksum.....	654
v6only.....	655
version.....	655
vip.....	655
vlan-stacking.....	656
vni.....	657
vni-downstream.....	657
voice.....	657
voice-signaling.....	658
vrrp.....	658
warm-reboot.....	659
warm-restart bgp.....	659
watermark interval.....	659
watermark telemetry.....	660
weight.....	660
write memory.....	660
write erase.....	661
write erase boot.....	661
write erase install.....	661
write-multiplier.....	662
write-quanta.....	662
ztp enable.....	662

CLI basics

This information describes how to use the Management Framework CLI from the console or through a network connection to configure and monitor a SONiC device. The Management Framework CLI runs on top of a Linux-based operating system kernel.

CLI command modes

The Management Framework CLI has two top-level modes:

- EXEC mode—Monitor, troubleshoot, check status, and network connectivity.
- CONFIGURATION mode—Configure network devices.

(i) NOTE: When you enter CONFIGURATION mode, you are changing the current running configuration. By default, configuration changes are not automatically saved. To save changes, you must enter the `write memory` command in EXEC mode.

CLI command hierarchy

Management Framework CLI commands are organized in a hierarchy, which you step through to configure the switch. To move up one command mode, enter the `exit` command. To move directly to the EXEC mode from any submode, enter the `end` command.

```
sonic# config terminal  
sonic(config)# interface Eth1/21  
sonic(config-if-Eth1/21)# no shutdown  
sonic(config-if-Eth1/21)# exit  
sonic(config)# exit  
sonic# write memory  
sonic#
```

OR

```
sonic# config terminal  
sonic(config)# interface Eth1/21  
sonic(config-if-Eth1/21)# no shutdown  
sonic(config-if-Eth1/21)# end  
sonic# write memory  
sonic#
```

The following shows the different CLI modes:

```
Mode EXEC  
sonic#  
  
Mode CONFIGURATION  
  
sonic# configure terminal  
sonic(config)#  
  
Mode INTERFACE  
  
sonic# configure terminal  
sonic(config)# interface Ethernet 0  
sonic(config-if-Ethernet0)# exit  
sonic(config)# interface PortChannel 1  
sonic(config-if-pol1)# exit  
sonic(config)# interface Vlan 100
```

```

sonic(config-if-Vlan100)# exit
sonic(config)# interface Ethernet 0.1
sonic(config-subif-Ethernet0.1)#

Mode INTERFACE-VLAN

sonic# configure terminal
sonic(config)# interface Vlan 200
sonic(config-if-Vlan200)#

Mode INTERFACE-PORTCHANNEL

sonic# configure terminal
sonic(config)# interface PortChannel 100
sonic(config-if-po100)#

Mode SUB-INTERFACE

sonic# configure terminal
sonic(config)# interface Ethernet 4.1
sonic(config-subif-Ethernet4.1)# exit
sonic(config)# interface PortChannel 22.1
sonic(config-subif-PortChannel22.1)#

Mode ROUTER-OSPF

sonic# configure terminal
sonic(config)# router ospf
sonic(config-router-ospf)#

Mode ROUTER-BGP

sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router-bgp)#

Mode BGP-NEIGHBOR

sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router-bgp)# neighbor 192.168.1.1
sonic(config-router-bgp-neighbor)#

Mode NEIGHBOR-ADDRESS-FAMILY

sonic(config)# router bgp 65000
sonic(config-router-bgp)# neighbor 192.168.1.1
sonic(config-router-bgp-neighbor)# address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af)# exit
sonic(config-router-bgp-neighbor)# address-family ipv6 unicast
sonic(config-router-bgp-neighbor-af)# exit
sonic(config-router-bgp-neighbor)#

Mode BGP-PEER-GROUP

sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router-bgp)# peer-group spine
sonic(config-router-bgp-pg)#

Mode PEER-GROUP-ADDRESS-FAMILY

sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router-bgp)# peer-group spine
sonic(config-router-bgp-pg)#
sonic1(config-router-bgp-pg)# address-family ipv4 unicast
sonic1(config-router-bgp-pg-af)# exit
sonic1(config-router-bgp-pg)# address-family ipv6 unicast
sonic1(config-router-bgp-pg-af)#

```

```

Mode BGP-ADDRESS-FAMILY

sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router-bgp)# address-family ipv4 unicast
sonic(config-router-bgp-af)#

Mode BGP-ADDRESS-FAMILY-L2VPN-EVPN

sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)#

Mode ADDRESS-FAMILY-VNI

sonic# configure terminal
sonic(config)# router bgp 65000
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)# vni 1000
sonic(config-router-bgp-af-vni)#

Mode ROUTE-MAP

sonic# configure terminal
sonic(config)# route-map sonic-routemap permit 1
sonic(config-route-map)#

Mode VRRP

sonic# configure terminal
sonic(config)# interface Ethernet 40
sonic(config-if-Ethernet40)# ip address 192.168.2.1/24
sonic(config-if-Ethernet40)# vrrp 1 address-family ipv4
sonic(config-if-Ethernet40-vrrp-ipv4-1)#end
sonic# configure terminal
sonic(config)# interface Ethernet 40
sonic(config-if-Ethernet40)# ipv6 address 2001:192::1/64
sonic(config-if-Ethernet40)# vrrp 1 address-family ipv6
sonic(config-if-Ethernet40-vrrp-ipv6-1)#

Mode TAM

sonic# configure terminal
sonic(config)# tam
sonic(config-tam)#

Mode TAM-DROP-MONITOR , TAM-DM, DROP-MONITOR

sonic# configure terminal
sonic(config)# tam
sonic(config-tam)# drop-monitor
sonic(config-tam-dm)#

Mode TAM-IFA

sonic# configure terminal
sonic(config)# tam
sonic(config-tam)# ifa
sonic(config-tam-ifa)#

Mode TAM-TS , TAIL-STAMPING

sonic# configure terminal
sonic(config)# tam
sonic(config-tam)# tail-stamping
sonic(config-tam-ts)#

Mode NAT

sonic# configure terminal
sonic(config)# nat

```

```
sonic(config-nat)#
Mode MCLAG
sonic# configure terminal
sonic(config)# mclag domain 256
sonic(config-mclag-domain-256)#
Mode LINK-STATE-TRACK
sonic# configure terminal
sonic(config)# link state track linkstatename
sonic(config-link-track)#
Mode MIRROR-SESSION
sonic# configure terminal
sonic(config)# mirror-session 1
sonic(config-mirror-1)#
Mode BFD-PEER
sonic# configure terminal
sonic(config)# bfd
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0
sonic(config-bfd-peer)#
Mode IP-SLA
sonic# configure terminal
sonic(config)# ip sla 1
sonic(config-ipsla-1)#
Mode TCP-CONNECT
sonic# configure terminal
sonic(config)# ip sla 1
sonic(config-ipsla-1)# tcp-connect 172.16.1.1 port 80
sonic(config-ipsla-1-tcp)#
Mode ICMP-ECHO
sonic# configure terminal
sonic(config)# ip sla 128
sonic(config-ipsla-128)# icmp-echo 172.16.1.2
sonic(config-ipsla-128-icmp)#
Mode SWITCH-RESOURCE
sonic# configure terminal
sonic(config)# switch-resource
sonic(config-switch-resource)#
Mode IPV4-ACCESS-LIST
sonic# configure terminal
sonic(config)# ip access-list sonic-ipv4-acl
sonic(config-ipv4-acl)#
Mode IPV6-ACCESS-LIST
sonic# configure terminal
sonic(config)# ipv6 access-list sonic-ipv6-acl
sonic(config-ipv6-acl)#
Mode MAC-ACCESS-LIST
sonic# configure terminal
sonic(config)# mac access-list sonic-mac-acl
sonic(config-mac-acl)#
Mode QOS MAP TC-DOT1P
```

```

sonic# configure terminal
sonic(config)# qos map tc-dot1p tc_dot1p
sonic(config-tc-dot1p-map-tc_dot1p)#

Mode WRED-GREEN

sonic# configure terminal
sonic(config)# qos wred-policy green
sonic(config-wred-green)# exit
sonic(config)# qos wred-policy wred
sonic(config-wred-wred)#

Mode CLASS-MAP

sonic# configure terminal
sonic(config)# class-map sonic-class-map match-type acl
sonic(config-class-map)# exit
sonic(config)# class-map sonic-class-map match-type copp
sonic(config-class-map)# exit
sonic(config)# class-map sonic-class-map1 match-type fields match-all
sonic(config-class-map)#

Mode POLICY-MAP

sonic# configure terminal
sonic(config)# policy-map sonic-policy-map-acl-copp type acl-copp
sonic(config-policy-map)# exit
sonic(config)# policy-map sonic-policy-map-monitoring type monitoring
sonic(config-policy-map)# exit
sonic(config)# policy-map sonic-policy-map-forwarding type forwarding
sonic(config-policy-map)# exit
sonic(config)# policy-map sonic-policy-map-monitoring type monitoring
sonic(config-policy-map)# exit
sonic(config-policy-map)# policy-map sonic-policy-map-qos type qos
sonic(config-policy-map)#

Mode COPP-ACTION

sonic# configure terminal
sonic(config)# copp-action sonic-copp
sonic(config-action)#

```

More Enterprise SONiC documentation

Table 1. More documentation

Document	Description
<i>Enterprise SONiC Distribution by Dell Technologies, 4.4.0 Quick Start Guide</i>	Installation and initial setup tasks
<i>Enterprise SONiC Distribution by Dell Technologies, 4.4.0 User Guide</i>	Product description and software configuration tasks
<i>Enterprise SONiC Distribution by Dell Technologies, 4.4.0 Compatibility Matrix</i>	Supported software features, scalability, interfaces, breakouts, cables, and optics
<i>Enterprise SONiC Distribution by Dell Technologies, 4.4.0 High Power Optics</i>	Supported high-power optics, thresholds, and switch ports
<i>Enterprise SONiC Distribution by Dell Technologies, 4.4.0 Release Notes</i>	New features introduced in the release; known and fixed issues

 **NOTE:** This guide may contain language from third-party content that is not under Dell Technology control and is not consistent with Dell Technology guidelines. Dell Technology plans to update this reference guide when the third party updates their content.

A commands

Topics:

- aaa authentication login console
- aaa authentication login default
- aaa authentication failthrough
- aaa authorization default group tacacs+
- aaa name-service group
- aaa name-service netgroup
- aaa name-service passwd
- aaa name-service shadow
- aaa name-service sudoers
- aaa server radius dynamic-author
- abort
- access-list
- activate
- add-reason
- addpath-tx-all-paths
- addpath-tx-bestpath-per-as
- address-family ipv4
- address-family ipv6
- address-family l2vpn
- advertise ipv4 unicast
- advertise ipv6 unicast
- advertise-all-vni
- advertise-default-gw
- advertise-pip
- advertise-svi-ip
- advertisement-interval
- aggregate-address
- aging-interval
- alarm acknowledge
- alarm unacknowledge
- algorithm
- alias
- allow high-wattage optics
- allowas-in
- always-compare-med
- area
- ars bind
- ars bind profile
- enable
- ars object
- ars port-profile
- ars profile
- as-notation
- as-override
- attribute-unchanged
- auditd-system rules
- auth-type

- authentication command bounce-port ignore
- authentication command disable-port ignore
- authentication event fail action authorize
- authentication event no-response
- authentication host-mode
- authentication max-users
- authentication monitor
- authentication open
- authentication order
- authentication periodic
- authentication port-control
- authentication priority
- authentication rest
- authentication telemetry
- authentication timer reauthenticate
- auto-breakout
- auto-cost
- autoneg
- autort
- autostate

aaa authentication login console

Enables local console authentication separately from the authentication methods configured with the aaa authentication login default command

Command	aaa authentication login console
Options	None
Modes	CONFIGURATION
Usage	In case the configured remote servers for user authentication fail and fail-through local authentication is not available, you can enable independent authentication from the local console. Local console authentication allows switch access for debugging and recovery purposes.
Examples	In this example, only TACACS+ authentication is configured. However, you can add local console authentication in case TACACS+ remote servers are unreachable. Then, only authenticated logins from the local console are supported <pre>sonic(config)# aaa authentication login default group tacacs+ sonic(config)# aaa authentication login console local sonic(config)# no aaa authentication login console</pre>
Releases	4.4.0 or later

aaa authentication login default

Configures AAA login authentication default list to authentication first with TACACS+.

Command	aaa authentication login default {group {ldap [local] radius [local] tacacs+ [local]} local [group [ldap radius tacacs+]]}
Options	<ul style="list-style-type: none"> • group ldap—Enables authentication using LDAP servers. • group radius—Enables authentication using RADIUS servers. • group tacacs+—Enables authentication using TACACS+ servers. • local—Enables authentication using the local user database (default).

Modes	CONFIGURATION
Usage	A switch uses a list of authentication methods to define the types of authentication and the sequence in which they apply. By default, only the local authentication method is used by authenticating users with the local user database. You can also configure TACACS+, RADIUS, or LDAP as the primary or secondary authentication method with local authentication. You can specify only one remote authentication service—TACACS+ or RADIUS or LDAP. The authentication methods in the method list are run in the order you configure them. Reenter the methods to change the order in the authentication method list. If you configure remote authentication using a TACACS+ or RADIUS server, all user logins are authenticated by the TACACS+ server. If the authentication fails, AAA checks the failthrough configuration and authenticates the user based on the local database if fail-through is enabled.
Examples	<pre>sonic# configure terminal sonic(config)# aaa authentication login default group tacacs+ local</pre> <pre>sonic(config)# aaa authentication login default local group ldap</pre> <pre>sonic(config)# no aaa authentication login default</pre>
Releases	3.1 or later

aaa authentication failthrough

Enables the authentication, authorization, and accounting (AAA) failthrough option.

Command	aaa authentication failthrough {enable disable}
Options	<ul style="list-style-type: none"> • enable—Allows AAA to process with local authentication if remote authentication fails. • disable—Disallows AAA to proceed further if remote authentication fails.
Modes	CONFIGURATION
Usage	By default, fail-through for TACACS+, RADIUS, and LDAP authentication is disabled. Use the fail-through option if you configure TACACS+- or RADIUS-based authentication with more than one remote server. The fail-through feature continues to access each server in the method list if an authentication request fails on one server. If authentication failthrough is disabled, the authentication process stops if the authentication request fails on the first server; the login is disallowed.
Examples	<pre>sonic(config)# aaa authentication failthrough enable</pre> <pre>sonic(config)# aaa authentication failthrough disable</pre>
Releases	3.0 or later

aaa authorization default group tacacs+

Enables TACACS+-based command authorization for locally authenticated users.

Command	aaa authorization commands default group tacacs+ local
Options	default group tacacs+ local—Use the default method list with the TACACS+ group of servers that are configured with the tacacs-server host command for command authorization. If none of the configured TACACS+ servers are reachable, use local role-based (RBAC) authorization to authorize commands.
Modes	CONFIGURATION
Usage	AAA authorization uses the TACACS+ servers that are configured for authentication. Command authorization is performed only after a user is authenticated. The server priority and timeout that is configured with the tacacs-server host command are used. For detailed information about how to

configure vendor-specific attributes on a security server, see the respective RADIUS or TACACS+ server documentation.

Examples

```
sonic# configure terminal  
sonic(config)# aaa authorization commands default group tacacs+ local  
  
sonic(config)# no aaa authorization commands default
```

Releases

4.1.0 or later

aaa name-service group

Configures the AAA name-service group to use LDAP.

Command

```
aaa name-service group {{[group ldap]} | [local] | [login]}
```

Options

- group ldap—(Optional) Enables AAA to use group LDAP for the name-service group
- local—(Optional) Enables AAA to use local for the name-service group
- login—(Optional) Enables AAA to use login for the name-service group

Modes

CONFIGURATION

Usage

Use this command to configure the AAA name-service group to use LDAP.

Examples

```
sonic# configure terminal  
sonic(config)# aaa name-service group group ldap  
  
sonic(config)# no aaa name-service group
```

Releases

3.1 or later

aaa name-service netgroup

Configures the AAA netgroup name-service to use LDAP.

Command

```
aaa name-service netgroup {{[group ldap]} | [local]}
```

Options

- group ldap—(Optional) Enables AAA to use group LDAP for the name-service netgroup
- local—(Optional) Enables AAA to use local for the name-service netgroup

Modes

CONFIGURATION

Usage

Use this command to configure the AAA netgroup name-service to use LDAP.

Examples

```
sonic# configure terminal  
sonic(config)# aaa name-service netgroup group ldap  
  
sonic(config)# no aaa name-service netgroup
```

Releases

3.1 or later

aaa name-service passwd

Configures the AAA password name-service to use LDAP.

Command

```
aaa name-service passwd {{[group ldap]} | [local] | [login]}
```

Options

- group ldap—(Optional) Enables AAA to use group LDAP for the name-service password

- local—(Optional) Enables AAA to use local for the name-service password
- login—(Optional) Enables AAA to use login for the name-service password

Modes CONFIGURATION

Usage Use this command to configure the AAA password name-service to use LDAP.

Examples

```
sonic# configure terminal
sonic(config)# aaa name-service passwd group ldap

sonic(config)# no aaa name-service passwd
```

Releases 3.1 or later

aaa name-service shadow

Configures the AAA shadow name-service to use LDAP.

Command aaa name-service shadow {[group ldap] | [local] | [login]}

- Options**
- group ldap—(Optional) Enables AAA to use group LDAP for the name-service shadow
 - local—(Optional) Enables AAA to use local for the name-service shadow
 - login—(Optional) Enables AAA to use login for the name-service shadow

Modes CONFIGURATION

Usage Use this command to configure the AAA shadow name-service to use LDAP.

Examples

```
sonic# configure terminal
sonic(config)# aaa name-service shadow group ldap

sonic(config)# no aaa name-service shadow
```

Releases 3.1 or later

aaa name-service sudoers

Configures the AAA sudoers name-service to use LDAP.

Command aaa name-service sudoers {[group ldap] | [local]}

- Options**
- group ldap—(Optional) Enables AAA to use group LDAP for the name-service sudoers
 - local—(Optional) Enables AAA to use local for the name-service sudoers

Modes CONFIGURATION

Usage Use this command to configure the AAA sudoers name-service to use LDAP.

Examples

```
sonic# configure terminal
sonic(config)# aaa name-service sudoers group ldap

sonic(config)# no aaa name-service sudoers
```

Releases 3.1 or later

aaa server radius dynamic-author

Enable DAS functionality and enter dynamic authorization local server configuration mode.

Command	aaa server radius dynamic-author
Options	None
Modes	CONFIGURATION
Usage	By default the DAS functionality is disabled. Use this command to enable DAS functionality and enter dynamic authorization local server configuration mode.
Examples	<pre>sonic# configure terminal sonic(config)# aaa server radius dynamic-author</pre>
Releases	4.1.0 or later

abort

Aborts the pending configurations under the MST configuration mode.

Command	abort
Options	None
Modes	SPANNING-TREE MST
Usage	This command aborts the pending configurations that are not yet activated under MST Configuration mode. The configurations that have already been activated are not affected by the abort operation.
Examples	<pre>sonic(config)# spanning-tree mst configuration sonic(config-mst)# abort</pre>
Releases	4.0 or later

access-list

Configures the ACL parameters.

Command	access-list
Options	None
Modes	HARDWARE
Usage	This command is used to enable access-list counters either per entry or per interface entry.
Examples	<pre>sonic(config)# hardware sonic(config-hardware)# access-list sonic(config-hardware-acl)# </pre>
Releases	4.0 or later

activate

Activates the configuration.

Command	activate
Options	None

Modes

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY
- SPANNING-TREE MST

Usage

Use the `activate` command to activate an address-family for a BGP neighbor or peer-group. You can run this command multiple times to enable additional address families for a BGP neighbor or peer-group. In addition, you can use this command to activate configurations, such as MSTP name, region, and instance-to-VLAN mapping. These configurations do not take effect until the command is run on the system, in this way reducing the number of frequent reconvergences.

Examples

Neighbor address family:

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 20.20.20.2
sonic(config-router-bgp-neighbor)# remote-as 300
sonic(config-router-bgp-neighbor)# address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af)# activate
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 20.20.20.2
sonic(config-router-bgp-neighbor)# remote-as 300
sonic(config-router-bgp-neighbor)# address-family 12vpn evpn
sonic(config-router-bgp-neighbor-af)# activate
```

Peer group address family:

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# remote-as 300
sonic(config-router-bgp-pg)# address-family ipv4 unicast
sonic(config-router-bgp-pg-af)# activate
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# remote-as 300
sonic(config-router-bgp-pg)# address-family 12vpn evpn
sonic(config-router-bgp-pg-af)# activate
```

Spanning-tree mst:

```
sonic(config)# spanning-tree mst configuration
sonic(config-mst)# name mst1
sonic(config-mst)# revision 300
sonic(config-mst)# instance 1 vlan 20
sonic(config-mst)# activate
```

```
sonic(config-router-bgp-pg-af)# no activate
sonic(config-router-bgp-neighbor-af)# no activate
```

Releases

3.0 or later

add-reason

Configures drop counter reason.

Command

```
add-reason reason
```

Options

`reason`—Reason of the drop counter. The supported drop counter reasons are ANY, MPLS_MISS, IP_HEADER_ERROR, FDB_AND_BLACKHOLE_DISCARDS, SMAC_EQUALS_DMAR, ACL_ANY, SIP_LINK_LOCAL, DIP_LINK_LOCAL, L3_EGRESS_LINK_DOWN, and EXCEEDS_L3_MTU.

Modes

DROPCOUNTERS

Usage

Drop reasons can be added or deleted when the drop counter is active. However, the counters cannot be cleared during adding or deleting a drop counter.

Examples

```
sonic(config) # dropcounters drop1
sonic(config-dropcounters-drop1) # add-reason any
```

Releases

4.0 or later

addpath-tx-all-paths

Enables BGP to advertise all paths to neighbors in a peer-group.

Command addpath-tx-all-paths

Options None

Modes

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY

Usage Use this command to enable all BGP paths to be advertised to neighbors.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af) # addpath-tx-all-paths
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # addpath-tx-all-paths
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # address-family ipv6 unicast
sonic(config-router-bgp-pg-af) # addpath-tx-all-paths
```

```
sonic(config-router-bgp-pg-af) # no addpath-tx-all-paths
```

Releases

3.0 or later

addpath-tx-bestpath-per-as

Enables advertisement of only the best-path to each AS in a BGP peer-group.

Command addpath-tx-bestpath-per-as

Options None

Modes PEER-GROUP-ADDRESS-FAMILY

Usage Use this command to enable BGP additional path capability, advertise multiple paths for the same prefix but allow only one path to be selected per autonomous system.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # addpath-tx-bestpath-per-as
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
```

```
sonic(config-router-bgp-pg)# address-family ipv6 unicast  
sonic(config-router-bgp-pg-af)# addpath-tx-bestpath-per-as  
  
sonic(config-router-bgp-pg-af)# no addpath-tx-bestpath-per-as
```

Releases 3.0 or later

address-family ipv4

Enters into IPv4 unicast address-family configuration mode.

Command address-family ipv4 unicast

Options None

Modes

- ROUTER-BGP
- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage Use this command to configure BGP neighbors and peer-groups. This command applies to all IPv4 peers belonging to the template or neighbors only.

Examples

```
sonic(config)# router bgp 65300  
sonic(config-router-bgp)# address-family ipv4 unicast  
sonic(config-router-bgp-af)#  
  
sonic(config)# router bgp 65300  
sonic(config-router-bgp)# neighbor 30.30.30.3  
sonic(config-router-bgp-neighbor)# address-family ipv4 unicast  
sonic(config-router-bgp-neighbor-af)#  
  
sonic(config)# router bgp 65300  
sonic(config-router-bgp)# peer-group PG_Ext  
sonic(config-router-bgp-pg)# address-family ipv4 unicast  
sonic(config-router-bgp-pg-af)#  
  
sonic(config-router-bgp-pg)# no address-family ipv4 unicast
```

Releases 3.0 or later

address-family ipv6

Enters IPv6 unicast address-family configuration mode.

Command address-family ipv6 unicast

Options None

Modes

- ROUTER-BGP
- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage Use this command to configure BGP neighbors and peer-groups. This command applies to all IPv6 peers belonging to the template or neighbors only.

Examples

```
sonic(config)# router bgp 65300
sonic(config-router-bgp)# address-family ipv6 unicast
sonic(config-router-bgp-af)#

sonic(config)# router bgp 65300
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# address-family ipv6 unicast
sonic(config-router-bgp-neighbor-af)#

sonic(config)# router bgp 65300
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# address-family ipv6 unicast
sonic(config-router-bgp-pg-af)#

sonic(config-router-bgp-pg)# no address-family ipv6 unicast
```

Releases

3.0 or later

address-family l2vpn

Enters L2VPN EVPN address-family configuration mode.

Command address-family l2vpn evpn**Options** None**Modes**

- ROUTER-BGP
- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage Use this command to configure BGP neighbors and peer-groups.**Examples**

```
sonic(config)# router bgp 65300
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)#

sonic(config)# router bgp 65300
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# address-family l2vpn evpn
sonic(config-router-bgp-neighbor-af)#

sonic(config)# router bgp 65300
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# address-family l2vpn evpn
sonic(config-router-bgp-pg-af)#

sonic(config-router-bgp-pg)# no address-family l2vpn evpn
```

Releases

3.0 or later

advertise ipv4 unicast

Enables tenant VRFs to announce IPv4 prefixes as EVPN type-5 routes.

Command advertise ipv4 unicast**Options** None**Modes** BGP-ADDRESS-FAMILY

Usage This command allows tenant VRFs to announce IPv4 prefixes as EVPN type-5 routes.

Examples

```
sonic(config) # router bgp 100 vrf Vrf1  
sonic(config-router-bgp) # address-family l2vpn evpn  
sonic(config-router-bgp-af) # advertise ipv4 unicast
```

```
sonic(config-router-bgp-af) # no advertise ipv4 unicast
```

Releases 3.0 or later

advertise ipv6 unicast

Enables tenant VRFs to announce IPv6 prefixes as EVPN type-5 routes.

Command advertise ipv6 unicast

Options None

Modes BGP-ADDRESS-FAMILY

Usage This command allows tenant VRFs to announce IPv6 prefixes as EVPN type-5 routes.

Examples

```
sonic(config) # router bgp 100 vrf Vrf1  
sonic(config-router-bgp) # address-family l2vpn evpn  
sonic(config-router-bgp-af) # advertise ipv6 unicast
```

```
sonic(config-router-bgp-af) # no advertise ipv6 unicast
```

Releases 3.0 or later

advertise-all-vni

Enables BGP control plane for all locally configured VNIs.

Command advertise-all-vni

Options None

Modes BGP-ADDRESS-FAMILY

Usage Use this command to advertise all VNIs configured on the switch.

Examples

```
sonic(config) # router bgp 100  
sonic(config-router-bgp) # address-family l2vpn evpn  
sonic(config-router-bgp-af) # advertise-all-vni
```

```
sonic(config-router-bgp-af) # no advertise-all-vni
```

Releases 3.0 or later

advertise-default-gw

Enables gateway advertisement.

Command advertise-default-gw

Options None

Modes • ADDRESS-FAMILY-VNI

- BGP-ADDRESS-FAMILY

Usage

Use this command to enable gateway advertisements for a specific VNI, or for gateway VTEPs to advertise their IP/MAC addresses.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)# vni 100
sonic(config-router-bgp-af-vni)# advertise-default-gw
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)# advertise-default-gw
```

```
sonic(config-router-bgp-af)# no advertise-default-gw
```

Releases

3.0 or later

advertise-pip

Configures PIP parameters.

Command `advertise-pip [ip A.B.C.D [peer-ip A.B.C.D] | [peer-ip A.B.C.D] {}]`

Options

- `ip A.B.C.D`—(Optional) IP address in A.B.C.D format
- `peer-ip A.B.C.D`—(Optional) Peer IP address in A.B.C.D format

Modes BGP-ADDRESS-FAMILY

Usage Once this feature is enabled, it is applied to all VRFs and cannot be controlled per VRF. Therefore, it is not recommended to remove the `advertise-pip` configuration using `no advertise-pip` command.

Examples

```
sonic# configure terminal
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)# advertise-pip peer-ip 1.1.1.1
```

Releases

3.2 or later

advertise-svi-ip

Enables SVI MAC IP routes advertisement into EVPN, or for a specific VNI.

Command `advertise-svi-ip`

Options None

Modes

- BGP-ADDRESS-FAMILY-L2VPN-EVPN
- VNI

Usage Use this command to advertise the SVI MAC-IP routes.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)# advertise-svi-ip
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family l2vpn evpn
```

```
sonic(config-router-bgp-af)# vni 100
sonic(config-router-bgp-af-vni)# advertise-svi-ip

sonic(config-router-bgp-af)# no advertise-svi-ip
```

Releases 3.1 or later

advertisement-interval

Sets the minimum time interval between sending routing updates to a neighbor, or neighbors in a peer-group.

Command	<code>advertisement-interval <i>seconds</i></code>
Options	<i>seconds</i> —Time value in seconds
Modes	<ul style="list-style-type: none">• BGP-NEIGHBOR• BGP-PEER-GROUP• VRRP
Usage	Use this command to configure the time in seconds between sending BGP route updates to neighbors, or neighbors in a peer-group. The time range for eBGP and iBGP is from 0 to 600 seconds. The default is 0. This command is also used to configure the advertisement-interval in seconds for VRRP. The time range for VRRP is from 1 to 255 seconds. The default is 1 second.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# advertisement-interval 10

sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# advertisement-interval 10

sonic(config-if-Ethernet4)# vrrp 1 address-family ipv4
sonic(config-if-Ethernet4-vrrp-ipv4-1)# advertisement-interval 1

sonic(config-if-Ethernet4)# vrrp 1 address-family ipv6
sonic(config-if-Ethernet4-vrrp-ipv6-1)# advertisement-interval 2

sonic(config-router-bgp-pg)# no advertisement-interval
```

Releases 3.0 or later

aggregate-address

Configures an aggregate address and enables aggregation of routes that falls in the aggregate address subnet.

Command	<code>aggregate-address <i>prefix</i> {[as-set] [summary-only] {[route-map <i>rtemap_name</i>]}}</code>
Options	<ul style="list-style-type: none">• <i>prefix</i>—IP address prefix in A.B.C.D/mask format• <i>as-set</i>—(Optional) Advertises the aggregate routes contained in the summary aggregate-prefix entry• <i>summary-only</i>—(Optional) Suppresses the advertisement of specific routes in the prefix range to neighbors• <i>route-map <i>rtemap_name</i></i>—(Optional) Route-map name
Modes	BGP-ADDRESS-FAMILY

Usage

Use this command to configure an aggregate address entry in the BGP routing table. Aggregate entries reduce the size of the routing table. An aggregate prefix combines contiguous networks into a summarized set of IP addresses. This command enables you to turn on aggregation of BGP routes. The `summary-only` option filters out all the aggregate routes and only the aggregate address is advertised by BGP. The `as-set` option ensures that the AS path of individual aggregated routes is also in the resulting aggregate route. The `route-map` option provides a finer control over the route attributes.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family ipv4 unicast
sonic(config-router-bgp-af)# aggregate-address 17.35.0.0/16

sonic(config-router-bgp-af)# no aggregate-address 17.35.0.0/16
```

Releases

3.0 or later

aging-interval

Configures an aging-interval for configured drop-monitor flows.

Command `aging-interval seconds`

Options `seconds`—Interval wait time in seconds (1 to 30)

Modes TAM-DROP-MONITOR

Usage The `aging-interval` command is used to configure an aging-interval for drop-monitor flows configured in the system. The aging interval determines how long the system waits before it decides that drops have ceased on a flow. Any changes to the aging interval are effective only for newly created sessions.

Examples

```
sonic(config)# tam
sonic(config-tam)# drop-monitor
sonic(config-tam-dm)# aging-interval 6
%Info: Any changes to aging-interval are effective for newly created
sessions only.

sonic(config-tam-dm)# no aging-interval
```

Releases

3.0 or later

alarm acknowledge

Acknowledges an alarm event to show that you are aware of the fault and do not consider the alarm condition to be significant.

Command `alarm acknowledge event-id`

Options `event-id`—Acknowledges the alarm with the specified event ID number in `show alarm` output.

Modes EXEC

Usage In the `show event` output, `ACKNOWLEDGE` indicates that a support engineer is aware of the alarm condition that has been raised and does not consider the fault to be catastrophic. The alarm is not cleared, but is removed from the count in alarm statistics.

Example

```
sonic# alarm acknowledge 3
```

Releases

4.2.0 or later

alarm unacknowledge

Unacknowledges an alarm event so that it is again raised as an active alarm.

Command	alarm unacknowledge <i>event-id</i>
Options	<i>event-id</i> —Unacknowledges the alarm with the specified event ID number in show alarm output.
Modes	EXEC
Usage	In the show event output, UNACKNOWLEDGE restores an alarm to RAISE status and updates the alarm statistics.
Example	<pre>sonic# alarm unacknowledge 3</pre>
Releases	4.2.0 or later

algorithm

Specifies the ARS algorithm to be used for quality computation in the ARS profile.

Command	algorithm EWMA
Options	EWMA—The only algorithm available is the exponential weighted moving average (EWMA). The default is EWMA.
Modes	ARS-PROFILE
Usage	This is the only available option for the algorithm command.
Examples	<pre>sonic(config-ars-profile)# algorithm EWMA</pre>
Releases	4.4.0 or later

alias

Adds drop counter alias.

Command	alias <i>string</i>
Options	<i>string</i> —Descriptive string (up to 24 characters)
Modes	DROPCOUNTERS
Usage	This command is used to assign an alias in place of the new counter name.
Examples	<pre>sonic# configure terminal sonic(config)# dropcounters drop1 sonic(config-dropcounters-drop1)# alias counter</pre>
Releases	4.0 or later

allow high-wattage optics

Enables high-power optics on ports.

Command	allow high-wattage optics
Options	None
Modes	INTERFACE

Usage

By default, this command is enabled on all the physical interfaces. Use the no version of this command to disable high-power optics on the interface or interfaces. If you disable high-power optics, this configuration is displayed in the show running-configuration command output. This command is applicable only on Z9332F-ON and Z9432F-ON devices. For more information about high-power optics, see *Enterprise SONiC Distribution high-power optics*.

Examples

```
sonic(config) # interface Eth1/1
sonic(config-if-Eth1/1) # allow high-wattage-optics
```

Releases

4.1.0 or later

allowas-in

Enables the BGP speaker to accept a route with the local AS number in updates received from a peer for the specified number of times.

Command

```
allowas-in {[number] | [origin]}
```

Options

number—(Optional) Number of occurrences for a local AS number (1 to 10)

Modes

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY

Usage

Use this command to configure the number of times the local AS number can appear in the BGP AS_PATH path attribute before the switch rejects the route. This command enables the BGP speaker to accept a route with the local AS number in updates received from a peer for the specified number of times. Accepting own AS in an AS path usually results in an AS loop. You can add the AS number to influence the BGP route selection process. This command enables you to control when a route with as-path containing its own AS number should be accepted or not. The command also provides flexibility in terms of the maximum number of occurrences of AS number in an AS path.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af) # allowas-in 5
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family 12vpn evpn
sonic(config-router-bgp-neighbor-af) # allowas-in 5
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # remote-as 300
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # allowas-in
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # remote-as 300
sonic(config-router-bgp-pg) # address-family 12vpn evpn
sonic(config-router-bgp-pg-af) # allowas-in
```

```
sonic(config-router-bgp-neighbor-af) # no allowas-in 5
sonic(config-router-bgp-neighbor-af) # no allowas-in 5
sonic(config-router-bgp-pg-af) # no allowas-in
```

Releases

3.0 or later

always-compare-med

Instructs BGP to always compare MED attributes in the paths that are received from different neighbors.

Command	always-compare-med
Options	None
Modes	ROUTER-BGP
Usage	Use this command to always compare the MED on routes, even when they are received from different neighbors. Setting this option makes the order of preference of routes more defined, and should eliminate MED induced oscillations.
Examples	<pre>sonic(config) # router bgp 65300 sonic(config-router-bgp) # always-compare-med</pre> <pre>sonic(config-router-bgp) # no always-compare-med</pre>
Releases	3.0 or later

area

Configures OSPF parameters.

Command	area areaid [[authentication [message-digest] [default-cost defaultcost] [filter-list {prefix {prefixlistname {in out}}}] [range {prefix {[advertise {[cost metrictcost]}]} [cost metrictcost] [not-advertise] [substitute rangenetworkprefix]}]} {[stub [no-summary]} {[virtual-link {vlinkip {{[authentication {[null] [message-digest]}]} {[authentication-key {auth-key [encrypted]}]} {[message-digest-key {keyid {md5 {md5key [encrypted]}}}]} {[dead-interval deadinterval]} {[hello-interval hellointerval]} {[retransmit-interval retransmitinterval]} {[transmit-delay transmitinterval]}]}]} {[shortcut {default disable enable}]}]
Options	<ul style="list-style-type: none">• <i>area_id</i>—Configures an area within the switch in A.B.C.D format or enter a number between 0 and 4294967295• <i>defaultcost</i>—Configures NSSA or the stub-area summary default cost (0 to 1677215)• <i>prefixlistname</i>—Configures the prefix-list for interarea prefix filtering; use this option to configure interarea prefix propagation policies• <i>prefix</i>—Configures the range prefix in A.B.C.D/mask format• <i>metrictcost</i>—Configures the metric cost• <i>rangenetworkprefix</i>—Configures the range network prefix in A.B.C.D/mask format• <i>vlinkip</i>—Configures the virtual link prefix in A.B.C.D format• <i>auth-key</i>—Configures the authentication key• <i>keyid</i>—Configures the authentication key ID• <i>md5key</i>—Configures the authentication MD5 key• <i>deadinterval</i>—Configures the dead interval• <i>hellointerval</i>—Configures the hello interval• <i>retransmitinterval</i>—Configures the retransmit interval• <i>transmitinterval</i>—Configures the transmit interval
Modes	ROUTER-OSPF
Usage	Use this command to configure area-related parameters within an OSPFv2 switch. Option <i>in</i> is used for filtering incoming prefixes from the area, and <i>out</i> is used for filtering outgoing prefixes from the area. This command configures prefix advertising rules directly without using any prefix list. The cost of an advertised prefix can be modified using this command. An advertised prefix can be substituted by another prefix. Virtual link configurations are allowed on a nonbackbone area. Virtual links can have clear text

password, message-digest based passwords, or no password configured. When a clear text and message digest password is configured, corresponding authentication-key or message-digest-key parameters must be configured. Timer parameters can also be configured for any virtual links. The authentication key or password will be saved in encrypted form in the configuration. You must provide an actual password while configuring authentication keys. It is not recommended to use an encrypted option of an authentication key.

Examples

```
sonic(config)# router ospf
sonic(config-router-ospf)# area 19
sonic(config-router-ospf)# area 19.1.1.19
sonic(config-router-ospf)# area 19 authentication
sonic(config-router-ospf)# area 19 authentication message-digest
sonic(config-router-ospf)# area 19 filter-list prefix plist-area10_in in
sonic(config-router-ospf)# area 19 filter-list prefix plist-area10_out out
sonic(config-router-ospf)# area 19 range 10.1.1.2/24
sonic(config-router-ospf)# area 19 range 10.1.1.0/24 cost 48
sonic(config-router-ospf)# area 19 range 10.2.2.0/24 not-advertise
sonic(config-router-ospf)# area 19 range 10.3.3.0/24 substitute 192.3.3.0/24
sonic(config-router-ospf)# area 19 stub
sonic(config-router-ospf)# area 19 stub no summary
sonic(config-router-ospf)# area 19 shortcut enable
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 authentication
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 authentication null
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 authentication message-digest
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 authentication-key password
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 message-digest-key 19 md5
md5password
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 dead-interval 60
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 hello-interval 20
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 retransmit-interval 15
sonic(config-router-ospf)# area 19 virtual-link 1.1.1.9 transmit-delay 10

sonic(config-router-ospf)# no area 19
sonic(config-router-ospf)# no area 19.1.1.19
sonic(config-router-ospf)# no area 19 authentication
sonic(config-router-ospf)# no area 19 authentication message-digest
sonic(config-router-ospf)# no area 19 filter-list prefix plist-area10_in in
sonic(config-router-ospf)# no area 19 filter-list prefix plist-area10_out out
sonic(config-router-ospf)# no area 19 range 10.1.1.2/24
sonic(config-router-ospf)# no area 19 range 10.1.1.0/24 cost 48
sonic(config-router-ospf)# no area 19 range 10.2.2.0/24 not-advertise
sonic(config-router-ospf)# no area 19 range 10.3.3.0/24 substitute 192.3.3.0/24
sonic(config-router-ospf)# no area 19 stub
sonic(config-router-ospf)# no area 19 stub no summary
sonic(config-router-ospf)# no area 19 shortcut enable
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 authentication
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 authentication null
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 authentication message-digest
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 authentication-key password
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 message-digest-key 19 md5
md5password
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 dead-interval 60
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 hello-interval 20
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 retransmit-interval 15
sonic(config-router-ospf)# no area 19 virtual-link 1.1.1.9 transmit-delay 10
```

Releases

3.2 or later

ars bind

Binds the ARS port profile to the port for the profile to take effect.

Command `ars bind port-profile-name`

Options `port-profile-name`—Enter a port profile name.

Modes INTERFACE

Usage You can bind a port profile only on physical ports. If a port already has a port profile and you try to bind with a new port profile, the new profile replaces the old port profile. You can bind a profile to a range of ports. If you configure breakout on a port, any existing ARS port-profile is removed.

Example

```
sonic(config-if-Ethernet32)# ars bind default
```

Releases 4.4.0 or later

ars bind profile

Binds an ARS profile to the switch.

Command `ars bind profile profile-name`

Options *profile-name*—ARS profile name.

Modes CONFIGURATION

Usage This command binds an ARS profile to the switch for the profile to take effect.

Examples

```
sonic(config) # ars bind profile default
```

Releases 4.4.0 or later

enable

Enables ARS on a port. By default, ARS disabled.

Command `enable`

Options None.

Modes ARS-PORT-PROFILE

Usage By default, this option is disabled.

Example

```
sonic(config-ars-port-profile) # enable
```

Releases 4.4.0 or later

ars object

Creates an ARS object with an object name.

Command `ars object ars-object-name`

Options *ars-object-name*—Enter an ARS object name.

Modes CONFIGURATION

Usage Create an ARS object for next-hop group-level binding.

Examples

```
sonic(config) #ars object default
```

Releases 4.4.0 or later

ars port-profile

Create a port profile for ARS with a profile name.

Command `ars port-profile ars-port-profile-name`

Options *ars-port-profile-name*—Enter a port profile name for ARS with a maximum of 15 characters.

Modes CONFIGURATION

Usage The profile takes effect once the same is bound to a port. If the profile exists, the command level changes to the port profile level.

Example

```
sonic(config) # ars port-profile default
```

Releases 4.4.0 or later

ars profile

Creates an adaptive routing and switching (ARS) profile with a profile name.

Command `ars profile profile-name`

Options *profile-name*—ARS profile name with a maximum of 15 characters.

Modes CONFIGURATION

Usage The profile takes effect after the same is bound to the switch. If the profile exists, the command level changes to the profile level.

Example

```
sonic(config) # ars profile default
sonic(config-ars-profile) #
```

Releases 4.4.0 or later

as-notation

Configures the display of AS numbers in show command outputs.

Command `as-notation {asdot | asdot+}`

Options

- `asdot`—Display AS numbers in both asplain (single 32-bit decimal integer, 1 to 4294967295) and asdot+ (two 16-bit decimal integers joined by a period, 0.1 to 65535.65535) format based on the numerical value of the AS number.
- `asdot+`—Display AS numbers in only asdot+ format (two 16-bit decimal integers joined by a period, 0.1 to 65535.65535).

Modes ROUTER-BGP

Usage The asdot notation combines both asdot+ notation and the default asplain notation (32-bit decimal integer) based on the numerical value of the AS number: Values equal to and above 65536 are formatted in asdot+ notation; values below 65536 are formatted in asplain notation. To restore the default AS display in asplain format, use the `no as-notation` command.

Examples

```
sonic# show configuration
router bgp 65636
...
sonic# configure terminal
sonic(config) # router bgp 65636
sonic(config-router-bgp) # as-notation asdot+
sonic(config-router-bgp) # show configuration
router bgp 1.100

sonic(config-router-bgp) # no as-notation
sonic(config-router-bgp) # show configuration
router bgp 65636
...
```

Releases 4.4.0 or later

as-override

Instructs BGP to override AS numbers in outbound updates if as-path equals remote-as.

Command	as-override
Options	None
Modes	<ul style="list-style-type: none">NEIGHBOR-ADDRESS-FAMILYPEER-GROUP-ADDRESS-FAMILY
Usage	Use this command to override the outbound route updates to an AS path that includes the remote AS configured with the BGP neighbor or peer-group <code>remote-as</code> command.
Example	<pre>sonic(config) # router bgp 100 sonic(config-router-bgp) # neighbor 20.20.20.2 sonic(config-router-bgp-neighbor) # remote-as 300 sonic(config-router-bgp-neighbor) # address-family ipv4 unicast sonic(config-router-bgp-neighbor-af) # as-override</pre> <pre>sonic(config) # router bgp 100 sonic(config-router-bgp) # peer-group PG_Ext sonic(config-router-bgp-pg) # address-family ipv4 unicast sonic(config-router-bgp-pg-af) # as-override</pre> <pre>sonic(config-router-bgp-neighbor-af) # no as-override sonic(config-router-bgp-pg-af) # no as-override</pre>
Releases	3.0 or later

attribute-unchanged

Instructs BGP to propagate route attributes unchanged to this neighbor, or neighbors in a peer-group.

Command	attribute-unchanged [as-path] [med] [next-hop]
Options	<ul style="list-style-type: none">as-path—(Optional) Use the AS path attribute to propagate unchangedmed—(Optional) Use the MED attribute to propagate unchangednext-hop—(Optional) Use the next-hop attribute to propagate unchanged
Modes	<ul style="list-style-type: none">NEIGHBOR-ADDRESS-FAMILYPEER-GROUP-ADDRESS-FAMILY
Usage	Use this command to propagate BGP route attributes unchanged to this neighbor, or neighbors in a peer-group. You can control which attributes are propagated unchanged.
Examples	<pre>sonic(config) # router bgp 100 sonic(config-router-bgp) # neighbor 20.20.20.2 sonic(config-router-bgp-neighbor) # remote-as 300 sonic(config-router-bgp-neighbor) # address-family ipv4 unicast sonic(config-router-bgp-neighbor-af) # attribute-unchanged as-path next-hop</pre> <pre>sonic(config) # router bgp 100 sonic(config-router-bgp) # neighbor 20.20.20.2 sonic(config-router-bgp-neighbor) # remote-as 300 sonic(config-router-bgp-neighbor) # address-family 12vpn evpn sonic(config-router-bgp-neighbor-af) # attribute-unchanged as-path next-hop</pre> <pre>sonic(config) # router bgp 100 sonic(config-router-bgp) # peer-group PG_Ext</pre>

```

sonic(config-router-bgp-pg)# address-family ipv4 unicast
sonic(config-router-bgp-pg-af)# attribute-unchanged as-path next-hop

sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# address-family l2vpn evpn
sonic(config-router-bgp-pg-af)# attribute-unchanged as-path next-hop

sonic(config-router-bgp-neighbor-af)# no attribute-unchanged
sonic(config-router-bgp-pg-af)# no attribute-unchanged

```

Releases

3.0 or later

auditd-system rules

Configures rules for the Linux Audit logging service (Auditd system) on the switch to monitor system components, including system and network changes, file access and updates, and user logins and logouts.

Command

auditd-system rules {basic | detail | custom}

Options

- basic—Use a basic set of Audit rules.
- detail—Use a more detailed set of Audit rules for finer filtering of Auditd messages.
- custom—Use a custom set of Audit rules that is named `auditd-custom.rules` and stored at `config://auditd-custom.rules`.

Modes

CONFIGURATION

Usage

In addition to the Syslog and Audit log messages (`event`, `log`, and `audit`) that you can send to a remote server, the `auditd-system` message is supported for kernel audit messages. The Auditd system is enabled by default in Enterprise SONiC, but Auditd logging rules are not configured. Use the `auditd-system rules` command to configure a set of Auditd logging rules. Only the `secadmin` role can configure and view Auditd system rules.

Examples

```

sonic(config)# auditd-system rules basic

sonic(config)# auditd-system rules detail

sonic# copy sourcefilepath config://auditd-custom.rules
sonic(config)# auditd-system rules custom

sonic(config)# no auditd-system rules custom

```

Releases

4.4.0 or later

auth-type

Specify the type of authorization that the device must use for clients.

Command

auth-type {any | all | session-key}

Options

- any—Selects all COA client authentication types. All authentication attributes must match for the authentication to succeed.
- all—Selects any COA client authentication type. Any authentication attribute may match for the authentication to succeed.
- session-key—Indicates that the session-key must match for authentication to succeed.

Modes

RADIUS-DA

Usage The client must match the configured attributes for authorization. When the device is configured to ignore the session-key using the `ignore session-key` command, authentication type of the device cannot be set to session-key. The default is all.

Examples

```
sonic(config-radius-da) # auth-type any
```

Releases 4.1.0 or later

authentication command bounce-port ignore

Configure the device to ignore a RADIUS server when it receives a `bounce-host-port` message.

Command `authentication command bounce-port ignore`

Options None

Modes EXEC

Usage Use this command to configure the device to ignore a RADIUS server `bounce-host-port` command. The `bounce-host-port` message causes a host to flap the link on an authentication port.

Examples

```
sonic# authentication command bounce-port ignore
```

Releases 4.1.0 or later

authentication command disable-port ignore

Configure the device to ignore a RADIUS server when it receives a `disable-host-port` message.

Command `authentication command disable-port ignore`

Options None

Modes EXEC

Usage Use this command to configure the device to ignore a RADIUS server `disable-host-port` command. The `disable-host-port` message puts the host port to D-Disabled state with the reason as `coa disabled`.

Examples

```
sonic# authentication command disable-port ignore
```

Releases 4.1.0 or later

authentication event fail action authorize

Configures the unauthenticated VLAN associated with the specified interface or range of interfaces.

Command `authentication event fail action authorize vlan vlan-id`

Options *vlan-id*—Enter the VLAN ID (1 to 4094)

Modes INTERFACE

Usage Use this command to configure the unauthenticated VLAN on an interface to authorize 802.1x-aware clients which fail authentication or when their authentication times out. This VLAN is used when the AAA server fails to recognize the client credentials and rejects the authentication attempt. The range is 1 to the maximum VLAN ID supported by the platform or alive server actions. By default, the guest VLAN is 0, which means it is not operational.

Examples

```
sonic# configure terminal
sonic(config)# interface Eth1/1
sonic(config-if-Eth1/1)# authentication event fail action authorize vlan
1
```

Releases

4.0 or later

authentication event no-response

Configures actions when no response is received for EAP.

Command

```
authentication event no-response action authorize vlan vlan-id
```

Options

vlan-id—Enter the VLAN ID (1 to 4094).

Modes

INTERFACE

Usage

Use this command to configure VLAN as guest VLAN on an interface. The range is 1 to the maximum VLAN ID supported by the platform or alive server actions. By default, the guest VLAN is 0, that is invalid and is not operational.

Examples

```
sonic# configure terminal
sonic(config)# interface Eth1/1
sonic(config-if-Eth1/1)# authentication event no-response action
authorize vlan 1
```

Releases

4.0 or later

authentication host-mode

Configures the host mode on an interface or range of interfaces.

Command

```
authentication host-mode {multi-auth | multi-domain | multi-host | single-
host}
```

Options

- *multi-auth*—Multi-authentication mode
- *multi-domain*—Multi-domain mode
- *multi-host*—Multi-host mode
- *single-host*—Single host mode

Modes

INTERFACE

Usage

The configuration on the interface mode takes precedence over the global configuration of this parameter.

Examples

```
sonic# configure terminal
sonic(config)# interface Eth1/1
sonic(config-if-Eth1/1)# authentication host-mode multi-domain
```

```
sonic# configure terminal
sonic(config)# interface Eth1/1
sonic(config-if-Eth1/1)# no authentication host-mode
```

Releases

4.0 or later

authentication max-users

Sets the maximum number of clients that are supported on an interface when multiauthentication host mode is enabled on the port.

Command	<code>authentication max-users <i>max-users</i></code>
Options	<i>max-users</i> —Enter the maximum users (1 through 48; default is 48).
Modes	INTERFACE
Usage	Use this command to set the maximum number of clients that are supported on an interface or range of interfaces when multiauthentication host mode is enabled on the port.
Examples	<pre>sonic# configure terminal sonic(config)# interface Eth1/1 sonic(config-if-Eth1/1)# authentication max-users 16</pre> <pre>sonic# configure terminal sonic(config)# interface Eth1/1 sonic(config-if-Eth1/1)# no authentication max-users</pre>
Releases	4.0 or later

authentication monitor

Enables or disables Authentication Monitor mode support on the switch.

Command	<code>authentication monitor</code>
Options	None
Modes	CONFIGURATION
Usage	The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an authentication enforced port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.
Example	<pre>sonic(config)# authentication monitor</pre>
Releases	3.1 or later

authentication open

Enables or disables Open Authentication mode on the specified interfaces.

Command	<code>authentication open</code>
Options	None
Modes	INTERFACE
Usage	This option is disabled by default.

Examples

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1  
sonic(config-if-Ethernet1)# authentication open
```

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1  
sonic(config-if-Ethernet1)# no authentication open
```

Releases

4.0 or later

authentication order

Sets the order of authentication methods that are used on the interface.

Command authentication order {dot1x [mab] | mab [dot1x]}

- Options**
- dot1x—Select IEEE 802.1X
 - mab—Select MAB

Modes INTERFACE**Usage**

This command sets the order of authentication methods that the switch attempts when trying to authenticate a new device connected to a port. If one method in the list is unsuccessful or timed out, the next method is attempted. Each method can only be entered once. The default order is dot1x and then MAB.

Examples

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1  
sonic(config-if-Ethernet1)# authentication order dot1x mab
```

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1  
sonic(config-if-Ethernet1)# no authentication order
```

Releases

4.0 or later

authentication periodic

Enables periodic reauthentication of the supplicant for the specified interface or range of interfaces.

Command authentication periodic**Options** None**Modes** INTERFACE**Usage** By default, this feature is disabled on the switch.**Examples**

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1  
sonic(config-if-Ethernet1)# authentication periodic
```

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1  
sonic(config-if-Ethernet1)# no authentication periodic
```

Releases

4.0 or later

authentication port-control

Sets the authentication mode to use on the specified interface or range of interfaces.

Command	authentication port-control {auto force-authorized force-unauthorized}
Options	<ul style="list-style-type: none">• auto — Enter auto for default Auto mode.• force-authorized — Enter force-authorized to disable authentication check.• force-unauthorized — Enter force-unauthorized to deny all access through this interface.
Modes	INTERFACE
Usage	The configuration on the interface mode takes precedence over the global configuration of this parameter.
Examples	<pre>sonic# configure terminal sonic(config)# interface Ethernet 1 sonic(config-if-Ethernet1)# authentication port-control auto</pre> <pre>sonic# configure terminal sonic(config)# interface Ethernet 1 sonic(config-if-Ethernet1)# no authentication port-control</pre>
Releases	4.0 or later

authentication priority

Sets the priority for the authentication methods to be used on the interface.

Command	authentication priority {dot1x [mab] mab [dot1x]}
Options	<ul style="list-style-type: none">• dot1x—Set IEEE 802.1X as the priority authentication method.• mab—Set MAB as the priority authentication method.
Modes	INTERFACE
Usage	The authentication priority determines if a client, which is already authenticated, needs to reauthenticate with the higher-priority method when the same authentication priority is received. The default order is dot1x, MAB.
Examples	<pre>sonic# configure terminal sonic(config)# interface Ethernet 1 sonic(config-if-Ethernet1)# authentication priority dot1x mab</pre> <pre>sonic# configure terminal sonic(config)# interface Ethernet 1 sonic(config-if-Ethernet1)# no authentication priority</pre>
Releases	4.0 or later

authentication rest

Configures REST authentication modes.

Command	authentication rest auth-mode
Options	<p>auth-mode—Where auth-mode is one or more of the following values that are separated by commas:</p> <ul style="list-style-type: none">• password—Enable HTTP password authentication.• jwt—Enable JWT token-based authentication.• cert—Enable certificate-based authentication.

- `none`—Remove the configured authentication modes, and restore the defaults: HTTP password and JWT authentication.

Modes CONFIGURATION

Usage Enter multiple values for `auth-mode` by separating them with a comma, as shown.

Examples

```
sonic(config)# authentication rest password,jwt,cert
```

Releases 3.1 or later

authentication telemetry

Configures the authentication telemetry modes.

Command `authentication telemetry auth_mode`

Options `auth_mode`—Where `auth-mode` is one or more of the following values that are separated by commas:

- `password`—Enable HTTP password authentication.
- `jwt`—Enable JWT token-based authentication.
- `cert`—Enable certificate-based authentication.
- `none`—Remove the configured authentication modes, and restore the defaults: HTTP password and JWT authentication.

Modes CONFIGURATION

Usage Enter multiple values for `auth-mode` by separating them with a comma, as shown.

Examples

```
sonic(config)# authentication telemetry password,jwt,cert
```

Releases 3.1 or later

authentication timer reauthenticate

Configures the time after which the authenticator attempts to reauthenticate a supplicant on the port.

Command `authentication timer reauthenticate {server | time-period}`

Options

- `server`—Get the reauthentication timeout value from the server.
- `time-period`—Enter the time period in seconds (1-65535).

Modes INTERFACE

Usage For periodic reauthentication to be performed after the configured or server-provided timeout period, you must configure the [authentication periodic](#) command. This command also provides an option to specify a reauthentication time-out value from a remote server such as a RADIUS server. When you configure the `server` option, the server-supplied session time-out and session termination-action are used by authenticator to reauthenticate a supplicant on the port. By default, the `server` option is enabled.

Examples

```
sonic# configure terminal
sonic(config)# interface Ethernet 1
sonic(config-if-Ethernet1)# authentication timer reauthenticate server
```

```
sonic# configure terminal
sonic(config)# interface Ethernet 1
sonic(config-if-Ethernet1)# no authentication timer reauthenticate
```

Releases 4.0 or later

auto-breakout

Enables front-panel Ethernet ports to automatically detect SFP media and auto-configure breakout interfaces.

Command	auto-breakout
Options	None
Modes	CONFIGURATION
Usage	<p>By default, auto-breakout is not enabled. If you enable auto-breakout on the switch and remove the manually configured breakout configuration on a port (<code>no interface breakout port slot/port</code> command), the auto-breakout setting based on the installed transceiver is applied on the port interface. Afterwards, when you plug a supported breakout cable in a QSFP+, QSFP28, QSFP56, QSFP-DD, or SFP56-DD port, the port auto-configures breakout interfaces for media type and speed. Later, if you use the <code>interface breakout port</code> command to manually configure breakout interfaces, the media type plugged into a port is no longer automatically learned. To disable the auto-breakout feature, use the <code>no auto-breakout</code> command. The current breakout configuration on port interfaces remains unchanged.</p>
Examples	<pre>sonic(config)# auto-breakout</pre>
Releases	4.4.0 or later

auto-cost

Calculates default metrics for the interface based on the configured auto-cost reference bandwidth value.

Command	auto-cost reference-bandwidth <i>ref-bandwidth</i>
Options	<i>ref-bandwidth</i> —Reference bandwidth value to calculate the interface cost in megabits per second (1 to 4294967; default 100)
Modes	ROUTER-OSPF
Usage	<p>Whenever interface cost is not configured explicitly, reference bandwidth value is used to calculate the interface cost. By default, OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface.</p>
Examples	<pre>sonic(config)# router ospf 10 sonic(config-router-ospf-10)# auto-cost reference-bandwidth 1000</pre> <pre>sonic(config-router-ospf-10)# no auto-cost reference-bandwidth</pre>
Releases	3.1 or later

autoneg

Configures autonegotiation on the Management interface.

Command	autoneg {on off}
Options	<ul style="list-style-type: none">• <code>on</code> — Enables interface speed autonegotiation• <code>off</code> — Disables interface speed autonegotiation (default)
Modes	INTERFACE
Usage	<p>Use this command to set a Management interface to autonegotiate speed with a connected device. Autonegotiation is disabled by default. Both sides of a link must have autonegotiation enabled or disabled for the link to come up. <code>no autoneg</code> command resets interface speed autonegotiation to the default: <code>autoneg off</code>.</p>

Examples

```
sonic(config) # interface Management 0
sonic(config-if-ma0) # autoneg

sonic(config-if-ma0) # no autoneg
```

Releases

3.0 or later

autort

Enables automatic derivation of route-distinguisher and route-targets.

Command autort rfc8365-compatible

Options None

Modes BGP-ADDRESS-FAMILY

Usage Use this command to enable the autogeneration of route-target import and export values as described in RFC 8365. A route target (RT) controls the way that EVPN routes are distributed and learned. A receiving VTEP downloads BGP EVPN route information for matching import RT values.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # address-family l2vpn evpn
sonic(config-router-bgp-af) # autort rfc8365-compatible

sonic(config-router-bgp-af) # no autort rfc8365-compatible
```

Releases

3.0 or later

autostate

Configures autostate on a VLAN interface.

Command autostate

Options None

Modes INTERFACE *vlan-if-name*

Usage

VLAN autostate is enabled by default on all VLANs. When enabled, the operational status of a VLAN is determined according to the operational status of its physical port and port channel members.

- If enabled, the VLAN Operstatus depends on the VLAN Member operstatus and the VRF-VNI mappings.
- If disabled, the VLAN Operstatus is set as Up after it is created.

To configure autostate settings, use the `interface Vlan`, `interface range create vlan_range_num`, and `interface range vlan_range_num` commands.

Examples

```
sonic-cli(config) # interface Vlan 10
sonic-cli(config-if-Vlan10) # autostate
```

```
sonic-cli(config) # interface Vlan 10
sonic-cli(config-if-Vlan10) # no autostate
```

Releases

4.0 or later

B commands

Topics:

- banner login
- banner motd
- bestpath as-path confed
- bestpath as-path ignore
- bestpath as-path multipath-relax
- bestpath compare-routerid
- bestpath med
- bfd
- bgp as-path-list
- bgp community-list
- bgp extcommunity-list
- binding
- buffer default-lossless-buffer-profile
- buffer init lossless
- buffer pool
- buffer priority-group
- buffer profile
- buffer queue

banner login

Configures a customized system login text banner.

Command `banner login delimiter`

Options `delimiter`—Enter a recommended delimiter character: @, %, ^, *, or + or an alphanumeric character, such as A, B, C... or 0, 1, 2.... Then press Enter.

Modes CONFIGURATION

Usage Enter each line of text and press **Enter**. You can enter a maximum of 4096 characters. Complete the login banner configuration by entering a line that contains only the delimiter character and press Enter. To delete a login banner and reset it to the default text, use the `no banner login` command. To disable the login banner so that it does not display, use the `banner login disable` command.

Example

```
sonic(config)# banner login %
Dell Z9664F-ON login
Enter your username and password
%
sonic(config) #
```

Releases

4.4.0 or later

banner motd

Configures a customized message of the day (MOTD) text banner.

Command `banner motd delimiter`

Options	<code>delimiter</code> —Enter a recommended delimiter character: @, %, ^, *, or + or an alphanumeric character, such as A, B, C... or 0, 1, 2.... Then press Enter.
Modes	CONFIGURATION
Usage	Enter each line of text and press Enter . You can enter a maximum of 4096 characters. There is no limit to the number of lines. Complete the MOTD banner configuration by entering a line that contains only the delimiter character and press Enter. To delete an MOTD banner and reset it to the default text, use the <code>no banner motd</code> command. To disable the MOTD banner so that it does not display, use the <code>banner motd disable</code> command.
Example	<pre>sonic(config)# banner motd % Dell Z9664F-ON Today's tip: Press tab or spacebar for command completion. Have a nice day! % sonic(config) #</pre>
Releases	4.4.0 or later

bestpath as-path confed

Instructs BGP to consider confederation path length in as-path length comparison during best-path selection process.

Command	<code>bestpath as-path confed</code>
Options	None
Modes	ROUTER-BGP
Usage	By default, the BGP algorithm selects the best path to a destination when given multiple alternative paths, using the prefix and path information stored in the BGP routing table. You can reconfigure the default settings that determine the best-path selection. Use this command to select a best path that is based on AS paths in the confederation.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# bestpath as-path confed</pre> <pre>sonic(config-router-bgp)# no bestpath as-path confed</pre>
Releases	3.0 or later

bestpath as-path ignore

Instructs BGP to ignore the as-path comparison during best-path calculations.

Command	<code>bestpath as-path ignore</code>
Options	None
Modes	ROUTER-BGP
Usage	The default is to use the AS path in best-path calculation. This command ignores the AS path length in best-path calculation.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# bestpath as-path ignore</pre> <pre>sonic(config-router-bgp)# no bestpath as-path ignore</pre>
Releases	3.0 or later

bestpath as-path multipath-relax

Specifies that BGP decision process should consider paths of equal AS_PATH length candidates for multipath computation.

Command	bestpath as-path multipath-relax [as-set]
Options	as-set — (Optional) Generates AS set-path information
Modes	ROUTER-BGP
Usage	Use this command to ignore as-path check for paths for the same prefix, making all the paths equal irrespective of their as-path. This command permits paths of equal length to be selected to allow for load sharing. The default is to select a best path that is an exact match from multiple alternative paths.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# bestpath as-path multipath-relax</pre> <pre>sonic(config-router-bgp)# no bestpath as-path multipath-relax</pre>
Releases	3.0 or later

bestpath compare-routerid

Influences best-path selection algorithm by comparing router-IDs for identical eBGP routes.

Command	bestpath compare-routerid
Options	None
Modes	ROUTER-BGP
Usage	Use this command to ensure that when comparing routes where both are equal on most metrics, including local-pref, AS_PATH length, IGP cost, and MED that the tie is broken based on the router-ID. If this option is enabled, the already-selected check where already selected eBGP routes are preferred is skipped. If a route has an ORIGINATOR_ID attribute because it has been reflected, that ORIGINATOR_ID is used. The router-ID of the peer the route was received from will otherwise be used. The advantage is that the route-selection (at this point) is more deterministic. The disadvantage is that a few or even one lowest-ID router may attract all traffic to otherwise-equal paths because of this check. It may increase the possibility of MED or IGP oscillation, unless other measures were taken to avoid these. The exact behavior will be sensitive to the iBGP and reflection topology.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# bestpath compare-routerid</pre> <pre>sonic(config-router-bgp)# no bestpath compare-routerid</pre>
Releases	3.0 or later

bestpath med

Changes the best-path MED attributes during MED comparison for path selection.

Command	bestpath med {{missing-as-worst [confed]} {confed [missing-as-worst]}}}
Options	<ul style="list-style-type: none">• confed — Compare MED among BGP confederation paths• missing-as-worst — Treat missing MED as the least preferred method
Modes	ROUTER-BGP
Usage	This command uses the multiexit discriminator (MED) value to select the best path learned from confederation peers if no external AS is in the path or assigns an infinite MED value to routes that

are missing the MED attribute, causing them to be the worst path alternative. The default is to assign 0 to routes with a missing MED value so that they are considered as the best alternative route.

Examples

```
sonic(config) # router bgp 65300
sonic(config-router-bgp) # bestpath med missing-as-worst confed

sonic(config-router-bgp) # no bestpath med missing-as-worst confed
```

Releases

3.0 or later

bfd

Enables bidirectional forwarding detection (BFD) liveliness check for BGP neighbors, and neighbors in a peer-group.

Command

```
bfd [[check-control-plane-failure] | [profile profile-name]]
```

Options

- *check-control-plane-failure*—(Optional) Links the data plane status to the BGP control plane
- *profile profile-name*—(Optional) Enable BFD profile

Modes

- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage

Use this command to enable BFD to detect forwarding-path failures in BGP routes. This command reduces BGP convergence time if there is a link failure.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 30.30.30.3
sonic(config-router-bgp-neighbor) # bfd

sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # bfd

sonic(config-router-bgp-neighbor) # no bfd
sonic(config-router-bgp-pg) # no bfd
```

Releases

3.0 or later

bgp as-path-list

Creates a BGP AS path list.

Command

```
bgp as-path-list AS-path-list-name [seq seq-num] {deny regx-id} | {permit regx-id}
```

Options

- *AS-path-list-name* — Enter a text string for a BGP AS path filter list.
- *seq seq-num* — (Optional) Enter a sequence number that specifies the order in which the permit/deny filter is applied to AS paths in route advertisements (1 to 4294967295) — supported in Release 4.1.0 and later. You cannot enter both sequenced and non-sequenced entries in the same AS path list.
- *regx_id* — Enter a regular expression in the format AA:NN to match an autonomous system path.

(i) NOTE: You cannot configure the same AS path list name twice — once with numbered entries and once with unnumbered (non-sequenced) entries. You can configure an AS path list with either all numbered or all unnumbered entries. In an AS path list with non-sequenced entries, you cannot enter both permit and deny filters. In an AS path list with sequenced entries, you can enter both permit and deny filters.

Modes

CONFIGURATION

Usage

Use this command to create a BGP AS path list. Enter a regular expression that is used to filter routes by matching the AS path in a route as an ASCII string. You can apply the BGP AS path list to a BGP neighbor address family or a BGP peer-group address family using the `filter-list as-path-list {in | out}` command.

Examples

```
sonic(config)# bgp as-path-list asp_private permit ^65000.*6510565109$  
  
sonic(config)# bgp as-path-list asp_private deny 65107.*65200  
  
sonic(config)# no bgp as-path-list asp_private permit ^65000.*6510565109$  
  
sonic(config)# bgp as-path-list asp_private2 seq 121 permit ^62.*65121$  
sonic(config)# bgp as-path-list asp_private2 seq 7371 deny ^67.*657371$  
  
sonic(config)# no bgp as-path-list asp_private2 seq 7371 deny  
^67.*657371$  
  
sonic(config)# no bgp as-path-list asp_private2
```

Releases

3.1 or later

bgp community-list

Creates a standard BGP community-list.

Command

```
bgp community-list {{standard {community-list-name {deny | permit} {{aann  
[local-as] [no-advertise] [no-export] [no-peer] {[any] | [all]}}} | {local-  
as [aann] [no-advertise] [no-export] [no-peer] {[any] | [all]}}} | {no-  
advertise [aann] [local-as] [no-export] [no-peer] {[any] | [all]}}} | {no-  
export [aann] [local-as] [no-advertise] [no-peer] {[any] | [all]}}} | {no-  
peer [aann] [local-as] [no-advertise] [no-export] {[any] | [all]}}}}} |  
{expanded {community-list-name {deny | permit} {line {[any] | [all]}}}}}}
```

Options

- `community_list_name` — Name of the community list used to identify one or more groups of communities
- `aa:nn` — Community number in `aa:nn` format, where `aa` is the number that identifies the autonomous system and `nn` is a number that identifies the community within the autonomous system
- `local-as` — BGP does not advertise this route to external peers
- `no-advertise` — BGP does not advertise this route to any internal or external peers
- `no-export` — BGP does not advertise this route outside a BGP confederation boundary
- `no-peer` — BGP does not advertise this route outside a BGP peer group
- `any` — BGP does not advertise any routes that do not match the filter
- `all` — BGP does not advertise all routes that do not match the filter
- `community_expanded_list_name` — Name of the expanded community list
- `deny` — Sets the BGP community-list default as deny
- `permit` — Sets the BGP community-list default as permit
- `line` — Expanded community-list line which matches any or all routes

Modes

CONFIGURATION

Usage

This command provides options to create expanded or standard community, and accepts community in AA:NN, IP:NN, and well-known communities format. This command also provides any and all constructs to enable you to design community filters with clause match any or all. For expanded community, specify a regular expression of communities.

Examples

```
sonic(config)# bgp community-list standard CommList_RT 100:200  
sonic(config)# bgp community-list standard CommList_RT no-export  
sonic(config)# bgp community-list standard CommList_RT no-peer  
sonic(config)# bgp community-list standard CommList_RT 65100:3456  
sonic(config)# no bgp community-list standard CommList_RT 65100:3456
```

Releases

3.2 or later

bgp extcommunity-list

Creates BGP extended-community list entries.

Command

```
bgp extcommunity-list {{standard {extcommunity-list-name {deny | permit} {{rt {aa | ipaddrnn} {[any] | [all]} } | {soo {aa | ipaddrnn} {[any] | [all]} }}} | {expanded {extcommunity-list-name {deny | permit} {line {[any] | [all]} }}}}}
```

Options

- `standard extcommunity_list_name` — Name of the extended-community list used to identify one or more groups of communities
- `rt aa` — Target route to match against in AA:NN format
- `any` — BGP does not advertise any routes that do not match the filter
- `all` — BGP does not advertise all routes that do not match the filter
- `soo aa` — Route origin to match against in AA:NN format
- `ipaddrnn` — IP address to match against in :NN format
- `expanded extcommunity_list_name` — Name of extended community-list
- `deny` — Sets the BGP extended community-list default to deny
- `permit` — Sets the BGP extended community-list default to permit
- `line` — Expanded community-list line which matches any or all routes

Modes

CONFIGURATION

Usage

Use this command to create BGP extended community list entries. The command provides options to create expanded or standard extended community list entries. For standard extended community, you can create `rt` or `soo` type of communities, and command will accept communities in AA:NN or IP:NN formats. For expanded extended community, the command accepts a regular expression of communities, which is flexible and powerful for matching communities in routes. This command also provides option for matching all or any extended communities.

Examples

```
sonic(config)# bgp extcommunity-list standard ExtComm_AllowInt rt 19.32.56.167:65011 all  
sonic(config)# bgp extcommunity-list standard ExtComm_AllowInt rt 31.67.182.214:3001 all  
sonic(config)# bgp extcommunity-list standard ExtComm_AllowInt soo 4001:65010 all  
sonic(config)# bgp extcommunity-list standard ExtComm_AllowInt soo 98.13.175.21:65101 all  
sonic(config)# no bgp extcommunity-list standard ExtComm_AllowInt soo 98.13.175.21:65101 all
```

Releases

3.2 or later

binding

Creates a binding between an ACL and NAT pool.

Command	<code>binding <i>binding_name</i> <i>pool_name</i> [<i>acl_name</i>] [<i>natType</i>] [<i>twice-nat-id</i>] <i>twice_nat_id_value</i></code>
Options	<ul style="list-style-type: none">• <i>binding_name</i> — Binding name• <i>pool_name</i> — Pool name• <i>acl_name</i> — (Optional) ACL table name (up to 63 characters)• <i>natType</i> — (Optional) NAT type; snat or dnat (default)• <i>twice_nat_id_value</i> — (Optional) Twice NAT ID value
Modes	NAT
Usage	<p>Use this command to create a binding between an ACL and NAT pool. You can use access-control list (ACL) to determine the IP addresses in a global NAT address pool. By default, if you specify an ACL, traffic for all IP hosts are allowed. A permit statement allows an IP address, where a deny statement denies the address. NAT types are snat which translates a source IP address to a global IP address in the pool, and dnat which translates a destination IP address to a global IP address in the pool. twice-nat-id-value performs address translation on both source and destination IP addresses using the address pool for static entries which have the same ID value.</p>
Examples	<pre>sonic(config) # nat sonic(config-nat)# binding Bind2 Pool2 12_ACL_IPV4 snat twice-nat-id 25 sonic(config-nat)# no binding Bind2</pre>
Releases	3.0 or later

buffer default-lossless-buffer-profile

Enables the default lossless buffer profile for RoCEv2-managed traffic on an interface.

Command	<code>buffer default-lossless-buffer-profile</code>
Options	None
Modes	INTERFACE
Usage	<p>Instead of configuring user-defined values for the ingress and egress lossless buffer profiles used for RoCEv2 traffic, you can enable the default lossless buffer settings. To view the default lossless profile settings, use the <code>show buffer profile</code> command. By default, enabling the RoCEv2 defaults (<code>roce enable</code>) enables the default buffer profiles on priority groups based on speed and cable length. Use the <code>no buffer default-lossless-buffer-profile</code> command to avoid overriding user-configured profiles with the default buffer profiles when there are changes in speed or cable length.</p>
Examples	<pre>sonic(config) # interface Ethernet0 sonic(config-if-Ethernet0)# buffer default-lossless-buffer-profile</pre>
Releases	4.1.0 or later

buffer init lossless

Installs platform-specific default configurations for lossless buffer profiles, including ingress and egress buffer pool sizes, priority groups, and queues.

Command	<code>buffer init lossless</code>
Options	None

Modes	CONFIGURATION
Usage	The <code>buffer init lossless</code> and <code>roce enable</code> commands are mutually exclusive. Use the <code>buffer init lossless</code> command to enable pre-configured switch-specific QoS buffer settings independent of RoCEv2 operation.
Examples	<pre>sonic(config)# buffer init lossless This command will also restart the node after saving all configurations. [Proceed y/N]:</pre> <pre>sonic(config)# no buffer init</pre>
Releases	4.1.0 or later

buffer pool

Configures the shared headroom (pool xoff) size for the ingress lossless pool for RoCEv2 data transmission.	
Command	<code>buffer pool ingress_lossless_pool shared-headroom-size <i>headroom-size</i></code>
Options	<i>headroom-size</i> — Enter the shared headroom size in bytes; the minimum and maximum bytes are platform-dependent.
Modes	CONFIGURATION
Usage	If the default headroom buffer size (pool xoff) is not sufficient, reconfigure the shared buffer size for the lossless ingress pool. All other buffer pool configurations are not user-configurable. To view the preset default buffer pool and profile configurations, use the <code>show running-configuration</code> command.
Examples	<pre>sonic(config)# buffer pool ingress_lossless_pool shared-headroom-size 100000</pre>
Releases	4.1.0 or later

buffer priority-group

Associates one or more ingress PFC priority groups with a lossless buffer profile on a RoCEv2 interface.	
Command	<code>buffer queue pg-value-range lossless-buffer-profile-name</code>
Options	<ul style="list-style-type: none"> • <i>pg-value-range</i> — Separate individual priorities and a priority range with a comma; for example, 1-3, 7. • <i>lossless-profile-name</i> — Enter a lossless buffer profile name (up to 63 characters)
Modes	INTERFACE
Usage	Only priority groups 3 and 4 are supported. Configure lossless buffer profiles using the <code>buffer profile</code> command. To disassociate a PFC priority group with a buffer profile, enter the <code>no buffer priority-group pg-value-range</code> command in Interface configuration mode.
Examples	<pre>sonic(config)# interface Eth1/1 sonic(config-if-Ethernet0)# buffer priority-group 3-4 profile_1</pre>
Releases	4.1.0 or later

buffer profile

Configures a lossless buffer profile for RoCEv2 transmission and associate it with the lossless ingress or egress buffer pool.

Command	<pre>buffer profile <i>buffer-pool-name</i> reserved-buffer-size-in-bytes {{dynamic-threshold static-threshold} <i>signed-integer-value</i>} {pause-threshold <i>bytes</i>} {resume-threshold <i>bytes</i>} {resume-offset-threshold <i>bytes</i>}</pre>
Options	<ul style="list-style-type: none">• <i>buffer-pool-name</i>—The valid buffer pool names are: <code>ingress_lossless_pool</code>, <code>egress_lossless_pool</code>, and <code>egress_lossy_pool</code>.• <i>reserved-buffer-size-in-bytes</i>—Enter the reserved buffer size in bytes reserved from the buffer pool (0 to 9216; no default).• <i>dynamic-threshold signed-integer-value</i>—Enter the dynamic size of the buffer threshold by specifying the number of low order bits that can contain data in queued packets. The valid values are -6, -5, -4, -3, -2, -1, 0, 1, 2, and 3; there is no default.• <i>static-threshold size-in-bytes</i>—Enter the fixed, static size in bytes of the maximum threshold used to buffer packets (0 to the maximum NPU buffer size; no default). This is not a reserved buffer.• <i>pause-threshold bytes</i>—(Mandatory for a buffer profile that creates ingress lossless pools; not required for a buffer profile with egress lossless and lossy pools) Enter the number of bytes for the maximum size of the shared headroom buffer used from the ingress pool (1 to the maximum platform-specific ingress pool shared headroom size; no default). An available buffer for a priority group that is less than the specified size triggers the sending of pause frames and is equal to the Xoff or headroom value.• <i>resume-threshold bytes</i>—(Mandatory for a buffer profile that creates ingress lossless pools; not required for a buffer profile egress lossless and lossy pools) Enter the number of bytes for the threshold that is used to resume packet transmission (1 to 18432 bytes; no default).• <i>resume-offset-threshold bytes [xon]</i>—(Mandatory for a buffer profile that creates ingress lossless pools; not required for egress lossless and lossy pools) Enter the number of bytes for the offset value that is used to resume packet transmission (1 to 18432 bytes; no default). Enter <code>xon</code> to send a notification to a sending device to indicate that the switch is now ready to accept data.
Modes	CONFIGURATION
Usage	A lossless buffer profile specifies the guaranteed (reserved) memory for queues or PFC priority groups, static or dynamic thresholds, and optional pause and resume thresholds. To delete a lossless buffer profile, enter the <code>no buffer profile <i>name</i></code> command.
Examples	<pre>sonic(config)# buffer profile profile_2 egress_lossy_pool 20000 dynamic-threshold -2 sonic(config)# buffer profile profile_3 ingress_lossless_pool 30000 pause pause-threshold 3000 resume-threshold 2000 resume-offset-threshold 200</pre>
Releases	4.1.0 or later

buffer queue

Associates an egress queue with a lossless buffer profile on a RoCEv2 interface.

Command	<pre>buffer queue <i>queue-range</i> <i>profile-name</i></pre>
Options	<ul style="list-style-type: none">• <i>queue-range</i> — Separate individual priorities and a priority range with a comma; for example, <code>1-2,7</code>.• <i>lossless-profile-name</i> — Enter a lossless buffer profile name (up to 63 characters)
Modes	INTERFACE
Usage	Queues 3 and 4 are not supported with a user-defined profile. To disassociate an egress queue with a lossless buffer profile, enter the <code>no buffer queue <i>queue-range</i></code> command in Interface configuration mode.

Examples

```
sonic(config) # interface Ethernet0
sonic(config-if-Ethernet0) # buffer queue 0-2 profile_2
```

Releases

4.1.0 or later

C commands

Topics:

- call
- capability dynamic
- capability extended-nexthop
- capability orf prefix-list
- channel-group
- cir
- class
- class-map
- classifier
- clear ars nhg-statistics
- clear audit-log
- clear authentication history interface
- clear authentication sessions
- clear bfd peer
- clear bgp all
- clear bgp ipv4
- clear bgp ipv6
- clear bgp l2vpn evpn
- clear buffer-pool
- clear core-files
- clear counters interface
- clear counters service-policy
- clear counters service-policy interface
- clear counters service-policy policy-map
- clear counters tam
- clear counters vxlan
- clear device
- clear error-database
- clear evpn dup-addr
- clear ip access-list counters
- clear ip arp
- clear ip arp interface
- clear ip dhcp snooping binding
- clear ip dhcp snooping statistics
- clear ip dhcp-relay
- clear ip helper-address statistics
- clear ip igmp interfaces
- clear ip igmp vrf
- clear ip mroute
- clear ip ospf
- clear ip pim
- clear ip sla
- clear ip sla all
- clear ipv6 access-list counters
- clear ipv6 dhcp snooping binding
- clear ipv6 dhcp snooping statistics
- clear ipv6 dhcp-relay

- clear ipv6 nd
- clear ipv6 neighbors
- clear ipv6 neighbors interface
- clear logging
- clear mac access-list counters
- clear mac address-table dynamic
- clear mac dampening-disabled-ports
- clear nat
- clear poe counters
- clear priority-group
- clear queue
- clear radius-server dynamic-author statistics
- clear radius-server statistics
- clear snmp counters
- clear spanning-tree counters
- clear threshold breach
- client
- client-to-client reflection
- clock timezone
- cluster-id
- coalesce-time
- collector
- compatible
- confederation
- configure terminal
- consistency-check start access-list
- consistency-check start route
- consistency-check stop
- copp-action
- copy
- core enable
- counter
- counters
- counters rif interval
- crm
- crm polling-interval
- crm threshold
- crm threshold type
- crypto ca-cert delete
- crypto ca-cert install
- crypto ca-cert verify expiry
- crypto cert delete
- crypto cert generate request
- crypto cert install cert-file key-file
- crypto cert verify expiry
- crypto fips enable
- crypto security-profile
- crypto security-profile certificate
- crypto security-profile trust-store
- crypto ssh-keygen
- crypto trust-store
- crypto trust-store ca-cert

call

Calls to another route-map after match_set.

Command	<code>call <i>match-call</i></code>
Options	<code><i>match-call</i></code> — Route-map name
Modes	ROUTE-MAP
Usage	Calls to another route-map after set actions. Set actions in called route-map get added to the routes. If that route-map returns a deny, route-map processing finishes and the route is denied.
Examples	<pre>sonic(config-route-map)# call match-call rmap1</pre> <pre>sonic(config-route-map)# no call</pre>
Releases	3.0 or later

capability dynamic

Allows BGP to advertise dynamically to a neighbor, or neighbors in a peer-group.

Command	<code>capability dynamic</code>
Options	None
Modes	<ul style="list-style-type: none">• BGP-NEIGHBOR• BGP-PEER-GROUP
Usage	Use this command enable dynamic BGP peering to exchange route information with remote neighbors or neighbors in a peer-group.
Examples	<pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# neighbor 30.30.30.3 sonic(config-router-bgp-neighbor)# capability dynamic</pre> <pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# peer-group PG_Ext sonic(config-router-bgp-pg)# capability dynamic</pre> <pre>sonic(config-router-bgp-neighbor)# no capability dynamic sonic(config-router-bgp-pg)# no capability dynamic</pre>
Releases	3.0 or later

capability extended-nexthop

Enables BGP to negotiate the extended next-hop capability with its peer, or peers in a peer-group.

Command	<code>capability extended-nexthop</code>
Options	None
Modes	<ul style="list-style-type: none">• BGP-NEIGHBOR• BGP-PEER-GROUP
Usage	This command is automatically enabled for IPv6 link-layer addressing. If you are peering over a IPv6 global address, this command allows BGP to install IPv4 routes with IPv6 next-hops if you do not have IPv4 configured on interfaces.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# capability extended-nexthop
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# capability extended-nexthop
```

```
sonic(config-router-bgp-neighbor)# no capability extended-nexthop
sonic(config-router-bgp-pg)# no capability extended-nexthop
```

Releases

3.0 or later

capability orf prefix-list

Enables BGP to advertise outbound route filtering (ORF) to a neighbor, or neighbors in a peer-group.

Command

```
capability orf prefix-list {send | receive | both}
```

Options

- **send** — Send advertisement packets to neighbor
- **receive** — Receive advertisement packets from neighbor
- **both** — Send and receive advertisement packets

Modes

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY

Usage

This command can be enabled in inbound and outbound direction separately.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 20.20.20.2
sonic(config-router-bgp-neighbor)# remote-as 300
sonic(config-router-bgp-neighbor)# address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af)# capability orf prefix-list send
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# address-family ipv4 unicast
sonic(config-router-bgp-pg-af)# capability orf prefix-list send
```

```
sonic(config-router-bgp-neighbor-af)# no capability orf prefix-list send
sonic(config-router-bgp-pg-af)# no capability orf prefix-list send
```

Releases

3.2 or later

channel-group

Assigns and configures a physical interface to a PortChannel group.

Command

```
channel-group lag-id
```

Options

lag-id— Enter a PortChannel number (1 to 128)

Modes

- INTERFACE
- INTERFACE RANGE

Usage

Use the `channel-group` command to assign members to a port-channel group. Configure these attributes on an individual member port. The member ports in a port channel must have the same setting for link speed and duplex capability. When you delete the last physical interface from a port channel, the port channel still remains in the system. The `no` version of this command removes an interface from the port-channel group.

Examples

```
sonic(config)#
sonic(config)# interface PortChannel 101
sonic(config-if-po101)# exit
sonic(config)# interface Eth 1/1
sonic(config-if-Eth1/1)# channel-group 101
sonic(config-if-Eth1/1)# end

sonic(config-if-Eth1/1)# no channel-group
```

Releases

3.0 or later

cir

Configures the committed information rate (CIR).

Command

`cir value`

Options

`value` — CIR in kbps

Modes

SCHEDULER POLICY QUEUE

Usage

Configure the committed information rate in kilobytes per second (Kb/s) for the amount of traffic sent in one particular queue.

Example

```
sonic(config)# qos scheduler-policy s
sonic(config-sched-policy-s)# queue 0
sonic(config-scheduler-s-queue-0)# cir 10

sonic(config-scheduler-s-queue-0)# no cir
```

Releases

3.1 or later

class

Configures the flow match criteria and its actions.

Command

`class fbs-class-name [priority fbs-flow-priority]`

Options

- `fbs-class-name`—FBS class name (up to 63 characters)
- `fbs-flow-priority`—FBS flow priority (0 to 4095)

Modes

POLICY MAP

Usage

Class names must begin with A-Z, a-z, or 0 through 9. You can use underscore (_) and hyphens (-) except as the first character.

Examples

```
sonic(config)# policy-map map1 type forwarding
sonic(config-policy-map)# class qos1 priority 100
```

Releases

4.0 or later

class-map

Configures a class-map.

Command

`class-map fbs-class-name match-type {acl | {fields match-all} | copp}`

Options

- `fbs-class-name`—Class-map name (up to 63 characters)

- `match-type`—Match the class-map to a specific type
- `acl`—Match to ACL
- `fields match-all`—Match to all fields
- `copp`—Match to CoPP

Modes CONFIGURATION

Usage Class-map names must begin with A-Z, a-z, or 0 through 9. You can use underscore (_) and hyphen (-) except as the first character.

Examples

```
sonic(config)# class-map map1 match-type acl

sonic(config)# no class-map map1
```

Releases 3.1 or later

classifier

Configures CoPP classifiers.

Command `classifier name match-type copp`

Options `name` — String (1 to 63)

Modes CONFIGURATION

Usage The name string must begin with an alpha numeric character. Rest of the characters can be alpha numeric or hyphen (-) or underscore (_).

Examples

```
sonic# configure terminal
sonic(config)# classifier copp-system-arp match-type copp
```

Releases 4.0 or later

clear ars nhg-statistics

Clears the ARS NHG statistics.

Command `clear ars nhg-statistics [nexthop-group-id]`

Options • `nexthop-group-id`—Enter the next-hop group ID of the routes.

Modes EXEC

Usage Use this command to clear the NHG statistics. Use the `show ars nhg-statistics` to view the statistics.

Example

```
sonic# clear ars nhg-statistics
Clear all NHG statistics [confirm y/N]: y
sonic#
```

Releases 4.4.0 or later

clear audit-log

Clears the audit log.

Command `clear audit-log`

Options None

Command mode	EXEC
Usage	Use this command to clear all entries in the audit log. Only the user with the admin role can clear the audit log.
Example	<pre>sonic# clear audit-log</pre>
Releases	3.1 or later

clear authentication history interface

Clears authentication history of an interface or all interfaces.

Command	<code>clear authentication history interface {all Eth slot/port}</code>
Options	<ul style="list-style-type: none"> • <code>all</code> — Clear authentication sessions on all interfaces. • <code>Eth slot/port</code> — Clear authentication sessions on an interface.
Modes	EXEC
Usage	Use this command to clear the authentication history log for an interface or all interfaces.
Examples	<pre>sonic# clear authentication history interface all</pre>
Releases	4.0 or later

clear authentication sessions

Clears authentication sessions of an interface or all interfaces.

Command	<code>clear authentication sessions {interface { all Ethernet port} mac mac-address}</code>
Options	<ul style="list-style-type: none"> • <code>all</code> — Clears authentication sessions of all the interfaces • <code>Ethernet port</code> — Clear authentication sessions of an interface • <code>mac mac-address</code> — Clears authentication sessions of a MAC address.
Modes	EXEC
Usage	All the authenticated clients are re-initialized and forced to authenticate again.
Examples	<pre>sonic# clear authentication sessions interface all sonic# clear authentication sessions mac xx:xx:xx:xx:xx:xx</pre>
Releases	4.0 or later

clear bfd peer

Clears counters of a specific bidirectional forwarding detection (BFD) peer with filters.

Command	<code>clear bfd peer {peer_ipv4 peer_ipv6} [vrf vrfname] [multihop] [local-address {local_ipv4 local_ipv6}] [interface interfacename] counters</code>
Options	<ul style="list-style-type: none"> • <code>peer_ipv4</code> — Peer IPv4 address in A.B.C.D format • <code>peer_ipv6</code> — Peer IPv6 address in A::B format • <code>vrfname</code> — (Optional) Name of the VRF • <code>local_ipv4</code> — (Optional) Local IPv4 address in A.B.C.D format • <code>local_ipv6</code> — (Optional) Local IPv6 address in A::B format

- *interfacename* — (Optional) Name of the interface (up to 63 characters)

Modes

EXEC

Usage

BFD packets are reset to zero.

Example

```
sonic# clear bfd peer 192.168.2.1 interface Ethernet0 counters
```

Releases

3.2 or later

clear bgp all

Clears or resets all BGP information including neighbors, peer-groups, and so on.

Command

```
clear bgp all [vrf vrf-name] {{{* {[in] | [out]} | {[soft {[in] | [out]}]} | {[as-num-dot {[in] | [out]} | {[soft {[in] | [out]}]}]} | {[ipv4 {[in] | [out]} | {[soft {[in] | [out]}]}]} | {[ipv6 {[in] | [out]} | {[soft {[in] | [out]}]}]} | {[dampening {[ip-addr] | [ip-prefix]}]} | {[external {[in] | [out]} | {[soft {[in] | [out]}]}]} | {[interface {Ethernet | PortChannel | Vlan}} | {peer-group peer-group-name {[in] | [out]} | {[soft {[in] | [out]}]}]}}}
```

Options

- *vrf-name* — (Optional) VRF name prefixed by Vrf
- *as-num-dot* — (Optional) ASN number (1 to 4294967295)
- *ipv4* — (Optional) IPv4 address in A.B.C.D format
- *ipv6* — (Optional) IPv6 address in A::B format
- *ip-addr* — (Optional) IP address in A.B.C.D format
- *ip-prefix* — (Optional) IP prefix in A.B.C.D/mask format
- *peer-group-name* — Peer group name

Command mode

EXEC

Usage

Use this command to clear BGP information. This is a partial list of information with command syntax that can be cleared:

- `clear bgp all *` — Clears all BGP neighbors in the all address families activated
- `clear bgp all A.B.C.D/A::B` — Clears peers with address of peer_ip and this address-family activated
- `clear bgp all A.B.C.D/A::B soft {in | out}` — Sends route-refresh request unless using soft-reconfiguration inbound for option in; resends all outbound updates for option out

Example

```
sonic# clear bgp all 14.14.14.1
```

Releases

3.1 or later

clear bgp ipv4

Clears or resets BGP information.

Command

```
clear bgp ipv4 unicast [vrf vrf-name] {* | as-num-dot | external | ip4-addr | ip6-addr | ip-prefix | {interface {Ethernet | PortChannel | Vlan}} | {peer-group [peer-group-name]} | {dampening {[ip-addr] | [ip-prefix]} } | {[in] | [out]} | {[soft {[in] | [out]}]} }}
```

Options

- *vrf-name* — (Optional) VRF name prefixed by Vrf (up to 15 characters)
- *as-num-dot* — (Optional) AS number (1 to 4294967295)
- *ip4-addr* — (Optional) IP address in A.B.C.D format
- *ip6-addr* — (Optional) IP address in A::B format
- *ip-prefix* — (Optional) IP prefix in A.B.C.D/mask format
- *peer-group-name* — (Optional) Peer-group name

- `in` — (Optional) Sends route-refresh request unless using [soft-reconfiguration inbound](#)
- `out` — (Optional) Resends all outbound updates
- `soft` — (Optional) Soft-reconfiguration

Modes

EXEC

Usage

- `clear bgp ipv4 unicast *` — Clears all BGP neighbors with this address-family and sub address-family activated
- `clear bgp ipv4 unicast peer_ip` — Clears peers with address of `peer_ip` and this address-family activated
- `clear bgp ipv4 unicast dampening {address | prefix | in | out | soft}` — Clears damped routes
- `clear bgp ipv4 unicast soft {in | out}` — Sends route-refresh request unless using soft-reconfiguration inbound for option `in`; resends all outbound updates for option `out`

Example

```
sonic# clear bgp ipv4 unicast 14.14.14.1
```

Releases

3.1 or later

clear bgp ipv6

Clears or resets BGP information.

Command

```
clear bgp ipv6 unicast [vrf vrf-name] {* | as-num-dot | external | ipv4-addr | ipv6-addr | ip-prefix | {interface {Ethernet | PortChannel | Vlan}} | {peer-group [peer-group-name]} | {dampening {[ip-addr] | [ip-prefix]}}} {[in] | [out] | {[soft {[in] | [out]}}}}]
```

Options

- `vrf-name` — (Optional) VRF name prefixed by `Vrf` (up to 15 characters)
- `as-num-dot` — (Optional) AS number (1 to 4294967295)
- `ip4-addr` — (Optional) IP address in A.B.C.D format
- `ip6-addr` — (Optional) IP address in A::B format
- `ip-prefix` — (Optional) IP prefix in A::B/mask format
- `peer-group-name` — (Optional) Peer-group name
- `in` — (Optional) Sends route-refresh request unless using [soft-reconfiguration inbound](#)
- `out` — (Optional) Resends all outbound updates
- `soft` — (Optional) Soft-reconfiguration

Modes

EXEC

Usage

- `clear bgp {ipv6} unicast *` — Clears all BGP neighbors with this address-family and sub address-family activated
- `clear bgp {ipv6} unicast peer_ip` — Clears peers with address of `peer_ip` and this address-family activated
- `clear bgp ipv6 unicast dampening {address | prefix | in | out | soft}` — Clears damped routes
- `clear bgp {ipv6} unicast soft {in | out}` — Sends route-refresh request unless using soft-reconfiguration inbound for option `in`; resends all outbound updates for option `out`

Example

```
sonic# clear bgp ipv6 unicast
```

Releases

3.1 or later

clear bgp l2vpn evpn

Clears BGP information for EVPN address-family on neighbors.

Command

```
clear bgp l2vpn evpn {{[as-num-dot] {[in] | [out] | {[soft] [in] [out]}}}|[*] {[in] | [out] | {[soft] [in] [out]}}}|{[external] {[in] | [out] | {[soft] [in] [out]}}}|{[interface] {ifname {[in] | [out] | {[soft] [in] [out]}}}}|{[peer-group] {peer-group name {[in] | [out] | {[soft] [in] [out]}}}}|{[neighbor-ipv6] {[in] | [out] | {[soft] [in] [out]}}}|{[neighbor-ipv4] {[in] | [out] | {[soft] [in] [out]}}}|{[in] | [out] | {[soft] [in] [out]}}|{[soft] [in] [out]}|{[*] {[in] | [out] | {[soft] [in] [out]}}}|{[external] {[in] | [out] | {[soft] [in] [out]}}}|{[interface] {ifname {[in] | [out] | {[soft] [in] [out]}}}}|{[peer-group] {peer-group name {[in] | [out] | {[soft] [in] [out]}}}}|{[neighbor-ipv6] {[in] | [out] | {[soft] [in] [out]}}}|{[neighbor-ipv4] {[in] | [out] | {[soft] [in] [out]}}}|{[in] | [out] | {[soft] [in] [out]}}}
```

Options

- *as-num-dot* — (Optional) AS number (1 to 4294967295)
- *ifname* — (Optional) Interface name
- *peer-group name* — (Optional) Peer-group name
- *neighbor-ipv6* — (Optional) IPv6 neighbor address in A::B format
- *neighbor-ipv4* — (Optional) IPv4 neighbor address in A.B.C.D format

Modes

EXEC

Usage

- `clear bgp l2vpn evpn *` — Clears all BGP neighbors with address-family l2vpn evpn activated
- `clear bgp l2vpn evpn {peer_ip} *` — Clear peers with address of peer_ip and address-family l2vpn evpn activated
- `clear bgp l2vpn evpn soft {in | out}` — Sends route-refresh request unless using soft-reconfiguration inbound for option in; resends all outbound updates for option out

Example

```
sonic# clear bgp l2vpn evpn *
```

Releases

3.0 or later

clear buffer-pool

Clears user and persistent watermark counters recorded by the system.

Command

```
clear buffer-pool {watermark | persistent-watermark} [interface if-id {unicast | shared} | multicast | shared]
```

Options

- *watermark*—Clears watermark counters
- *persistent-watermark*—Clears persistent-watermark counters
- *if-id*—Interface name to clear counters for a specific interface
- *multicast*—Multicast buffer type
- *shared*—Shared buffer type

Command mode

EXEC

Usage

- `clear buffer-pool watermark`—Clears the system-recorded watermark counters
- `clear buffer-pool persistent-watermark`—Clears the system-recorded persistent-watermark counters
- `clear buffer-pool interface if-id {unicast | shared}`—Clears counters for a specific interface
- `clear buffer-pool multicast`—Clears the system-recorded multicast buffer type counters
- `clear buffer-pool shared`—Clears the system-recorded shared buffer type counters

Examples

```
sonic# clear buffer-pool watermark  
sonic# clear buffer-pool persistent-watermark
```

Releases

3.1 or later

clear core-files

Clear application core dumps.

Command clear core-files**Options** None**Modes** EXEC**Usage** This command removes all core files and also removes core description from the system. This operation also removes all the information from the system which is not related to core files.**Examples**

```
sonic# clear core-files
```

Releases

4.0 or later

clear counters interface

Clears all interface counters or for a specific interface.

Command clear counters interface {all | Ethernet *if-name* | PortChannel *port-channel-id* | rif}**Options**

- *all*—Clears all interface counters
- *Ethernet if-name*—Clears Physical interface counters
- *PortChannel port-channel-id*—Clears PortChannel interface counters
- *rif*—Clears all route interface counters

Modes EXEC**Usage** Use this command to clear all interface counters. This command is also used to clear counters for a specific Ethernet, PortChannel, or route interface.**Examples**

```
sonic# clear counters interface Ethernet 0  
Clear counters for Ethernet0 [confirm y/N]: y
```

```
sonic# clear counters interface rif
```

Releases

3.1 or later

clear counters service-policy

Clears counters for policies based on the switch, or globally for all policies matching that interface.

Command clear counters service-policy {Switch | CtrlPlane} [type {qos | monitoring | forwarding | copp | acl-copp}]**Options**

- *qos* — (Optional) Clears counters for a QoS service policy
- *monitoring* — (Optional) Clears counters for a monitoring service policy
- *forwarding* — (Optional) Clears counters for a forwarding service policy

- `copp` — (Optional) Clears counters for a CoPP service policy
- `acl-copp` — (Optional) Clears counters for an ACL CoPP service policy

Modes EXEC

Usage Policy-map type argument is optional. If policy-map type not specified it clear fbs policies counters for given interfaces for all policies matching that interface.

Example

```
sonic# clear counters service-policy interface Vlan 100 type qos
```

Releases 3.2 or later

clear counters service-policy interface

Clears counters for service policies applied to an interface.

Command `clear counters service-policy interface {eth-if-id | po-if-id | vlan-if-id | eth-sub-if-id | po-sub-if-id | CPU} [type {qos | monitoring | forwarding | copp | acl-copp}]`

Options

- `eth-if-id` — Ethernet interface ID
- `po-if-id` — PortChannel interface ID
- `vlan-if-id` — Vlan interface ID
- `eth-sub-if-id` — Ethernet subinterface ID
- `qos` — (Optional) Clears counters for a QoS service policy
- `monitoring` — (Optional) Clears counters for a monitoring service policy
- `forwarding` — (Optional) Clears counters for a forwarding service policy
- `copp` — (Optional) Clears counters for a CoPP service policy
- `acl-copp` — (Optional) Clears counters for an ACL CoPP service policy

Modes EXEC

Usage Policy-map type argument is optional. If policy-map type not specified it clear fbs policies counters for given interfaces for all policies matching that interface.

Example

```
sonic(config)# clear counters service-policy interface Vlan 100 type qos
```

Releases 3.2 or later

clear counters service-policy policy-map

Clears flow-based services applied policy counters by policy name.

Command `clear counters service-policy policy-map fbs-policy-name {{{interface {eth-if-id | po-if-id | vlan-if-id | eth-sub-if-id | po-sub-if-id | CPU}} | [Switch] | [CtrlPlane]}}}`

Options

- `fbs_policy_name` — Name of the flow-based service policy
- `eth-if-id` — (Optional) Ethernet interface ID
- `po-if-id` — (Optional) PortChannel interface ID
- `vlan-if-id` — (Optional) VLAN interface ID
- `eth-sub-if-id` — (Optional) Ethernet subinterface ID
- `po-sub-if-id` — (Optional) PortChannel subinterface ID
- `Switch` — (Optional) Clears all counters on the switch

Modes EXEC

Usage Policy-map type argument is optional. If policy-map type not specified it clear fbs policies counters for given interfaces for all policies matching that interface.

Example

```
sonic# clear counters service-policy policy-map policy_vrf interface Vlan 100
```

Releases

3.2 or later

clear counters tam

Clears flow-group counters.

Command `clear counters tam {flow-groups {all | name}}`

- Options**
- `all`—Clears all flow-groups
 - `name`—Flow-group name to clear

Modes EXEC

Usage Use this command to clear the packet count of TAM flow-group counters.

Examples

```
sonic# clear counters tam flow-groups all
```

```
sonic# clear counters tam flow-groups flowgroup10
```

Releases

3.1 or later

clear counters vxlan

Clears VXLAN tunnel counters per remote VTEP or all remote VTEPs.

Command `clear counters vxlan [vtep-ip]`

Options `vtep-ip` — (Optional) Remote VTEP IP address

Modes EXEC

Usage Use this command to clear traffic statistics in all VXLAN tunnels on a VTEP. To clear traffic statistics for a specified VXLAN tunnel, enter the destination IP address.

Examples

```
sonic# clear counters vxlan
```

```
sonic# clear counters vxlan 1.1.1.1
```

Releases

4.0 or later

clear device

Clears device-level watermark counters.

Command `clear device {persistent-watermark | watermark}`

- Options**
- `persistent-watermark`—Clear persistent-watermark counters
 - `watermark`—Clear user watermark counters

Modes EXEC

- Usage**
- `clear device persistent-watermark`—Clears the device-level persistent-watermark counters
 - `clear device watermark`—Clears the device-level watermark counters

Examples

```
sonic# clear device persistent-watermark  
sonic# clear device watermark
```

Releases

4.0 or later

clear error-database

Clears error database table.

Command

```
clear error-database {ALL | ERROR_ROUTE_TABLE | ERROR_NEIGH_TABLE |  
ERROR_IPMC_ROUTE_TABLE}
```

Options

- ALL—Clears all tables
- ERROR_IPMC_ROUTE_TABLE—Clears IPMC route table
- ERROR_NEIGH_TABLE—Clears neighbor table
- ERROR_ROUTE_TABLE—Clear route table

Modes

EXEC

Usage

Use this command to clear all the error in the IPMC, route, and neighbor tables.

Examples

```
sonic# clear error-database ALL  
ALL Table(s) cleared successfully
```

```
sonic# clear error-database ERROR_ROUTE_TABLE  
ERROR_ROUTE_TABLE Table(s) cleared successfully
```

Releases

4.1.0 or later

clear evpn dup-addr

Clears duplicate address.

Command

```
clear evpn dup-addr vni {vni-number [mac mac-addr] | all}
```

Options

- *vni-number*—VNI number (1 to 16777215)
- *mac mac-addr*—MAC address
- *all*—All VNIs

Modes

EXEC

Usage

Use this command to clear the detected duplicate MAC addresses for a specific VNI, All VNIs, or MAC address.

- `clear evpn dup-addr vni vni-number`—Clears the detected duplicate MAC addresses for a specific VNI
- `clear evpn dup-addr vni vni-number mac mac-addr`—Clears the detected duplicate MAC addresses for a MAC address
- `clear evpn dup-addr vni all`—Clears the detected duplicate MAC addresses for all VNIs

Examples

```
sonic# clear evpn dup-addr vni all  
sonic# clear evpn dup-addr vni 1 mac 00:e0:ec:20:12:62
```

Releases

4.0 or later

clear ip access-list counters

Clears IPv4 ACL counters.

Command	<code>clear ip access-list counters [access-list-name {[interface {Ethernet PortChannel Vlan eth-sub-if-id po-sub-if-id}] [Switch]}}]</code>
Options	<ul style="list-style-type: none">• <i>access-list_name</i> — (Optional) ACL name (up to 63 characters)• <i>PortChannel</i> — (Optional) PortChannel ID (1 to 128)• <i>Vlan</i> — (Optional) VLAN ID (1 to 4094)• <i>eth-sub-if-id</i> — (Optional) Ethernet subinterface ID• <i>po-sub-if-id</i> — (Optional) PortChannel subinterface ID• <i>Switch</i> — (Optional) Clears all ACLs on the switch
Modes	EXEC
Usage	ACL name and interface names are optional. If ACL name is not specified then all IPv4 ACLs statistics will be cleared.
Example	<pre>sonic# clear ip access-list counters ipacl-example</pre>
Releases	3.2 or later

clear ip arp

Clears all IPv4 ARP entries.

Command	<code>clear ip arp [ip-addr] [vrf {vrfname mgmt all}]</code>
Options	<ul style="list-style-type: none">• <i>ip-addr</i> — (Optional) IPv4 address of the ARP entry to clear in A.B.C.D format• <i>vrfname</i> — (Optional) VRF name prefixed by Vrf (up to 15 characters)
Modes	EXEC
Usage	Use this command to delete dynamically learned IPv4 entries from the ARP table. Use show ip arp to verify the IPv4 entries have been deleted.
Examples	<pre>sonic# clear ip arp 192.168.1.4 sonic# show ip arp Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP) ----- Address Hardware address Interface Egress Interface Type Action ----- 192.168.2.4 00:01:02:03:ab:cd PortChannel1200 - Dynamic Fwd 192.168.3.6 00:01:02:03:04:05 Vlan100 Eth1/2 Dynamic Fwd 10.11.48.254 00:01:e8:8b:44:71 Management0 - Dynamic Fwd 10.14.8.102 00:01:e8:8b:44:71 Management0 - Dynamic Fwd sonic# clear ip arp interface Vlan 100 sonic# show ip arp Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP) ----- Address Hardware address Interface Egress Interface Type Action ----- 192.168.2.4 00:01:02:03:ab:cd PortChannel1200 - Dynamic Fwd 10.11.48.254 00:01:e8:8b:44:71 Management0 - Dynamic Fwd 10.14.8.102 00:01:e8:8b:44:71 Management0 - Dynamic Fwd</pre>
Releases	3.0 or later

clear ip arp interface

Clears ARP interface entries.

Command `clear ip arp interface {phy-if-name | subif-name | mgmt-if-name | po-if-name | vlan-if-name}`

- Options**
- *phy-if-name* — Ethernet interface ID
 - *subif-name* — Subinterface type
 - *mgmt-if-name* — Management interface ID
 - *po-if-name* — PortChannel interface ID
 - *vlan-if-name* — VLAN interface ID

Modes EXEC

Usage Use this command to delete dynamically learned IPv4 interface entries from the ARP table. To clear sub interface ARP entries, use the *subif-name* and *port.subport* options.

Examples

```
sonic# clear ip arp interface Vlan 100

sonic# show ip arp
-----
Address        Hardware address        Interface        Egress Interface
-----
192.168.1.4    00:01:02:03:44:55    Ethernet8        -
192.168.2.4    00:01:02:03:ab:cd    PortChannel1200   -
10.11.48.254   00:01:e8:8b:44:71    Management0     -
10.14.8.102    00:01:e8:8b:44:71    Management0     -
```

```
sonic# clear ip arp interface Management 0

sonic# show ip arp
-----
Address        Hardware address        Interface        Egress Interface
-----
192.168.1.4    00:01:02:03:44:55    Ethernet8        -
192.168.2.4    00:01:02:03:ab:cd    PortChannel1200   -
10.14.8.102    00:01:e8:8b:44:71    Management0     -
```

Releases 3.2 or later

clear ip dhcp snooping binding

Clears all or a specific DHCPv4 snooping binding entry.

Command `clear ip dhcp snooping binding [ip-address mac-address vlan vlan-id {Ethernet phy-if-name | PortChannel port-channel-id}]`

- Options**
- *ip-address*—(Optional) IP address in A.B.C.D format
 - *mac-address*—(Optional) MAC address in nn:nn:nn:nn:nn:nn format
 - *vlan-id*—(Optional) VLAN ID (1 to 4094)
 - *phy-if-name*—(Optional) Ethernet ID
 - *port-channel-id*—(Optional) PortChannel ID (1 to 256)

Modes EXEC

Usage Use this command to clear all or specific dynamic IP DHCP snooping binding entries.

Examples To clear all DHCPv4 DHCP snooping binding:

```
sonic# clear ip dhcp snooping binding
```

To clear a specific DHCPv4 DHCP snooping binding:

```
sonic# clear ip dhcp snooping binding 1.1.1.1 00:00:5e:00:53:af Vlan 10  
Ethernet 5
```

Releases 4.0 or later

clear ip dhcp snooping statistics

Clears IPv4 DHCP snooping statistics.

Command `clear ip dhcp snooping statistics {detail | Ethernet if-name | PortChannel Port-channel-id}`

Options

- *detail*—Clears IP DHCP Snooping statistics details.
- *if-name*—Enter the Ethernet ID.
- *Port-channel-id*—Enter the PortChannel ID.

Modes EXEC

Usage Use this command to clear the global IP DHCP snooping statistics. Provide the interface name with this command to clear the IP DHCP snooping statistics for an interface.

Examples

```
sonic# clear ip dhcp snooping statistics Ethernet 2
```

```
sonic# clear ip dhcp snooping statistics PortChannel 1
```

```
sonic# clear ip dhcp snooping statistics detail
```

Releases 4.0 or later

clear ip dhcp-relay

Clears IPv4 DHCP relay statistics.

Command `clear ip dhcp-relay {statistics ifName}`

Options *ifName* — (Optional) Clear statistics based on the interface name (up to 32 characters)

Modes EXEC

Usage Use this command to clear the global IP DHCP relay statistics. Enter the `statistics` keyword along with the interface name to clear the IP DHCP relay statistics for a particular interface.

Examples

```
sonic# clear ip dhcp-relay
```

```
sonic# clear ip dhcp-relay statistics Vlan100
```

Releases 3.1 or later

clear ip helper-address statistics

Clears IP helper counters on an interface.

Command `clear ip helper-address statistics [iface]`

Options *iface*—(Optional) Interface type

Modes EXEC

Usage Use this command to clear IP helper statistics on all interfaces or an interface.

Examples

```
sonic# clear ip helper-address statistics
```

```
sonic# clear ip helper-address statistics Ethernet0
```

Releases 3.1 or later

clear ip igmp interfaces

Clears or resets IGMP.

Command clear ip igmp interfaces

Options None

Command mode EXEC

Usage Use this command to clear all IGMP interfaces.

Example

```
sonic# clear ip igmp interfaces
```

Releases 3.2 or later

clear ip igmp vrf

Clears or resets IGMP.

Command clear ip igmp vrf *vrf-name* interfaces

Options *vrf-name* — VRF name prefixed by Vrf

Command mode EXEC

Usage Use this command to clear all IGMP interfaces in a VRF.

Example

```
sonic# clear ip igmp vrf vrf-name interfaces
```

Releases 3.2 or later

clear ip mroute

Clears IP multicast routes.

Command clear ip mroute [*vrf vrf-name*]

Options *vrf-name* — (Optional) VRF name prefixed by Vrf.

Command mode EXEC

Usage Use this command to clear all IP multicast routes, or for a specific VRF.

Examples

```
sonic# clear ip mroute
```

```
sonic# clear ip mroute vrf Vrf1
```

Releases 3.2 or later

clear ip ospf

Clears or resets sessions on an OSPF interface.

Command	<code>clear ip ospf {{interface [interface-name]} {vrf {vrf-name {interface [interface-name]}}}}</code>
Options	<ul style="list-style-type: none">• <i>interface-name</i> — (Optional) Clears all OSPF sessions on a specific interface• <i>vrf-name</i> — VRF name
Modes	EXEC
Usage	<ul style="list-style-type: none">• <code>clear ip ospf interface <i>interface-name</i></code> — Clears all OSPFv2 sessions on an OSPFv2 interface• <code>clear ip ospf vrf <i>vrf-name</i> interface <i>interface-name</i></code> — Clears all OSPFv2 sessions on interface in VRF <i>vrf-name</i>
Examples	<pre>sonic# clear ip ospf interface Ethernet64</pre> <pre>sonic# clear ip ospf vrf default interface Ethernet64</pre>
Releases	3.1 or later

clear ip pim

Clears PIM interfaces.

Command	<code>clear ip pim [vrf <i>vrf-name</i>] {[interfaces] [oil]}</code>
Options	<i>vrf-name</i> — (Optional) VRF name prefixed by Vrf
Command mode	EXEC
Usage	<ul style="list-style-type: none">• <code>clear ip pim [vrf <i>vrf-name</i>] interfaces</code> — Clears all PIM interfaces of a specific VRF• <code>clear ip pim [vrf <i>vrf-name</i>] oil</code> — Clears PIM oil (outgoing interfaces list) of all multicast entries of a specific VRF
Examples	<pre>sonic# clear ip pim interfaces</pre> <pre>sonic# clear ip pim vrf Vrf2 interfaces</pre> <pre>sonic# clear ip pim oil</pre> <pre>sonic# clear ip pim vrf Vrf2 oil</pre>
Releases	3.2 or later

clear ip sla

Clears statistics and history for an IP SLA instance.

Command	<code>clear ip sla <i>id</i></code>
Options	<i>id</i> —IP SLA ID of an instance.
Modes	EXEC
Usage	The range for IP SLA ID is from one to 255.

Examples

```
sonic# clear ip sla 10
```

Releases

3.1 or later

clear ip sla all

Clears statistics and history of all IP SLA instances.

Command `clear ip sla all`**Options** None**Modes** EXEC**Usage** None**Examples**

```
sonic# clear ip sla all
```

Releases

3.1 or later

clear ipv6 access-list counters

Clears IPv6 ACL counters.

Command `clear ipv6 access-list counters [access-list-name {[interface {Ethernet | PortChannel | Vlan | eth-sub-if-id | po-sub-if-id}] | [Switch]}}]`**Options**

- *access-list_name* — (Optional) ACL name (up to 63 characters)
- *PortChannel* — (Optional) PortChannel ID (1 to 128)
- *Vlan* — (Optional) VLAN ID (1 to 4094)
- *eth-sub-if-id* — (Optional) Ethernet subinterface ID
- *po-sub-if-id* — (Optional) PortChannel subinterface ID
- *Switch* — (Optional) Clears all ACLs on the switch

Modes EXEC**Usage**

ACL name and interface names are optional. If ACL name is not specified then all IPv6 ACLs statistics will be cleared.

Example

```
sonic# clear ipv6 access-list counters ipv6acl-example
```

Releases

3.2 or later

clear ipv6 dhcp snooping binding

Clears all or a specific IPv6 DHCP snooping binding entry.

Command `clear ipv6 dhcp snooping binding [ip-address {mac-address {vlan vlan-id {phy-if-name | PortChannel PortChannel-id}}}]`**Options**

- *ip-address*—IP address in A::B format
- *mac-address*—MAC address in nn:nn:nn:nn:nn:nn format
- *vlan-id*—VLAN ID (1 to 4094)
- *phy-if-name*—Ethernet ID
- *PortChannel-id*—PortChannel ID (1 to 256)

Modes

EXEC

Usage	Use this command to clear all or specific dynamic IPv6 DHCP snooping binding entries.
Examples	<p>To clear all DHCPv6 DHCP snooping binding</p> <pre>sonic# clear ipv6 dhcp snooping binding</pre> <p>To clear a specific DHCPv6 DHCP snooping binding</p> <pre>sonic# clear ipv6 dhcp snooping binding 2001:0db8:00:00:5e:00:53:af Vlan 10 Ethernet 5</pre>
Releases	4.0 or later

clear ipv6 dhcp snooping statistics

Clears IPv6 DHCP snooping statistics.	
Command	<code>clear ipv6 dhcp snooping statistics {detail Ethernet <i>if-name</i> PortChannel <i>Port-channel-id</i>}</code>
Options	<ul style="list-style-type: none"> • <i>detail</i>—Clears IP DHCP Snooping statistics details • <i>if-name</i>—Ethernet ID • <i>Port-channel-id</i>—PortChannel ID
Modes	EXEC
Usage	Use this command to clear the global IPv6 DHCP snooping statistics. Provide the interface name with this command to clear the IPv6 DHCP snooping statistics for an interface.
Examples	<pre>sonic# clear ipv6 dhcp snooping statistics Ethernet 2</pre> <pre>sonic# clear ipv6 dhcp snooping statistics PortChannel 1</pre> <pre>sonic# clear ipv6 dhcp snooping statistics detail</pre>
Releases	4.0 or later

clear ipv6 dhcp-relay

Clears IPv6 dhcp-relay statistics.	
Command	<code>clear ipv6 dhcp-relay {statistics <i>interface_name</i>}</code>
Options	<code>statistics <i>interface_name</i></code> — (Optional) Clear statistics based on the interface name (up to 32 characters)
Modes	EXEC
Usage	Use this command to clear the global IPv6 DHCP relay statistics. Enter the <code>statistics</code> keyword along with the interface name to clear the IPv6 DHCP relay statistics for a particular interface.
Examples	<pre>sonic# clear ipv6 dhcp-relay</pre> <pre>sonic# clear ipv6 dhcp-relay statistics Vlan100</pre>
Releases	3.1 or later

clear ipv6 nd

Clears neighbor discovery information.

Command clear ipv6 nd ra-interfaces [[Ethernet port] | [PortChannel ID] | [Vlan vlan-id]]

- Options**
- *port*—(Optional) Physical interface details
 - *ID*—(Optional) PortChannel interface details (1 to 256)
 - *vlan-id*—(Optional) VLAN ID (1 to 4094)

Modes EXEC

Usage Use this command to clear the router advertisement statistics of any interface or all the interfaces.

Examples

```
sonic# clear ipv6 nd ra-interfaces
```

```
sonic# clear ipv6 nd ra-interfaces Vlan 1
```

Releases 4.1.0 or later

clear ipv6 neighbors

Clears entries in the IPv6 neighbor discovery cache, or neighbors of a specific interface.

Command clear ipv6 neighbors [ip-addr] [vrf {vrfname | mgmt | all}]

- Options**
- *ip-addr*—(Optional) IPv6 address of the neighbor in A::B format
 - *vrfname*—(Optional) VRF name prefixed by Vrf (up to 15 characters)

Modes EXEC

Usage To specify the entries to be deleted, enter an interface, port channel, or VLAN, an IPv6 address, or a combination to match. Use [show ipv6 neighbors](#) to verify that the IPv6 entries have been deleted.

Examples

```
sonic# show ipv6 neighbors
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address          Hardware address      Interface     Egress Interface  Type   Action
-----
20::1            00:01:02:03:44:55    Ethernet8      -              Dynamic  Fwd
20::2            00:01:02:03:ab:cd    PortChannel1200 -              Dynamic  Fwd
20::3            00:01:02:03:04:05    Vlan100       Ethernet4      Dynamic  Fwd
fe80::e6f0:4ff:fe79:34c7 00:01:e8:8b:44:71  Management0  -              Dynamic  Fwd
```

```
sonic# clear ipv6 neighbors interface Vlan 100
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address          Hardware address      Interface     Egress Interface  Type   Action
-----
20::1            00:01:02:03:44:55    Ethernet8      -              Dynamic  Fwd
20::2            00:01:02:03:ab:cd    PortChannel1200 -              Dynamic  Fwd
fe80::e6f0:4ff:fe79:34c7 00:01:e8:8b:44:71  Management0  -              Dynamic  Fwd
```

```
sonic# show ipv6 neighbors
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address          Hardware address      Interface     Egress Interface  Type   Action
-----
20::1            00:01:02:03:44:55    Ethernet8      -              Dynamic  Fwd
20::2            00:01:02:03:ab:cd    PortChannel1200 -              Dynamic  Fwd
20::3            00:01:02:03:04:05    Vlan100       Ethernet4      Dynamic  Fwd
fe80::e6f0:4ff:fe79:34c7 00:01:e8:8b:44:71  Management0  -              Dynamic  Fwd
```

```
sonic# clear ipv6 neighbors fe80::e6f0:4ff:fe79:34c7
sonic# show ipv6 neighbors
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address          Hardware address      Interface     Egress Interface  Type   Action
-----
20::1            00:01:02:03:44:55    Ethernet8      -              Dynamic  Fwd
```

20::2	00:01:02:03:ab:cd	PortChannel1200	-	Dynamic	Fwd
20::3	00:01:02:03:04:05	Vlan100	Ethernet4	Dynamic	Fwd

Releases 3.1 or later

clear ipv6 neighbors interface

Clears IPv6 neighbors of a specific interface.

Command `clear ipv6 neighbors interface {phy-if-name | subif-name | mgmt-if-name | po-if-name | vlan-if-name}`

- Options**
- *phy-if-name* — Ethernet interface ID
 - *subif-name* — Subinterface type
 - *mgmt-if-name* — Management interface ID
 - *po-if-name* — PortChannel interface ID
 - *vlan-if-name* — VLAN interface ID

Modes EXEC

Usage Use this command to delete or remove IPv6 neighbors of Ethernet, VLAN, PortChannel, or a Management interface. To specify entries to delete, enter an interface type and interface ID. Use [show ipv6 neighbors](#) to verify the entries have been deleted.

Example

```
sonic# clear ipv6 neighbors 20::2
sonic# show ipv6 neighbors
-----
Address           Hardware address      Interface      Egress Interface
-----
fe80::e6f0:4ff:fe79:34c7  e4:f0:04:79:34:c7  Management0  -
```

Releases 3.2 or later

clear logging

Clears or resets logging information.

Command `clear logging`

Options None

Modes EXEC

Usage Use this command to clear all Syslog messages.

Example

```
sonic# clear logging
```

Releases 3.1 or later

clear mac access-list counters

Clears MAC ACL counters for a specific interface.

Command `clear mac access-list counters [access-list-name {[interface {Ethernet | PortChannel | Vlan | eth-sub-if-id | po-sub-if-id}] | [Switch]}}`

- Options**
- *access-list_name* — (Optional) ACL name (up to 63 characters)
 - *PortChannel* — (Optional) PortChannel ID (1 to 128)
 - *Vlan* — (Optional) VLAN interface ID (1 to 4094)
 - *eth-sub-if-id* — (Optional) Ethernet subinterface ID
 - *po-sub-if-id* — (Optional) PortChannel subinterface ID

Modes	EXEC
Usage	ACL name and interface names are optional. If ACL name is not specified then all MAC ACLs statistics are cleared.
Example	<pre>sonic# clear mac access-list counters</pre>
Releases	3.2 or later

clear mac address-table dynamic

Clears L2 dynamic address entries from the MAC address-table.

Command	<code>clear mac address-table dynamic {all {address <i>mac-addr</i>} {Vlan <i>vlan-id</i>} {interface {Ethernet PortChannel}}}</code>
Options	<ul style="list-style-type: none"> • <i>all</i> — Deletes all MAC address-table entries • <i>mac-addr</i> — Deletes a configured MAC address from the address-table in nn:nn:nn:nn:nn:nn format • <i>vlan-id</i> — Deletes all entries based on the VLAN number from the address-table (1 to 4094)
Modes	EXEC
Usage	Use this command to clear all or specific entries in the MAC address table. Use the <i>all</i> option to remove all dynamic entries from the address-table.
Examples	<pre>sonic# clear mac address-table dynamic all</pre> <pre>sonic# clear mac address-table dynamic Vlan 20</pre>
Releases	3.0 or later

clear mac dampening-disabled-ports

Clears MAC dampening disabled ports.

Command	<code>clear mac dampening-disabled-ports {all <i>Port-id</i> <i>Port-channel-id</i>}</code>
Options	<ul style="list-style-type: none"> • <i>all</i>—Clears all MAC dampening disabled ports • <i>Port-id</i>—Clears ports based on the port ID • <i>Port-channel-id</i>—Clears ports based PortChannel ID (1 to 128)
Modes	EXEC
Usage	Resets the ports that are disabled due to MAC dampening.
Example	<pre>sonic# clear mac dampening-disabled ports all</pre>
Releases	3.1 or later

clear nat

Clears network address translations and statistics.

Command	<code>clear nat {translations statistics}</code>
Options	None
Modes	EXEC
Usage	Use this command to clear the entries in the NAT translation table.

Example

```
sonic# clear nat translations
```

Releases

3.0 or later

clear poe counters

Clears all or one the PoE port counters.

Command `clear poe counters [port]`**Options** `port`—Ethernet port number**Modes** EXEC**Usage** Use this command to clear PoE error counters on a specified port or on all ports.**Examples**

```
sonic# clear poe counters
```

```
sonic# clear poe counters Ethernet0
```

Releases

4.0 or later

clear priority-group

Clears priority-group watermarks, persistent-watermarks, breaches, and so on.

Command `clear priority-group {{watermark {{headroom {[interface {phy-intf-name}]}}} | {shared {[interface {phy-intf-name}]} }}} | {persistent-watermark {{headroom {[interface {phy-intf-name}]}}} | {shared {[interface {phy-intf-name}]} }}}}`**Options** `phy-intf-name`—(Optional) Ethernet interface ID**Modes** EXEC**Usage** Use this command to clear priority-group watermarks, persistent-watermarks, breaches, and so on.**Examples**

```
sonic# clear priority-group watermark shared interface Ethernet 0
```

```
sonic# clear priority-group persistent-watermark headroom
```

Releases

3.1 or later

clear queue

Clears queue counters, watermarks, persistent-watermarks, and breaches for all interfaces or for a specific interface.

Command `clear queue {{[wred-ecn] counters {[interface {{phy-intf-name {[queue queue-id]}}} | {CPU {[queue queue-id]}}}}} | {watermark {{unicast {[interface {phy-intf-name}]}}} | {multicast {[interface {phy-intf-name}]}}} | CPU}} | {persistent-watermark {{unicast {[interface {phy-intf-name}]}}} | {multicast {[interface {phy-intf-name}]}}} | CPU}}`**Options**

- `phy-intf-name` — (Optional) Ethernet interface ID
- `queue_id` — (Optional) Queue ID
- `counters` — Clears all counters on a specified interface queue.
- `wred-ecn counters` — Clears only WRED and ECN counters on all queues of a specified interface.

- `watermark` — Clears queue watermarks for unicast or multicast interfaces.
- `persistent-watermark` — Clears queue persistent-watermarks for unicast or multicast interfaces

Modes

EXEC

Usage

- `clear queue counters (interface Ethernet | CPU [phy-intf-name] (queue [queue-id]))` — Clears all queue counters
- `clear queue (watermark | persistent-watermark) (unicast| multicast) (interface Ethernet | CPU [phy-intf-name])` — Clears all queue watermarks.

Examples

```
sonic# clear queue counters interface Ethernet 0 queue 0
```

```
sonic# clear queue watermark unicast
```

```
sonic# clear queue persistent-watermark multicast interface Ethernet 0
```

```
sonic# clear queue wred-ecn counters interface Eth1/56
```

Releases

3.1 or later

clear radius-server dynamic-author statistics

Clear radius dynamic authorization global counters and per DAS client counters.

Command

```
clear radius-server dynamic-author statistics [client {all | ipv4 | ipv6 | hostname}]
```

Options

- `all` — Clear radius dynamic authorization for all clients.
- `ipv4` — Clear radius dynamic authorization for an IPv4 client.
- `ipv6` — Clear radius dynamic authorization for an IPv6 client.
- `hostname` — Clear radius dynamic authorization for a host.

Modes

EXEC

Usage

Use this command to clear radius dynamic authorization global counters and per DAS client counters.

Examples

```
sonic# clear radius-server dynamic-author statistics
```

Releases

4.1.0 or later

clear radius-server statistics

Clears radius-server statistics.

Command

```
clear radius-server statistics
```

Options

None

Modes

EXEC

Usage

Use this command to clear radius-server statistics.

Example

```
sonic# clear radius-server statistics
```

Releases

3.1 or later

clear snmp counters

Clears global SNMP counter.

Command	clear snmp counters
Options	None
Modes	EXEC
Usage	Use this command to clear global SNMP counter.
Example	<pre>sonic# clear snmp counters</pre>

Releases	3.1 or later
-----------------	--------------

clear spanning-tree counters

Clears spanning-tree counters.

Command	clear spanning-tree counters {interface <i>if-name</i> vlan <i>vlan-id</i> }
Options	<ul style="list-style-type: none">• <i>if-name</i>—Interface name to clear counters for a specific interface• <i>vlan-id</i>—VLAN ID (1 to 4094)
Modes	EXEC
Usage	Use this command to clear the spanning-tree counters. Enter the <i>interface</i> keyword and the interface name or <i>vlan</i> keyword and the VLAN ID to clear the spanning-tree counters for that specific interface or VLAN.
Examples	<pre>sonic# clear spanning-tree counters interface Ethernet 1</pre> <pre>sonic# clear spanning-tree counters vlan 1</pre>
Releases	4.0 or later

clear threshold breach

Clears threshold breaches for all or for a specific breach event.

Command	clear threshold breach {all <i>eventId</i> }
Options	<ul style="list-style-type: none">• <i>all</i> — Clears all threshold breaches.• <i>eventId</i> — Event ID of the threshold breach to clear.
Modes	EXEC
Usage	Use this command to delete the threshold breaches recorded on the switch. To delete a specified breach event, enter the <i>event-id</i> . Use show threshold breaches to view all current system breaches.
Example	<pre>sonic# clear threshold breach all</pre> <pre>sonic# clear threshold breach 100</pre>
Releases	3.1 or later

client

Configures the IP address, IPV6 address, or hostname of the client (Dynamic Authorization Client).

Command `client { ip-address | ipv6-address | hostname } [server-key key-string [encrypted]]`

- Options**
- *ip-address* — Specify the IP address of the client.
 - *ipv6-address* — Specify the IPv6 address of the client.
 - *hostname* — Specify the hostname of the client.
 - *server-key key-string* — Encrypt the key string.

Modes RADIUS-DA

Usage The command uses the optional *server-key* keyword and string argument to configure the server key at the client level. The encrypted keyword is hidden.

Examples

```
sonic(config-radius-da)# client 10.1.2.3
```

Releases 4.1.0 or later

client-to-client reflection

Enables route reflection between clients in a cluster.

Command `client-to-client reflection`

Options None

Modes ROUTER-BGP

Usage Use this command to configure the route-reflector to enable the sharing of route information between members of a peer-group that is configured as a BGP route-reflector client. Route information received from one peer-group member is sent to all other members. You must fully mesh all clients before you disable route-reflection.

Examples

```
sonic(config)# router bgp 65300
sonic(config-router-bgp)# client-to-client reflection
```

```
sonic(config-router-bgp)# no client-to-client reflection
```

Releases 3.0 or later

clock timezone

Configures the user-defined time zone.

Command `clock timezone {timezone-string}`

Options *timezone-string* — Name of the time zone

Modes CONFIGURATION

Usage You can use the ? character or press the tab key for command completion and view a list of supported standard time zones. Define region names with a "/" at the end of the string. The "/" character indicates that a time zone string follows the region name. For example, "Asia/Kolkata."

Examples

```
sonic(config)# clock timezone Asia/Kolkata
```

```
sonic(config)# no clock timezone
```

Releases	4.0 or later
-----------------	--------------

cluster-id

Assigns a cluster ID to a BGP cluster with multiple route-reflectors.

Command	<code>cluster-id <i>intval-ip</i></code>
Options	<code><i>intval-ip</i></code> — IP address in A.B.C.D format (default), or route-reflector cluster ID as a 32-bit number (1 to 4294967295)
Modes	ROUTER-BGP
Usage	Use this command to configure a cluster ID (an IP address or a 32-bit number) on a BGP router. A cluster is a collection of route reflectors and their clients, and is used by route reflectors to avoid looping. If a cluster contains only one route-reflector, the cluster ID is the route-reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster. The default format to display the cluster ID is A.B.C.D format.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# cluster-id 23.79.154.17 sonic(config-router-bgp)# no cluster-id</pre>
Releases	3.0 or later

coalesce-time

Configures the coalesce timer interval.

Command	<code>coalesce-time <i>coaltime</i></code>
Options	<code><i>coaltime</i></code> — Coalesce time in milliseconds (1 to 4294967295)
Modes	ROUTER-BGP
Usage	Coalesce time is the time that BGP delays before deciding what peers are put into an update-group together in order to generate a single update for them.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# coalesce-time 2000 sonic(config-router-bgp)# no coalesce-time</pre>
Releases	4.2.0 or later

collector

Configures the external collector IP address and port.

Command	<code>collector <i>name</i> ip <i>ip_address</i> port <i>port_number</i> [protocol <i>protocol_type</i>] [<i>vrf-name</i>]</code>
Options	<ul style="list-style-type: none">• <code><i>name</i></code>—Collector name (up to 63 characters)• <code><i>ip_address</i></code>—IPv4 or IPv6 address in A.B.C.D or A::B format• <code><i>port_number</i></code>—Port number• <code><i>protocol_type</i></code>—Transport protocol type; UDP or TCP• <code><i>vrf-name</i></code>—Name of the VRF

Modes	CONFIGURATION
Usage	This command configures collector information. A collector is typically a machine reachable from the switch, where the telemetry reports are sent.
Examples	Collector configuration on default VRF: sonic(config-tam) # collector c2 ip 2.2.2.2 port 7676 protocol UDP
	Collector configuration on different user-specified VRF: sonic(config-tam) # collector mod_col ip 10.16.12.5 port 6666 vrf VRF_Blue sonic(config-tam) # no collector c1
Releases	3.1 or later

compatible

Configures OSPFv2 RFC1583 compatibility.

Command	compatible rfc1583
Options	None
Modes	OSPF-VRF
Usage	OSPFv2 RFC2328, the successor to RFC1583, provides a change to the path preference algorithm that prevents possible routing loops, which were possible in the previous OSPFv2 version. The updated RFC states that inter-area paths and intra-area backbone paths are now of equal preference, but both are still preferred to external paths.
Examples	sonic(config) # router ospf sonic(config-router-ospf) # compatible rfc1583 sonic(config-router-ospf) # no compatible rfc1583
Releases	3.0 or later

confederation

Configures an identifier for a BGP confederation.

Command	confederation {{identifier id-as} {peers peer-as}}
Options	<ul style="list-style-type: none"> • identifier id-as — AS number (0 to 65535 for 2 bytes, 1 to 4294967295 for 4 bytes, or 0.1 to 65535.65535 for dotted format) • peers peer-as — AS number for peers in the BGP confederation (1 to 4294967295)
Modes	ROUTER-BGP
Usage	Use this command to configure your system to accept 4-byte formats before entering a 4-byte AS number. All routers in the confederation must be 4-byte or 2-byte identified routers. You cannot have a mix of 2-byte and 4-byte identified routers. The autonomous system number that you configure in this command is visible to the eBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next-hop (MED) and local preference information is preserved throughout the confederation. The system accepts confederation eBGP peers without a LOCAL_PREF attribute. SONiC sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

Examples

```
sonic(config)# router bgp 65300
sonic(config-router-bgp)# confederation identifier 65000
sonic(config-router-bgp)# confederation peers 65100
sonic(config-router-bgp)# confederation peers 65200
sonic(config-router-bgp)# confederation peers 65300

sonic(config-router-bgp)# no confederation peers 65300
```

Releases

3.0 or later

configure terminal

Enters CONFIGURATION mode.

Command configure terminal**Options** None**Modes** EXEC**Usage** Commands in this mode are written to the running configuration file as soon as you enter them. Use [show running-configuration](#) to view the changes to the configuration that you have made. You can also use the shortcut config t.**Example**

```
sonic# configure terminal
sonic(config)# end
sonic# exit
admin@sonic:~$
```

Releases

3.0 or later

consistency-check start access-list

Starts the consistency check of the ACL entries in all databases.

Command consistency-check start [access-list {[mac [access-list-name]] | [ipv4 [access-list-name]] | [ipv6 [access-list-name]]}]**Options** *access-list-name*—Enter the MAC, IPv4, or IPv6 access list name (up to 63 characters)**Modes** EXEC**Usage** Use this command to start the consistency check of the ACL entries in all databases.**Examples**

```
sonic# consistency-check start access-list ipv4 ipv4list
```

Releases

4.0 or later

consistency-check start route

Starts route consistency checker per VRF per AFI.

Command consistency-check start [route [vrf *vrf-name*] [address-family [ipv4 | ipv6]]]**Options**

- *vrf-name*—VRF name
- *ipv4*—Checks IPv4 address-family
- *ipv6*—Checks IPv6 address-family

Modes EXEC

Usage	Use this command to start the consistency check of the route entries in all databases.
Examples	<pre>sonic# consistency-check start route vrf Vrf1 address-family ipv4</pre>
Releases	4.0 or later

consistency-check stop

Stops the consistency check.

Command	<code>consistency-check stop [access-list route]</code>
Options	<ul style="list-style-type: none"> <code>access-list</code>—(Optional) Stops the access-list consistency-checker <code>route</code>—(Optional) Stops the route consistency-checker
Modes	EXEC
Usage	Use this command to stop the consistency check of ACL or route entries while it is running.
Examples	<pre>sonic# consistency-check stop</pre>
Releases	4.0 or later

copp-action

Configures a CoPP action group.

Command	<code>copp-action <i>copp_action_name</i></code>
Options	<code>copp_action_name</code> —Name of the CoPP action (up to 63 characters)
Modes	CONFIGURATION
Usage	Use this command to create a CoPP action group to configure the trap and police actions to perform on the classified traffic.
Examples	<pre>sonic(config)# copp-action copp1</pre> <pre>sonic(config)# no copp-action copp1</pre>
Releases	3.1 or later

copy

Copies any file from a source to a destination.

Command	<code>copy {{copy_config_url {running-configuration [overwrite replace]}}} {running-configuration <i>filepath</i>} {startup-configuration {running-configuration [overwrite]}}}</code>
Options	<ul style="list-style-type: none"> <code>copy_config_url</code> — URL to copy files to or from. <code>filepath</code> — File path to copy files to or from. <code>overwrite</code> — Overwrite the running configuration with a specified configuration file from a remote server or the local file system, and restart core services on the switch.
Modes	EXEC
Usage	Use the <code>copy</code> command to copy the running configuration to the startup configuration, transfer coredump files to a remote location, and backup the startup configuration. You can also retrieve a

previously backed-up configuration, replace the startup configuration file, or transfer support bundles. In interactive mode, you can use special characters in passwords; in non-interactive mode, passwords with special characters are not supported.

Examples

```
sonic# copy http://10.206.28.174:/startup.xml config://test
```

Releases

3.1 or later

core enable

Enables the generation of a core file when an application crash is detected by the kernel.

Command core enable**Options** None**Modes** CONFIGURATION**Usage** Core file generation is enabled by default. Check if the COREDUMP feature is administratively enabled or disabled using the `show core config` command.**Example**

```
sonic(config)# core enable
```

Releases

3.1 or later

counter

Configures VXLAN counter parameters.

Command counter polling-interval *interval***Options** *interval* — Polling interval time in seconds (3 to 30; default is 5)**Modes** INTERFACE-VXLAN**Usage** Use this command to configure the polling interval for all VXLAN tunnels on a VTEP.**Examples**

```
sonic(config)# interface vxlan vtep1
sonic(config-if-vxlan-vtep1)# counter polling-interval 3
```

Releases

4.0 or later

counters

Enables the collection of ACL statistics on a per-interface or per-ACL entry.

Command counters {per-entry | per-interface-entry}**Options**

- **per-entry**—Collects ACL statistics on all interfaces for each ACL permit/deny entry (default).
- **per-interface-entry**—Collects ACL statistics on each interface for each permit/deny entry in the ACLs applied on the interface.

Modes ACCESS-LIST**Usage** Counter modes can be changed only when ACLs are not applied. Some features, such as PAC, generate internal ACLs for their functionality, thus the recommendation is to change the counter mode from default to the mode required and save it. Counter mode change may necessitate HW reprogramming, so to avoid traffic impact, and returns an error if the ACLs are already active.

Examples

```
sonic(config) # hardware
sonic(config-hardware) # access-list
sonic(config-hardware-acl) # counters per-entry
```

Releases

3.1 or later

counters rif interval

Configures interval between two consecutive fetches for L3 routing interface counters.

Command counters rif interval value**Options** value — Route interface interval time in seconds (1 to 10000; default is 5)**Modes** CONFIGURATION**Usage** A routing interface includes the routing port, L3 interface and subinterfaces, and configured VLANs.**Examples**

```
sonic# configure terminal
sonic(config)# counters rif internal 400
```

Releases

4.0 or later

crm

Configures critical resource monitoring.

Command crm {{polling {interval c₁rm-subcmd-data}} | {thresholds {{all {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {acl {{group {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}} | {entry {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {counter {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {table {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {dnat {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {snat {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {fdb {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {ipmc {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {ipv4 {{neighbor {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {nexthop {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {route {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {ipv6 {{neighbor {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {nexthop {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {route {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {nexthop {{group {{member {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}} | {object {{type c₁rm-subcmd-data} | {high c₁rm-subcmd-data} | {low c₁rm-subcmd-data}}}}}}}}}}**Options**

- **interval c₁rm-subcmd-data**—CRM subcommand data
- **thresholds**—Thresholds

Modes CONFIGURATION**Usage** Use this command to set the polling interval and resource monitoring thresholds for ASIC resources.**Examples**

```
sonic(config)# crm polling interval 60
sonic(config)# no crm polling interval
```

Releases	3.1 or later
-----------------	--------------

crm polling-interval

Configures the CRM polling interval.

Command	<code>crm polling-interval interval</code>
Options	<code>interval</code> — Polling interval in seconds (0-9999; default 300)
Modes	CONFIGURATION
Usage	CRM monitoring periodically polls SAI counters to determine ASIC resource usage. To reset the polling interval to the default value of 5 minutes, use the <code>no crm polling interval</code> command.
Examples	<pre>sonic(config)# crm polling-interval 100</pre>

Releases	4.2.1 or later
-----------------	----------------

crm threshold

Configures the high and low thresholds for CRM resources.

Command	<code>crm threshold resource {high low} value</code>
Options	<ul style="list-style-type: none">• <code>resource</code> — Specify a CRM resource. Valid values are:<ul style="list-style-type: none">◦ <code>acl group counter</code> — ACL counter resources◦ <code>acl group entry</code> — ACL entries◦ <code>acl table</code> — ACL table resources◦ <code>dnat</code> — Destination Network Address Translation (NAT) entries◦ <code>fdb</code> — MAC forwarding database (FDB) entries◦ <code>ipv4 neighbor</code> — IPv4 neighbor entries◦ <code>ipv4 nexthop</code> — IPv4 next-hop entries◦ <code>ipv4 route</code> — IPv4 route entries◦ <code>ipv6 neighbor</code> — IPv6 neighbor entries◦ <code>ipv6 nexthop</code> — IPv6 next-hop entries◦ <code>ipv6 route</code> — IPv6 route entries◦ <code>ipmc</code> — IP multicast entries◦ <code>nexthop group member</code> — Next-hop group member resources◦ <code>nexthop group object</code> — Next-hop group object resources◦ <code>snat</code> — Source Network Address Translation entries◦ <code>all</code> — Use the <code>all</code> value to set the threshold type for all CRM resources.• <code>high</code> — Configures the high threshold for a CRM resource (0-100 percent or 0-4294967295 for used or free entries; default 85%).• <code>low</code> — Configures the low threshold for a CRM resource (0-100 percent or 0-4294967295 for used or free entries; default 70%).• <code>value</code> — Configures high and low resource thresholds as the percentage or number of used or available resource entries.
Modes	CONFIGURATION

Usage	You can configure the high and low thresholds for monitoring CRM resources. Use the <code>all</code> option to set the high or low threshold for all CRM resources. The high and low values that you set depend on the configured threshold type (<code>crm threshold type</code> command). When a resource exceeds its high or low threshold value, a Syslog message is generated. To remove a CRM resource threshold and reset the default value, use the <code>no crm threshold resource {high low}</code> command.
--------------	---

Examples

```
sonic(config) # crm threshold all high 90  
sonic(config) # crm threshold ipmc low 65
```

```
sonic(config) # no crm threshold fdb low  
sonic(config) # no crm threshold all
```

Releases

4.2.1 or later

crm threshold type

Configures the format in which thresholds for critical resources are monitored.

Command

```
crm threshold resource type {percentage | used | free}
```

Options

- *resource* — Specify a CRM resource. Valid values are:
 - acl group counter — ACL counter resources
 - acl group entry — ACL entries
 - acl table — ACL table resources
 - dnat — Destination Network Address Translation (NAT) entries
 - fdb — MAC forwarding database (FDB) entries
 - ipv4 neighbor — IPv4 neighbor entries
 - ipv4 nexthop — IPv4 next-hop entries
 - ipv4 route — IPv4 route entries
 - ipv6 neighbor — IPv6 neighbor entries
 - ipv6 nexthop — IPv6 next-hop entries
 - ipv6 route — IPv6 route entries
 - ipmc — IP multicast entries
 - nexthop group member — Next-hop group member resources
 - nexthop group object — Next-hop group member resources
 - snat — Source Network Address Translation entries
 - all — Use the *all* value to set the threshold type for all CRM resources.
- *percentage* — Configures high and low resource thresholds as a percentage (default).
- *used* — Configures high and low resource thresholds as the number of resource entries used.
- *free* — Configures high and low resource thresholds as the number of available resource entries.

Modes

CONFIGURATION

Usage

The CRM high and low thresholds can be specified by the percentage of available resource used, the actual number of resource entries used, or the current number of free, available resource entries. To reset the threshold type to the default value (*percentage*) for a specified resource, use the `no crm threshold resource type` command.

Examples

```
sonic(config) # crm threshold all type percentage  
sonic(config) # crm threshold ipmc type used
```

```
sonic(config) # no crm threshold fdb type  
sonic(config) # no crm threshold all type
```

Releases

4.2.1 or later

crypto ca-cert delete

Removes an installed CA certificate/key pair.

Command

```
crypto ca-cert delete {certificate-name | all}
```

Options	<ul style="list-style-type: none"> • <i>certificate-name</i> — Delete the specified CA certificate and key. • <i>all</i> — Delete all installed CA certificate/key pairs.
Modes	EXEC
Usage	This command does not allow you to delete a CA certificate that is used by a trust store. Use the crypto ca-cert install command to install a CA certificate on the switch.
Example	<pre>sonic# crypto ca-cert delete GeoTrust_Universal_CA.crt</pre>

Releases 4.1.0 or later

crypto ca-cert install

Installs a CA certificate on the switch from the specified URL.

Command	<code>crypto ca-cert install cert-file <i>certificate-url</i></code>
Options	<i>cert-file certificate-url</i> — Enter the URL for a CA certificate in one of the following formats:
	<ul style="list-style-type: none"> • <code>ftp://userid:passwd@hostip/filepath</code> — Installs a CA certificate file from a remote FTP server. • <code>home://filename</code> — Installs a CA certificate file from the home directory. • <code>http://hostip/filepath</code> — Installs a CA certificate file from a remote HTTP server. • <code>scp://userid:passwd@hostip/filepath</code> — Installs a CA certificate file from a remote SCP server.
Modes	EXEC
Usage	Use a CA certificate to verify the client certificates that are used to authenticate access to the REST API and telemetry server. To delete an installed CA certificate pair, use the crypto ca-cert delete command.
Example	<pre>sonic# crypto ca-cert install home://ca.crt Processing certificate ... Installed Root CA certificate as "ca" CommonName = localhost IssuerName = localhost</pre>
Releases	4.1.0 or later

crypto ca-cert verify expiry

Verifies that an installed CA certificate is still valid and has not expired.

Command	<code>crypto ca-cert verify certificate-name expiry</code>
Options	<i>certificate-name</i> —Check to see if an installed CA certificate has expired. Enter a certificate name installed with the crypto ca-cert install command.
Modes	EXEC
Usage	When you install a CA certificate and key, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than 14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated. To view the raw ASCII format of CA host certificates, use the show crypto ca-cert file command.
Example	<pre>sonic# crypto ca-cert verify CA expiry Certificate is valid!</pre>

Or if no longer valid:

```
sonic# crypto ca-cert verify CA expiry  
Certificate has expired!
```

Releases

4.1.0 or later

crypto cert delete

Removes an installed host certificate/key pair.

Command

```
crypto cert delete {certificate-name | all}
```

Options

- *certificate-name* — Delete the specified host certificate and key.
- *all* — Delete all installed host certificate/key pairs.

Modes

EXEC

Usage

Use the [crypto cert install cert-file key-file](#) command to install a host certificate on the switch.

Example

```
sonic# crypto cert delete server.crt
```

Releases

4.1.0 or later

crypto cert generate request

Installs a CA certificate request at a specified URL.

Command

```
crypto cert generate request cert-file certificate-url key-file key-url  
[password] [parameters]
```

Options

- *cert-file certificate-url key-file key-url* — Enter the URLs for a CA certificate/key request in one of the following formats:
 - *ftp://userid:passwd@hostip/filepath* — Installs a host certificate request on a remote FTP server.
 - *home://filename* — Installs a host certificate request in the home directory.
 - *http://hostip/filepath* — Installs a host certificate request on a remote HTTP server.
 - *scp://userid:passwd@hostip/filepath* — Installs a host certificate request on a remote SCP server.
 - *usb://filepath* — Installs a host certificate request on an attached USB device.
- *password* — Enter an optional password if a private key file is password-protected.
- *parameters* — Add optional parameters to the host certificate request, such as a DNS server name and a common name to identify the certificate. For detailed information on the optional parameters you can enter in a host certificate request, refer to the X.509 specification.

Modes

EXEC

Usage

You can create a host certificate request that you send to a Certificate Authority to receive a CA-signed certificate. To install the certificate, use the [crypto cert install cert-file key-file](#) command. The CA-signed host certificate replaces the self-signed local certificate that SONiC generates by default.

Example

```
sonic# crypto cert generate request cert-file home://server-req.csr key-  
file home://server.key cname myserver altname DNS:myserver
```

Releases

4.1.0 or later

crypto cert install cert-file key-file

Installs a certificate-key pair for use with the REST server on the switch from the specified URLs.

Command	<code>crypto cert install cert-file <i>certificate-url</i> key-file <i>key-url</i> [<i>password</i>]</code>
Options	<code>cert-file <i>certificate-url</i> key-file <i>key-url</i></code> — Enter a URL in one of the following formats: <ul style="list-style-type: none">• <code>ftp://userid:passwd@hostip/filepath</code> — Installs a host certificate file from a remote FTP server.• <code>home://filename</code> — Installs a host certificate file from the home directory.• <code>http://hostip/filepath</code> — Installs a host certificate file from a remote HTTP server.• <code>scp://userid:passwd@hostip/filepath</code> — Installs a host certificate file from a remote SCP server.• <code>password</code> — Enter an optional password if a private key file is password-protected.
Modes	EXEC
Usage	By default, SONiC generates a self-signed host certificate for the REST and telemetry servers. Use this command to replace the auto-generated certificate with a host certificate that has been signed by a Certificate Authority. The certificate-key pair is maintained across image upgrades. Installing a host certificate triggers a certificate expiration check. To delete a host certificate/key pair, use the crypto cert delete command.
Example	<pre>sonic# crypto cert install cert-file home://server.crt key-file home://server.key Processing certificate ... Installed host certificate CommonName = server IssuerName = www.dell.com</pre>
Releases	4.1.0 or later

crypto cert verify expiry

Verifies that an installed certificate is still valid and has not expired.

Command	<code>crypto cert verify <i>certificate-name</i> expiry</code>
Options	<code><i>certificate-name</i></code> —Check to see if an installed certificate has expired. Enter a certificate name installed with the crypto cert install cert-file keyfile command.
Modes	EXEC
Usage	When you install a certificate and key, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than 14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated.
Example	<pre>sonic# crypto rest-cert verify server expiry Certificate is valid!</pre>
	Or if no longer valid:
	<pre>sonic# crypto rest-cert verify server expiry Certificate has expired!</pre>
Releases	4.1.0 or later

crypto fips enable

Enables FIPS mode for FIPS-compliant services.

Command	<code>crypto fips enable</code>
Options	None
Modes	CONFIGURATION
Usage	FIPS mode is disabled by default. When you enable or disable FIPS mode, FIPS-compliant services are restarted. For SSH, SSH host keys are regenerated. Existing SSH sessions are not affected. To disable FIPS mode for FIPS-compliant services, use the <code>no crypto fips enable</code> command.
Example	<pre>sonic (config)# crypto fips enable WARNING: Upon committing this configuration, the system will regenerate SSH keys. Please consult documentation to get information about FIPS mode. Continue? [yes/no(default)]:yes sonic(config)# sonic(config)# no crypto fips enable WARNING: Upon committing this configuration, the system will regenerate SSH keys. Please consult documentation to get information about FIPS mode. Continue? [yes/no(default)]:yes sonic(config)# </pre>
Releases	4.2.1 or later

crypto security-profile

Creates a security profile for REST and telemetry services. You can sue the command to configure optional security profile settings.

Command	<code>crypto security-profile [cdp-list <i>cdp-list</i>] [oscp-list <i>oscp-list</i>] <i>profile-name</i> [<i>cdp-list</i>] [<i>cdp-list</i>] [key-usage-check {True False}] [peer-name-check {True False}] [revocation-check {True False}]</code>
Options	<ul style="list-style-type: none">• <i>profile-name</i> — Profile name (up to 63 characters)• <i>cdp-list cdp-list</i> — (Optional) Adds a global Certificate Revocation List (CRL) Distribution Point (CDP) list to receive CRL updates in addition to the CDPs defined in installed certificates. For <i>cdp-list</i>, enter a comma-separate list of the URLs for remote CDP servers in the format <code>http://host-ip/filepath</code>.• <i>oscp-list oscp-list</i> — Adds a global Online Certificate Status Protocol (OSCP) responder list in addition to the responders defined in installed certificates. For <i>oscp-list</i>, enter a comma-separate list of the URLs for remote OSCP responder servers in the format <code>http://host-ip/filepath</code>.• <i>key-usage-check {True False}</i> — (Optional) Requires the REST API to verify if the key used to authenticate a remote device is associated with a CA-signed host certificate or a client certificate. Enter True to ensure that the correct certificate/key pair is used to access the switch; enter False not to check whether authentication is performed in server or client certificate mode. Default: False.• <i>peer-name-check {True False}</i> — (Optional) Requires the REST API service to verify if the remote device name matches the name on the certificate used to authenticate the device: True verifies the device name; False does not perform a remote device name check. Default: False.• <i>revocation-check {True False}</i> — (Optional) Requires immediate revocation of an installed certificate if the revocation check returns a valid response: True performs a certificate check; False does not use certificate revocation. Default: False.
Modes	CONFIGURATION

Usage Use this command to create a security profile for an Enterprise SONiC service, such as telemetry and REST, in which you store installed CA certificates that authenticate client access. To associate the security profile with a CA certificate, use the [crypto security-profile certificate](#) command.

Examples

```
sonic(config)# crypto security-profile myserver  
  
sonic(config)# crypto security-profile myserver key-usage-check true  
peer-name-check false revocation-check true  
  
sonic(config)# crypto security-profile cdp-list myserver http://  
a.example.com/cdp,http://b.example.com/cdp  
  
sonic(config)# crypto security-profile ocsp-list myserver http://  
a.example.com/ocsp,http://b.example.com/ocsp
```

Releases

4.1.0 or later

crypto security-profile certificate

Associates a host certificate with a security profile for REST or telemetry services.

Command `crypto security-profile certificate profile-name certificate-filename`

Options

- *profile-name* — Enter the name of a security profile.
- *certificate-name* — Enter the certificate name created with the [crypto cert install cert-file keyfile](#) command.

Modes

CONFIGURATION

Usage

Use this command to configure a certificate for a security profile. To create a security profile for REST and telemetry services, use the [crypto security-profile](#) command.

Examples

```
sonic(config)# crypto security-profile certificate myserver server
```

Releases

4.1.0 or later

crypto security-profile trust-store

Associates a trust store with a security profile for REST or telemetry services.

Command `crypto security-profile trust-store profile-name trust-store-name`

Options

- *profile-name* — Enter the name of a security profile.
- *trust-store-name* — Enter the name of a trust store created with the [crypto trust-store](#) command.

Modes

CONFIGURATION

Usage

Use this command to associate a trust store with CA certificates with a security profile. To associate a CA certificate with a trust store, use the [crypto trust-store ca-cert](#) command. To create a security profile for REST and telemetry services, use the [crypto security-profile](#) command.

Examples

```
sonic(config)# crypto security-profile trust-store myserver @telemetry
```

Releases

4.1.0 or later

crypto ssh-keygen

Generates SSH host keys for use in encrypted connections with SSH clients.

Command	<code>crypto ssh-keygen {ecdsa {256 384 521} rsa {2048 3072 4096}}</code>
Options	<ul style="list-style-type: none"><code>ecdsa {256 384 521}</code> — Generate an ECDSA key type of the specified length in bits (default 256).<code>rsa {2048 3072 4096}</code> — Generate an RSA key type of the specified length in bits (default 2048).
Mode	EXEC
Usage	When you configure SSH, take into account that the SSH keys generated for use with SSH clients consist of a key algorithm, key size, and key pair generation. SSH key generation supports various cryptographic algorithms, such as RSA and ECDSA, and key-length customization based on security requirements.
Examples	<pre>sonic# crypto ssh-keygen ecdsa 256 Processing SSH Key Gen request ... Generated 256-bit ecdsa key!!!</pre> <pre>sonic(config)# no crypto ssh-keygen ecdsa</pre> <pre>sonic# crypto ssh-keygen rsa 2048 Processing SSH Key Gen request ... Generated 2048-bit rsa key!!!</pre>
Releases	4.4.1 or later

crypto trust-store

Creates a trust store in which you store CA certificates that are used to validate client certificates.

Command	<code>crypto trust-store <i>trust-store-name</i></code>
Options	<code><i>trust-store-name</i></code> — Enter the name of a trust store (up to 63 characters).
Modes	CONFIGURATION
Usage	Use this command to create a trust store in which you store CA certificates, which you can later associate with security profiles. To associate a CA certificate with a trust store, use the crypto trust-store ca-cert command. To associate a trust store with CA certificates with a security profile, use the crypto security-profile trust-store command.
Examples	<pre>sonic(config)# crypto trust-store telemts</pre>
Releases	4.1.0 or later

crypto trust-store ca-cert

Adds a CA certificate to a trust store.

Command	<code>crypto trust-store <i>trust-store-name</i> ca-cert <i>certificate-name</i></code>
Options	<code><i>certificate-name</i></code> — Enter a certificate name installed with the crypto cert install cert-file keyfile command.
Modes	CONFIGURATION
Usage	Use this command to associate a CA certificate with a trust store. Use the crypto security-profile trust-store command to associate the trust store with a security profile.

Examples

```
sonic(config)# crypto trust-store telemts ca-cert CA
```

Releases

4.1.0 or later

D commands

Topics:

- dampening
- debug shell
- default interface
- default ipv4-unicast
- default local-preference
- default show-hostname
- default shutdown
- default subgroup-pkt-queue-max
- default-information
- default-metric
- default-originate
- default-originate
- delay-restore
- delete
- delete-reason
- description
- destination
- destination CPU
- destination erspan
- detect-multiplier
- deterministic-med
- df-election-time
- df-preference
- diag-mode
- dir
- disable-connected-check
- disable-ead-evi-rx
- disable-ead-evi-tx
- disable-ebgp-connected-route-check
- distance
- distance bgp
- dont-capability-negotiate
- dot1p
- dot1x pae
- dot1x system-auth-control
- dot1x timeout
- downstream all-mclag
- downstream all-evpn-es
- drop-monitor
- dropcounters
- dscp
- duplex
- dup-addr-detection
- dup-addr-detection freeze

dampening

Enables BGP route-flap dampening and configures the dampening parameters.

Command	<code>dampening [halflife] {[reusethr] {suppressthr maxsuppress}}</code>
Options	<ul style="list-style-type: none">• <i>halflife</i> — (Optional) Half-life time, in minutes, after which the penalty decreases; after the router assigns a penalty of 1024 to a route, the penalty decreases by half after the half-life period expires (1 to 45; default 15)• <i>reusethr</i> — (Optional) Reuse threshold value which compares to the flapping route's penalty value; if the penalty value is less than the reuse value, the flapping route advertises again and is not suppressed (1 to 20000; default 750)• <i>suppressthr</i> — Suppress threshold value which compares to the flapping route's penalty value; if the penalty value is greater than the suppress value, the flapping route is no longer advertised (1 to 20000; default 2000)• <i>maxsuppress</i> — Maximum number of minutes a route is suppressed (1 to 255; default 60)
Modes	BGP-ADDRESS-FAMILY
Usage	Use this command to reduce the instability of the BGP process. After you set up the dampening parameters, clear information about route dampening and return the suppressed routes to the Active state.
Examples	<pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# address-family ipv4 unicast sonic(config-router-bgp-af)# dampening 10 1200 2000 40</pre> <pre>sonic(config-router-bgp-af)# no dampening</pre>
Releases	3.0 or later

debug shell

Debug shell for SONiC.

Command	<code>debug shell</code>
Options	None
Modes	EXEC
Usage	(i) NOTE: This mode is restricted to admin role.
Examples	<pre>sonic# debug shell sonic(debugsh) #</pre>
Releases	4.0 or later

default interface

Restores a selected port to the factory default configuration.

Command	<code>default interface {Ethernet iface range Ethernet iface-range}</code>
Options	<ul style="list-style-type: none">• <i>iface</i> — Resets an Ethernet interface to its default settings• <i>range Ethernet iface-range</i> — Resets a range of Ethernet interfaces to their default settings
Modes	CONFIGURATION

Usage

Use this command to remove the configuration from an Ethernet interface and reset the interface to its default settings. This command removes all software settings and all L3, VLAN, and port channel configurations on a physical interface. Enter multiple interfaces in a comma-separated string or a port range using the `default interface range` command.

Example

```
sonic(config)# default interface Ethernet 8

sonic(config)# default interface range Ethernet 1-4,6,8-10

Leaf1# show running-configuration interface Ethernet 73
!
interface Ethernet73
mtu 9100
speed 10000
unreliable-los auto
no shutdown
switchport trunk allowed Vlan 100
Leaf1# configure terminal
Leaf1(config)# default interface Ethernet 73
Leaf1(config)# exit
Leaf1# show running-configuration interface Ethernet 73
!
interface Ethernet73
mtu 9100
speed 10000
unreliable-los auto
shutdown
Leaf1#
```

Releases

3.1 or later

default ipv4-unicast

Enables IPv4 unicast address-family for a BGP peer.

Command `default ipv4-unicast`

Options None

Modes ROUTER-BGP

Usage This command resets the automatic exchange of IPv4 address prefixes as the default when a BGP peer session starts. The default is to advertise only IPv4 prefix routes if you previously changed the default by entering the `no default ipv4-unicast` command.

Examples

```
sonic(config)# router bgp 65300
sonic(config-router-bgp)# default ipv4-unicast
```

```
sonic(config-router-bgp)# no default ipv4-unicast
```

Releases

3.0 or later

default local-preference

Configures the default value for the local preference attribute.

Command `default local-preference value`

Options `value` — Enter a number to assign to routes as the degree of preference for those routes (1 through 4294967295; default is 100)

Modes ROUTER-BGP

Usage Use this command to set the default value of the local preference parameter. During BGP best-path selection, the local preference value is applied to the routes exchanged with a neighbor. The no form of this command deletes the local preference value.

Examples

```
sonic(config)# router bgp 65300  
sonic(config-router-bgp)# default local-preference 200
```

```
sonic(config-router-bgp)# no default local-preference
```

Releases 3.0 or later

default show-hostname

Configures BGP to display the hostname in specific display commands.

Command default show-hostname

Options None

Modes ROUTER-BGP

Usage Use this command to display the hostname in addition to the IP address of the local BGP router in show output.

Examples

```
sonic(config)# router bgp 65300  
sonic(config-router-bgp)# default show-hostname
```

```
sonic(config-router-bgp)# no default show-hostname
```

Releases 3.0 or later

default shutdown

Configures BGP to make newly created BGP neighbors in admin shutdown state.

Command default shutdown

Options None

Modes ROUTER-BGP

Usage By default, newly created BGP neighbors are in admin enabled state.

Examples

```
sonic(config)# router bgp 65300  
sonic(config-router-bgp)# default shutdown
```

```
sonic(config-router-bgp)# no default shutdown
```

Releases 3.0 or later

default subgroup-pkt-queue-max

Configures the maximum packet queue length for update groups.

Command default subgroup-pkt-queue-max value

Options value — Maximum packet queue length

Modes ROUTER-BGP

Usage	This command sets the maximum number of packets that are allowed in a retransmit queue in a sub-AS.
Examples	<pre>sonic(config) # router bgp 65300 sonic(config-router-bgp) # default subgroup-pkt-queue-max 50</pre> <pre>sonic(config-router-bgp) # no default subgroup-pkt-queue-max</pre>
Releases	3.0 or later

default-information

Generates and distributes a default external route to the OSPF routing domain.

Command	<code>default-information originate {[always] {[metric <i>metric_value</i>] {[metric-type <i>metric_type</i>] {[route-map <i>route-map_name</i>]}}}}</code>
Options	<ul style="list-style-type: none"> • <i>always</i> — (Optional) Always advertises the default route • <i>metric_value</i> — (Optional) Metric that is used for generating the default route; defaults to 10 if not specified • <i>metric_type</i> — (Optional) External link type associated with the default route that is advertised into the OSPF routing domain; valid values are type 1 or type 2 (default) • <i>route-map_name</i> — (Optional) Route-map name (up to 15 characters)
Modes	ROUTER-OSPF
Usage	Use this command to configures default route information origination parameters. Metric value and metric type can be explicitly specified for default routes. Route map rules can also be applied on default routes.
Examples	<pre>sonic(config) # router ospf 10 sonic(config-router-ospf-10) # default-information originate always</pre> <pre>sonic(config-router-ospf-10) # default-information originate metric 80</pre> <pre>sonic(config-router-ospf-10) # default-information originate metric-type 1</pre> <pre>sonic(config-router-ospf-10) # default-information originate route-map rmap_droute</pre> <pre>sonic(config-router-ospf-10) # no default-information originate</pre>
Releases	3.1 or later

default-metric

Sets default metric values for the OSPF routing protocol.

Command	<code>default-metric <i>metric_value</i></code>
Options	<i>metric_value</i> — Default metric value appropriate for the specified routing protocol (0 to 16777214)
Modes	ROUTER-OSPF
Usage	This command is used on conjunction with redistribute to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. When metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

```
sonic(config) # router ospf 10
sonic(config-router-ospf-10) # default-metric 2000

sonic(config-router-ospf-10) # no default-metric
```

Releases

3.1 or later

default-originate

Configures the default route to a BGP peer or neighbor.

Command `default-originate [route-map] rtemap`**Options** `rtemap` — Route-map name (up to 140 characters)**Modes**

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY

Usage Use this command to configure the default route to this neighbor, or neighbors in a peer-group. You can optionally use route-map to specify criteria to originate a default.**Examples**

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af) # default-originate

sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # default-originate

sonic(config-router-bgp-neighbor-af) # no default-originate
sonic(config-router-bgp-pg-af) # no default-originate
```

Releases

3.0 or later

default-originate

Enables border-leaf to originate IPv4 default type-5 EVPN routes.

Command `default-originate {ipv4 | ipv6}`**Options**

- `ipv4`—IPv4 default type-5 EVPN routes
- `ipv6`—IPv6 default type-5 EVPN routes

Modes BGP-ADDRESS-FAMILY**Usage** Use this command to advertise the EVPN type-5 default route from the border leaf router, allowing leaf nodes in the EVPN fabric to connect to the external network using border-leaf.**Examples**

```
sonic(config) # router bgp 100 vrf Vrf1
sonic(config-router-bgp) # address-family l2vpn evpn
sonic(config-router-bgp-af) # default-originate ipv4

sonic(config-router-bgp-af) # no default-originate ipv4
```

Releases

3.0 or later

delay-restore

Configures the MCLAG delay restore time in seconds.

Command	<code>delay-restore <i>seconds</i></code>
Options	<code><i>seconds</i></code> — Delay restore time in seconds (1 through 3600; default is 300)
Modes	MCLAG
Usage	Use this command to delay the system from bringing up the port for a brief period to allow the exchange of control information, such as, MAC and ARP tables between MCLAG peers. This delay restore works only if MCLAG is configured as downstream under link state tracking.
Examples	<pre>sonic(config-mclag-domain-100)# delay-restore 180</pre>
Releases	3.1 or later

delete

Deletes the file from local file systems.

Command	<code>delete {config:/ coredump:/ event-profile:/ home:/ tech-support:/}</code>
Options	<ul style="list-style-type: none">• <code>config:/</code>—Delete from configuration directory• <code>coredump:/</code>—Delete from coredump directory• <code>event-profile:/</code>—Delete from event-profile directory• <code>home:/</code>—Delete from home directory• <code>tech-support:/</code>—Delete from tech-support directory
Modes	EXEC
Usage	Use this command to delete a system file from a specified directory.
Examples	<pre>sonic# delete config:/ support Proceed to delete config:/support? [y/N]: y</pre>
Releases	4.0 or later

delete-reason

Deletes drop counter reason.

Command	<code>delete-reason <i>reason</i></code>
Options	<code><i>reason</i></code> — Reason of the drop counter.
Modes	DROPCOUNTERS
Usage	The supported drop counter reasons are ANY, MPLS_MISS, IP_HEADER_ERROR, FDB_AND_BLACKHOLE_DISCARDS, SMAC_EQUALS_DMAC, ACL_ANY, SIP_LINK_LOCAL, DIP_LINK_LOCAL, L3_EGRESS_LINK_DOWN, and EXCEEDS_L3_MTU.
Examples	<pre>sonic# configure terminal sonic(config)# dropcounters drop1 sonic(config-dropcounters-drop1)# delete-reason any</pre>
Releases	4.0 or later

description

Configures a description for an interface, link state group, BGP neighbor, and BGP peer-group.

Command	<code>description string</code>
Options	<code>string</code> — Descriptive string.
Modes	<ul style="list-style-type: none">• DROPCOUNTERS• INTERFACE• LINK-STATE-GROUP• BGP-NEIGHBOR• BGP-PEER-GROUP• POLICY-MAP
Usage	In INTERFACE, LINK-STATE-GROUP, BGP-NEIGHBOR, and BGP-PEER-GROUP mode, the description string can be up to 240 characters. In POLICY-MAP mode, the description string can be up to 256 characters. Special characters are allowed. To use spaces between characters, enclose the entire description in quotation marks; for example "text description". The text string that you enter overwrites any previously configured text string.
Examples	<pre>sonic(config)# interface Eth 1/1/1 sonic(config-if-Eth1/1/1)# description "100G_Link_Connected_To_S5232" sonic(config-if-Eth1/1/1)# do show running-configuration interface Eth 1/1/1 ! interface Eth1/1/1 description 100G_Link_Connected_To_S5232 mtu 9100 speed auto fec RS unreliable-los auto no shutdown</pre> <pre>sonic# show interface Eth 1/1/1 Eth1/1/1 is up, line protocol is up, reason oper-up Hardware is Eth, address is e8:b5:d0:02:6e:81 Description: 100G_Link_Connected_To_S5232 Mode of IPV4 address assignment: not-set Mode of IPV6 address assignment: not-set Interface IPv6 oper status: Disabled IP MTU 9100 bytes LineSpeed 100GB, Auto-negotiation on Link-training: trained Unreliable-LOS: off FEC: RS Events: initialized at 2023-03-07T13:37:27.947896Z admin-up at 2023-03-07T13:39:20.600276Z xcvr-status-down at 2023-03-07T13:40:58.283562Z xcvr-status-up at 2023-03-07T13:41:31.127281Z</pre> <pre>sonic(config)# dropcounters count1 sonic(config-dropcounters-count1)# description dropcounter1</pre>

Releases	3.0 or later
-----------------	--------------

destination

Configures an SPAN mirror-sessions for port mirroring.

Command	<code>destination phy-if-id [source {phy-if-name po-if-name}] [direction {rx tx both}]</code>
----------------	---

Options	<ul style="list-style-type: none"> • <i>phy-if-id</i> — Ethernet interface ID • <i>phy-if-id</i> — (Optional) Source interface ID • <i>po-if-id</i> — (Optional) PortChannel interface ID • {rx tx both} — (Optional) Port mirror session direction; rx, tx, or both
Modes	MIRROR-SESSION
Usage	In mirror-session mode, use this command to configure the local destination port interface, source interfaces if different from the interface on which the policy is applied, and the direction in which mirrored traffic is sent (tx) or received (rx).
Example	<pre>sonic(config) # mirror-session Mirror1 sonic(config-mirror-Mirror1) # destination Ethernet0 source Ethernet4 direction rx Success sonic(config-mirror-Mirror1) # exit</pre>
Releases	3.1 or later

destination CPU

Configures SPAN mirror-session to the CPU port.

Command	destination CPU [source { <i>phy-if-name</i> <i>po-if-name</i> }] [direction {rx tx both}]
Options	<ul style="list-style-type: none"> • <i>source</i> — (Optional) Destination source • <i>phy-if-name</i> — (Optional) Ethernet interface number • <i>po-if-name</i> — (Optional) PortChannel interface number • <i>direction</i> {rx tx both} — (Optional) Port mirror-session direction; rx, tx, or both
Modes	MIRROR-SESSION
Usage	In mirror-session mode, use this command to specify the CPU local destination port, source interfaces if different from the interface on which the policy is applied, and the direction in which mirrored traffic is sent (tx) or received (rx).
Example	<pre>sonic(config) # mirror-session Mirror1 sonic(config-mirror-Mirror1) # destination CPU source Ethernet4 direction rx Success sonic(config-mirror-Mirror2) #</pre>
Releases	3.1 or later

destination erspan

Configures an encapsulated remote switch port analyzer (ERSPAN) mirror-session.

Command	destination erspan [<i>dst-ip dst_ip</i>] [<i>src-ip src_ip</i>] [<i>scp ip_dscp</i>] [<i>gre ip_gre</i>] [<i>ttl ip_ttl</i>] [<i>queue queue_val</i>] [<i>source {phy-if-name po-if-name}</i>] [<i>direction sess-direction</i>]
Options	<ul style="list-style-type: none"> • <i>dst_ip</i> — (Optional) Destination IP address in A.B.C.D format • <i>src_ip</i> — (Optional) Source IP address in A.B.C.D format • <i>ip_dscp</i> — (Optional) DSCP • <i>ip_gre</i> — (Optional) Greater or equal to • <i>ip_ttl</i> — (Optional) TTL • <i>queue_val</i> — (Optional) Queue • <i>phy-if-name</i> — (Optional) Ethernet interface ID • <i>po-if-name</i> — (Optional) PortChannel interface ID • <i>sess-direction</i> — (Optional) Port mirror-session direction; rx, tx, or both

Modes	MIRROR-SESSION
Usage	Supports mirroring to any destination IP. Source interface can be either port or PortChannel. Supports mirroring in rx, tx, or both directions. Mirror-session can be used in ACL configurations.
Example	<pre>sonic(config)# mirror-session Mirror2 sonic(config-mirror-Mirror2)# destination erspan dst-ip 10.1.1.1 src-ip 11.1.1.1 dscp 10 ttl 10 gre 0x88ee queue 10 source Ethernet4 direction rx Success sonic(config-mirror-Mirror2) #</pre>
Releases	3.1 or later

detect-multiplier

Configures a detection multiplier to determine packet loss.

Command	<code>detect-multiplier <i>multiplier</i></code>
Options	<code>multiplier</code> — Peer detect multiplier value to determine packet loss. The default value is 3.
Modes	<ul style="list-style-type: none"> • BFD PEER • BFD PROFILE
Usage	None
Example	Example for PEER mode:

```
device()#configure terminal
device(config)#bfd
device(config-bfd)# peer 192.168.0.5 interface Ethernet0
device(config-bfd-peer)# detect-multiplier 2
```

Example for PROFILE mode:

```
device()#configure terminal
device(config)#bfd
device(config-bfd)# profile fast
device(config-bfd-profile)# detect-multiplier 2
```

Releases	3.0 or later
-----------------	--------------

deterministic-med

Carries out route-selection that produces deterministic results locally.

Command	<code>deterministic-med</code>
Options	None
Modes	ROUTER-BGP
Usage	Use this command to carry out route-selection in a way that produces deterministic results locally, even in the face of MED and the lack of a well-defined order of preference it can induce on routes. Without this option, the preferred route with MED may be determined largely by the order that routes were received in. Setting this option will have a performance cost that may be noticeable when there are many routes for each destination. BGP is implemented in a way that scales poorly as the number of routes per destination increases. By default deterministic-med is disabled.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# deterministic-med</pre> <pre>sonic(config-router-bgp)# no deterministic-med</pre>

Releases	3.0 or later
-----------------	--------------

df-election-time

Configures the time period for which the Designated Forwarder election is delayed after the Ethernet Segment port channel comes up on a multihomed VTEP.

Command	<code>df-election-time seconds</code>
Options	<code>seconds</code> — Enter the time period in seconds (0-86400; default 3) for which the designated forwarder election is delayed after the ES port channel comes up on a multihomed VTEP.
Modes	EVPN ETHERNET-SEGMENT
Usage	DF election is triggered when the ES port channel comes up on a multihomed VTEP. Configure the same <code>df-election-time</code> value on all multihomed VTEPs.
Examples	<pre>sonic(config)# evpn esi-multihoming sonic(config-evpn-esi-mh)# df-election-time 5</pre>

Releases	4.4.0 or later
-----------------	----------------

df-preference

Configures a designated forwarder (DF) value to determine which VTEP in an active-active Ethernet segment forwards BUM traffic.

Command	<code>df-preference df-number</code>
Options	<code>df-number</code> —Configures the designated forwarder preference (1-65535; default 32767). The VTEP with the highest DF value in the Ethernet segment is selected as the designated forwarder.
Modes	EVPN ETHERNET-SEGMENT
Usage	By default, the VTEP with the highest DF value is selected as the designated forwarder. If the configured DF values on multihomed VTEPs are the same, the VTEP with the lowest source IP address is chosen as the DF. For detailed information, see RFC 7432 .
Examples	<pre>sonic(config)# interface PortChannel1 sonic(config-if-pol1)# evpn ethernet-segment 00:11:22:33:44:55:66:77:88:01 sonic(es-id-00:11:22:33:44:55:66:77:88:01)# df-preference 1</pre>

Releases	4.2.0 or later
-----------------	----------------

diag-mode

Configures port Diagnostic mode.

Command	<code>diag-mode {on off}</code>
Options	<ul style="list-style-type: none"><code>on</code>—Enables port Diagnostic mode<code>off</code>—Disables port Diagnostic mode
Modes	INTERFACE
Usage	This command configures the port to Diagnostic mode.
Examples	<pre>sonic(config)# interface Ethernet1 sonic(config-if-Ethernet1)# diag-mode on</pre>

Releases	4.0 or later
-----------------	--------------

dir

Displays folder contents.

Command	dir {config:/ coredump:/ event-profile:/ home:/ log:/ tech-support:/}
----------------	---

Options	<ul style="list-style-type: none">• config:/—Folder containing config files• coredump:/—Folder containing core dump files• event-profile:/—Folder containing event-profile files• home:/—Home folder of the user• dir:/—Folder containing log files• tech-support:/—Folder containing the tech support files
----------------	---

Modes	EXEC
--------------	------

Usage	Use this command to view system files in a specified directory.
--------------	---

Examples	
-----------------	--

```
sonic# dir home://
-----
Date>Last Modified) Size(Bytes) Type Filename
-----
2021-11-02 13:02 19144 - config_db.json
2021-11-02 13:01 30720 - running-1.tar
2021-11-02 13:02 30720 - running-2.tar
```

Releases	4.0 or later
-----------------	--------------

disable-connected-check

Disables the restriction that eBGP peers must be directly connected.

Command	disable-connected-check
----------------	-------------------------

Options	None
----------------	------

Modes	<ul style="list-style-type: none">• BGP-NEIGHBOR• BGP-PEER-GROUP
--------------	---

Usage	Use this command to allow peerings between directly connected eBGP peers using loopback addresses.
--------------	--

Examples	
-----------------	--

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# disable-connected-check
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# disable-connected-check
```

```
sonic(config-router-bgp-neighbor)# no disable-connected-check
sonic(config-router-bgp-pg)# no disable-connected-check
```

Releases	3.0 or later
-----------------	--------------

disable-ead-evi-rx

Disables the learning of EAD-per-EVI routes so that BGP EVPN multihoming for the L2VPN EVPN address family on an Enterprise SONiC switch is compatible with EVPN on third-party VTEP switches, which do not support EAD-per-EVI routes.

Command	disable-ead-evi-rx
Options	None
Modes	BGP-ADDRESS-FAMILY
Usage	To disable the advertisement of EAD-per-EVI routes in BGP EVPN multihoming, use the disable-ead-evi-tx command.
Examples	<pre>sonic(config)# router bgp 10 sonic(config-router-bgp)# address-family l2vpn evpn sonic(config-router-bgp-af)# disable-ead-evi-rx</pre>
Releases	4.2.0 or later

disable-ead-evi-tx

Disables the advertisement of EAD-per-EVI routes so that BGP EVPN multihoming for the L2VPN EVPN address family on an Enterprise SONiC switch is compatible with EVPN on third-party VTEP switches.

Command	disable-ead-evi-tx
Options	None
Modes	BGP-ADDRESS-FAMILY
Usage	To disable the leaning of EAD-per-EVI routes in BGP EVPN multihoming, use the disable-ead-evi-rx command.
Examples	<pre>sonic(config)# router bgp 10 sonic(config-router-bgp)# address-family l2vpn evpn sonic(config-router-bgp-af)# disable-ead-evi-tx</pre>
Releases	4.2.0 or later

disable-ebgp-connected-route-check

Disables eBGP connected route check.

Command	disable-ebgp-connected-route-check
Options	None
Modes	ROUTER-BGP
Usage	Use this command to disable checking if next-hop is connected on eBGP sessions. When BGP peering is between the loopback interfaces, enable this option.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# disable-ebgp-connected-route-check</pre> <pre>sonic(config-router-bgp)# no disable-ebgp-connected-route-check</pre>
Releases	3.0 or later

distance

Defines OSPF route administrative distances based on route type.

Command `distance {[admindistance] | {[ospf {[external extdistance]} {[inter-area interdistance]} {[intra-area intradistance]}]}}`

- Options**
- *admindistance*—(Optional) Sets the administrative distance for routes
 - *extdistance*—(Optional) Sets the distance for routes from other routing domains, learned by redistribution (1 to 255; default is 110)
 - *interdistance*—(Optional) Sets the distance for all routes from one area to another area (1 to 255; default is 110)
 - *intradistance*—(Optional) Sets the distance from all routes within an area (1 to 255; default is 110)

Modes ROUTER-OSPF

Usage Use this command when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from each other.

Examples

```
sonic(config)# router ospf 10
sonic(config-router-ospf)# distance ospf external 100
```

```
sonic(config-router-ospf)# no distance ospf external
```

Releases 3.1 or later

distance bgp

Sets the administrative distance for BGP routes.

Command `distance bgp external {internal local}`

- Options**
- *external* — Number to assign to routes learned from a neighbor external (eBGP) to the AS (1 to 255; default 20)
 - *internal* — Number to assign to routes learned from a router within (iBGP) the AS (1 to 255; default 200)
 - *local* — Number to assign to routes learned from networks (1 to 255; default 200)

Modes BGP-ADDRESS-FAMILY

Usage Use this command to configure the administrative distance for eBGP route, iBGP route, and local BGP route. The command allows finer control to change the distance values for external routes, internal routes, and local routes separately. Administrative distance indicates the reliability of the route; the lower the administrative distance, the more reliable the route is. Routes that are assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as iBGP routes.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family ipv4 unicast
sonic(config-router-bgp-af)# distance bgp 100 50 10
```

```
sonic(config-router-bgp-af)# no distance bgp
```

Releases 3.0 or later

dont-capability-negotiate

Disables capability negotiation for a BGP neighbor, or neighbors in a peer-group.

Command	<code>dont-capability-negotiate</code>
Options	None
Modes	<ul style="list-style-type: none">• BGP-NEIGHBOR• BGP-PEER-GROUP
Usage	This command suppresses the sending capability negotiation as OPEN message optional parameter to the peer. This command only affects the peer is configured other than IPv4 unicast configuration. When a remote peer does not have capability negotiation feature, remote peer will not send any capabilities at all — BGP configures the peer with configured capabilities. You may prefer locally configured capabilities more than the negotiated capabilities even though remote peer sends capabilities. If the peer is configured by override-capability, BGP ignores received capabilities then override negotiated capabilities with configured values. This feature fundamentally disables the ability to use widely deployed BGP features such as BGP unnumbered, hostname support, AS4, addpath, route refresh, ORF, dynamic capabilities, and graceful restart.
Examples	<pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# neighbor 30.30.30.3 sonic(config-router-bgp-neighbor)# dont-capability-negotiate</pre> <pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# peer-group PG_Ext sonic(config-router-bgp-pg)# dont-capability-negotiate</pre> <pre>sonic(config-router-bgp-neighbor)# no dont-capability-negotiate sonic(config-router-bgp-pg)# no dont-capability-negotiate</pre>
Releases	3.0 or later

dot1p

Adds dot1p to the traffic class entry in the map.

Command	<code>dot1p dot1p_list {traffic-class tc}</code>
Options	<ul style="list-style-type: none">• <code>dot1p_list</code>—dot1p name (up to 63 characters)• <code>tc</code>—Traffic class number (0 to 7)
Modes	QOS-MAP
Usage	Use the <code>dot1p</code> command to configure a dot1p-to-traffic class map. To separate individual dot1p values and dot1p ranges, use a hyphen (-) or comma (,) ; for example, 0,2-7.
Examples	<pre>sonic# configure terminal sonic(config)# qos map dot1p-tc test sonic(config-dot1p-tc-map-test)# dot1p 1 traffic-class 0 sonic(config-dot1p-tc-map-test)# dot1p 2 traffic-class 0 sonic(config-dot1p-tc-map-test)# dot1p 3 traffic-class 1</pre> <pre>sonic# configure terminal sonic(config-dot1p-tc-map-test)# no dot1p 1 traffic-class 0 sonic(config-dot1p-tc-map-test)# no dot1p 2 traffic-class 0 sonic(config-dot1p-tc-map-test)# no dot1p 3 traffic-class 1</pre>
Releases	4.0 or later

dot1x pae

Sets the dot1x role for an interface.

Command	dot1x pae {authenticator none}
Options	<ul style="list-style-type: none">• authenticator—Enable Authenticator mode• none—Disable Authenticator mode

Modes	INTERFACE
--------------	-----------

Usage	The port can serve either as an authenticator or none. The default setting is none.
--------------	---

Examples	<pre>sonic# configure terminal sonic(config)# interface Ethernet1 sonic(config-if-Ethernet1)# dot1x pae authenticator</pre>
-----------------	---

Releases	4.0 or later
-----------------	--------------

dot1x system-auth-control

Enables the dot1x authentication support on the switch.

Command	dot1x system-auth-control
----------------	---------------------------

Options	None
----------------	------

Modes	CONFIGURATION
--------------	---------------

Usage	When dot1x authentication is disabled, the dot1x configuration is retained and can be changed, but is not activated.
--------------	--

Examples	<pre>sonic# configure terminal sonic(config)# dot1x system-auth-control</pre>
-----------------	---

<pre>sonic# configure terminal sonic(config)# no dot1x system-auth-control</pre>
--

Releases	4.0 or later
-----------------	--------------

dot1x timeout

Configures dot1x timers on an interface.

Command	dot1x timeout {quiet-period <i>quiet-period</i> server-timeout <i>server-timeout</i> }
----------------	--

Options	<ul style="list-style-type: none">• quiet-period <i>quiet-period</i>—Enter a value in seconds (1-65535; default 60).• server-timeout <i>server-timeout</i>—Enter a value in seconds (1-65535; default 30).
----------------	---

Modes	INTERFACE
--------------	-----------

Usage	The <i>quiet-period</i> is the time during which dot1x does not attempt to acquire a supplicant. During the <i>quiet-period</i> , the authenticator state machine remains in HELD state. The <i>server-timeout</i> is the time used by dot1x to time out the authentication server.
--------------	---

Examples	<pre>sonic (config-if-Eth1/1)# dot1x timeout quiet-period 400 sonic (config-if-Eth1/1)# dot1x timeout server-timeout 400</pre>
-----------------	--

Releases	4.1.0 or later
-----------------	----------------

downstream all-mclag

Sets downstream ports.

Command	downstream all-mclag
Options	None
Modes	LINK-TRACK
Usage	Use this command to enable link tracking for downstream links. Use link state tracking to allow traffic from downstream links to be sent to an MCLAG peer if all upstream links on the local switch are down. Downstream MLAG interfaces on the local switch are shut down. Upstream links on the MLAG peer transmit traffic to the spine. Link state tracking avoids the need to increase bandwidth on the peer link to handle the additional upstream traffic.
Examples	<pre>sonic(config) # link state track track1 sonic(config-link-track) # downstream all-mclag sonic(config-link-track) # exit</pre> <pre>sonic(config-link-track) # no downstream all-mclag</pre>
Releases	3.0 or later

downstream all-evpn-es

Associates all downstream EVPN multihoming interfaces to a link track group.

Command	downstream all-evpn-es
Options	None
Modes	LINK-TRACK
Usage	The downlink interfaces on an EVPN multihomed VTEP are shut down if all uplink interfaces on the VTEP go down. To create a link-state track group, use the link state track command.
Examples	<pre>sonic(config) # link state track trackGrp sonic(config-link-track) # downstream all-evpn-es</pre>
Releases	4.2.0 or later

drop-monitor

Enters drop-monitor configuration mode.

Command	drop-monitor [<i>flows-name</i>]
Options	<i>flows-name</i> — Select min or none
Modes	<ul style="list-style-type: none">• TAM• DROP-MONITOR
Usage	The <i>flows-name</i> option only applies to DROP-MONITOR mode.

Examples

```
sonic(config-tam) # drop-monitor  
  
sonic(config-switch-resource) # drop-monitor flows min  
  
sonic(config-tam) # no drop-monitor  
  
sonic(config-switch-resource) # no drop-monitor flows
```

Releases

3.0 or later

dropcounters

Configure drop counters.

Command`dropcounters counter-name`**Options**

counter-name — Drop counter name (up to 32)

Modes

CONFIGURATION

Usage

This command enables the drop counters. The counter name must begin with alpha numeric character.

Examples

```
sonic# configure terminal  
sonic(config)# dropcounters drop1  
sonic(config-dropcounters-drop1) #  
  
sonic(config) # no dropcounters drop1
```

Releases

4.0 or later

dscp

Adds DSCP to the traffic class entry in the map.

Command`dscp dscp_list {traffic-class tc}`**Options**

- *dscp_list*—DSCP name (up to 63 characters)
- *tc*—Traffic class number

Modes

QOS-MAP DSCP-TC *name*

Usage

Use this command to configure DSCP to traffic class-map. Use hyphen (-) or comma (,) separated individual DSCP and ranges of DSCP. For example, 0, 2-16, 63.

Examples

```
sonic# configure terminal  
sonic(config)# qos map dscp-tc  
sonic(config-tc-dscp-map-tc1) # dscp 1 traffic-class 0  
sonic(config-tc-dscp-map-tc1) # dscp 2 traffic-class 0  
sonic(config-tc-dscp-map-tc1) # dscp 3 traffic-class 1  
  
sonic# configure terminal  
sonic(config) # no dscp 1 traffic-class 0  
sonic(config) # no dscp 2 traffic-class 0  
sonic(config) # no dscp 3 traffic-class 1
```

Releases

4.0 or later

duplex

Configures duplex mode.

Command	<code>duplex {full half}</code>
Options	<code>full/half</code> —Duplex mode configuration of the interface
Modes	<ul style="list-style-type: none">• INTERFACE <i>phy-if-name</i>• INTERFACE RANGE
Usage	Half-duplex is supported on N3248X-ON, N3248PXE-ON, and E3248PXE-ON switches at 10 Mbps, 100 Mbps, and 1Gbps speeds.
	<p>(i) NOTE: The value of the duplex configured in that particular interface is displayed in the <code>show interface Ethernet <port></code> command. When the interface is configured with no <code>duplex</code> command, both full and half-duplex are negotiated, and the link is established based on the peer-end duplex configuration, but the <code>show interface Ethernet <port></code> command output does not have a duplex field.</p>
Examples	<pre>sonic# configure terminal sonic(config)# interface Ethernet1 sonic(config-if-Eth1)# duplex half</pre>
Releases	4.1.0 or later

dup-addr-detection

Configures the threshold for address moves.

Command	<code>dup-addr-detection [max-moves] {nummoves {time timevalue}}</code>
Options	<ul style="list-style-type: none">• <code>nummoves</code> — Number of moves (2 to 1000; default 5)• <code>timevalue</code> — Time in seconds (2 to 1800; default 180)
Modes	BGP-ADDRESS-FAMILY
Usage	Use this command to configure threshold address moves including maximum moves allowed and maximum time interval.
Examples	<pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# address-family l2vpn evpn sonic(config-router-bgp-af)# dup-addr-detection max-moves 10 time 1200 sonic(config-router-bgp-af)# no dup-addr-detection max-moves 10 time 1200</pre>
Releases	3.0 or later

dup-addr-detection freeze

Configures duplicate address detection.

Command	<code>dup-addr-detection freeze {permanent time}</code>
Options	<code>time</code> — Amount of time to freeze in seconds (30 to 3600; default 180)
Modes	BGP-ADDRESS-FAMILY
Usage	Use this command to configure the action to be taken on duplicate address detection. You can configure freezing the address permanently or for a specified duration.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # address-family l2vpn evpn
sonic(config-router-bgp-af) # dup-addr-detection freeze permanent
```

```
sonic(config-router-bgp-af) # no dup-addr-detection freeze permanent
```

Releases

3.0 or later

E, F, and G commands

Topics:

- ebgp-multipath
- echo-interval
- echo-mode
- ecn
- enable
- encapsulation dot1q vlan-id
- end
- enforce-first-as
- enforce-multipath
- enterprise-id
- entry
- errdisable recovery cause
- errdisable recovery interval
- es-activation-delay
- evpn esi-multipathing
- evpn ethernet-segment
- exit
- external-ip
- fabric-external
- factory default profile
- fast-convergence
- fast-external-failover
- fast-reboot
- fec
- filter-list
- flow-group
- forwarding-fbs
- frequency
- graceful-restart
- graceful-restart enable
- graceful-restart helper enable
- graceful-restart helper strict-lsa-checking
- graceful-restart helper supported-grace-time
- graceful-restart helper planned-only
- graceful-restart preserve-fw-state
- graceful-restart restart-time
- graceful-restart stalepath-time
- graceful-shutdown (BGP)
- graceful-shutdown (Port Channel)
- green
- group

ebgp-multipath

Allows eBGP neighbors on indirectly connected networks.

Command	<code>ebgp-multipath [hop-count]</code>
Options	<code>hop-count</code> — (Optional) Maximum number of hops allowed to communicate with a peer in a remote network (1 to 255; default 255 for eBGP)
Modes	<ul style="list-style-type: none">• BGP-ADDRESS-FAMILY• BGP-PEER-GROUP
Usage	Use this command to configure a peer-group with eBGP neighbors as members that are multiple hops away. You can optionally set the maximum hops that BGP neighbors in peer-group can be apart. This command avoids installation of default multi-hop peer routes to prevent loops and creates neighbor relationships between peers. Networks indirectly connected are not valid for best-path selection.
Examples	<pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# peer-group PG_Ext sonic(config-router-bgp-pg)# ebgp-multipath 10 sonic(config-router-bgp-pg)# no ebgp-multipath 10</pre>
Releases	3.0 or later

echo-interval

Configures the echo packet transmit interval for a bi-directional forwarding detection (BFD) peer.

Command	<code>echo-interval echo_interval</code>
Options	<code>echo_interval</code> —Echo packet transmit interval in milliseconds (10 to 60000; default is 50)
Modes	<ul style="list-style-type: none">• PEER• BFD PROFILE
Usage	Use this command to configure the minimum transmission interval that this switch wants to use to send BFD echo packets.
Example	Example for PEER mode: <pre>sonic# configure terminal sonic(config)# bfd sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0 sonic(config-bfd-peer)# echo-interval 11</pre> Example for PROFILE mode: <pre>sonic# configure terminal sonic(config)# bfd sonic(config-bfd)# profile fast sonic(config-bfd-profile)# echo-interval 11</pre>
Releases	3.0 or later

echo-mode

Enables echo-mode for a bidirectional forwarding detection (BFD) peer.

Command	<code>echo-mode</code>
Options	None

Modes

- PEER
- BFD PROFILE

Usage

Use this command to enable echo mode for BFD single-hop peer. Echo mode is not supported for multihop peers. By default, Echo mode is disabled for a BFD peer.

Examples

Example for PEER mode:

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0  
sonic(config-bfd-peer)# echo-mode
```

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0  
sonic(config-bfd-peer)# no echo-mode
```

Example for PROFILE mode:

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# profile fast  
sonic(config-bfd-profile)# echo-mode
```

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# profile fast  
sonic(config-bfd-profile)# no echo-mode
```

```
sonic(config-bfd-peer)# no echo-mode
```

Releases

3.0 or later

ecn

Enables Explicit Congestion Notification (ECN) based on color.

Command

```
ecn [none | green]
```

Options

- none—Disables ECN
- green—Enables ECN for green alone

Modes

WRED-WRED

Usage

Use this command to enable ECN in WRED policy for early detection and management of queue congestion.

Examples

```
sonic(config-wred-wred-green)# ecn green
```

```
sonic(config-wred-wred-green)# no ecn
```

Releases

3.1 or later

enable

Activates the IFA feature.

Command

```
enable
```

Options

None

Modes

- TAM-IFA
- TAM-DM
- TAM-TS

Usage

IFA activated switches act as intermediate nodes for all IFA-tagged flows transiting the switch.

Examples

```
sonic(config) # tam
sonic(config-tam) # ifa
sonic(config-tam-if) # enable
sonic(config-tam-if) # end
sonic# show tam ifa
Status : Active
Switch ID : 9876
Enterprise ID : 8798
Version : 2.0
Number of sessions : 0
Number of collectors : 0
```

```
sonic(config-tam-dm) # enable
sonic(config-tam-dm) # end
sonic# show tam drop-monitor
Status : Active
Switch ID : 9876
Number of sessions : 2
Number of collectors : 1
Aging Interval : 30
```

```
sonic(config) # tam
sonic(config-tam) # tail-stamping
sonic(config-tam-ts) # enable
sonic(config-tam-ts) # end
sonic# show tam tail-stamping
Status : Active
Switch ID : 9876
Number of sessions : 0
```

```
sonic(config-if-nat) # no enable
sonic(config-tam-dm) # no enable
sonic(config-tam-ts) # no enable
```

Releases

3.0 or later

encapsulation dot1q vlan-id

Configures the dot1q VLAN ID.

Command `encapsulation dot1q vlan-id vlanid`

Options `vlanid` — VLAN ID (1 to 4094)

Modes SUB INTERFACE

Usage Use this command to configure a Ethernet or PortChannel sub dot1q VLAN ID.

Example

```
sonic (config) # interface Ethernet 80.1
```

```
sonic (config-subif-Ethernet80.1) encapsulation dot1q vlan-id 10
```

Releases

3.2 or later

end

Returns to EXEC mode from any other command mode.

Command	end
Options	None
Modes	All
Usage	Use the end command from any mode to return to EXEC mode.
Examples	<pre>sonic# configure terminal sonic(config)# bfd sonic(config-bfd)# end sonic#</pre>
Releases	3.0 or later

enforce-first-as

Enforces the first AS in the AS path of the route received from an eBGP peer to be the same as the configured remote AS.

Command	enforce-first-as
Options	None
Modes	<ul style="list-style-type: none">• BGP-NEIGHBOR• BGP-PEER-GROUP
Usage	Use this command to enforce that first AS in as-path of route received from an eBGP peer must be the peer's local AS number. If routes are rejected, the session is reset. In the event of a failure, the existing BGP sessions flap. For updates received from eBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer, otherwise the update drops and the counter increments.
Examples	<pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# neighbor 30.30.30.3 sonic(config-router-bgp-neighbor)# enforce-first-as</pre> <pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# peer-group PG_Ext sonic(config-router-bgp-pg)# enforce-first-as</pre> <pre>sonic(config-router-bgp-neighbor)# no enforce-first-as sonic(config-router-bgp-pg)# no enforce-first-as</pre>
Releases	3.0 or later

enforce-multipath

Configures eBGP neighbors or neighbors in a peer-group to perform multi-hop.

Command	enforce-multipath
Options	None
Modes	<ul style="list-style-type: none">• BGP-NEIGHBOR• BGP-PEER-GROUP
Usage	None

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# enforce-multipath
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# enforce-multipath
```

```
sonic(config-router-bgp-neighbor)# no enforce-multipath
sonic(config-router-bgp-pg)# no enforce-multipath
```

Releases

3.0 or later

enterprise-id

Configures a 32-bit identifier used in IPFIX telemetry reports.

Command `enterprise-id id`

Options `id` — Identifier (1 to 4294967295)

Command mode TAM

Usage When not configured, the last 16-bits from the system MAC address are used. Use [show tam switch](#) to view the TAM device configuration.

Examples

```
sonic(config)# tam
sonic(config-tam)# enterprise-id 5678
sonic(config-tam)# exit
sonic(config)# exit
sonic# show tam switch
TAM Device information
-----
Switch ID      : 1234
Enterprise ID  : 5678
```

```
sonic(config-tam)# no enterprise-id
```

Releases

3.1 or later

entry

Configures the next-hop group member at a specified index.

Command `entry index next-hop ip-address [vrf vrf-name | default] [non-recursive | overlay | recursive] [single-copy]`

Options

- `entry-index`—Index entry
- `ip-address`—IP address in A::B format
- `vrf-name`—VRF name prefixed by Vrf (up to 15 characters)
- `non-recursive`—(Optional) Next hop must be nonrecursively resolved through an underlay interface
- `overlay`—(Optional) Next hop must be reachable through an overlay interface
- `recursive`—(Optional) Next hop must be recursively resolved through an underlay interface
- `single-copy`—(Optional) Enable a single path to create copy

Modes

- PBF-NEXT-HOP
- PBF-REPLICATION-GROUP

Usage

If recursive, non-recursive, or overlay is not specified and then the next-hop can be reachable by any means. The single-copy option is applicable only on PBF REPLICATION GROUP. This option

disables replication of the packet to the path and pick one path to create a copy to send to an ECMP-reachable path.

Examples

```
sonic(config) # pbf replication-group rps type ip
sonic(config-pbf-ip-repl-group) # entry 1 next-hop 1.1.1.1 recursive
single-copy
```

Releases

3.2 or later

errdisable recovery cause

Enables error disable recovery for the specific cause.

Command

```
errdisable recovery cause {bpdukguard | link-flap | udld}
```

Options

- **udld** — Enables a timer to recover from the unidirectional link detection (UDLD) error disabled state
- **bpdukguard** — Enables a timer to recover from bridge protocol data unit (BPDU) guard error disable state
- **link-flap** — Enables error disable for link-flaps

Modes

CONFIGURATION

Usage

The **bpdukguard** option only applies to STP-enabled ports. The command takes effect only when BPDU guard is configured on a port and **errdisable detect cause bpdukguard** is enabled. When the recovery option is enabled, the port is brought up after the recovery timer expires. When the recovery option is disabled, the port is shut down indefinitely. You must manually bring up the port using **shutdown** and **no shutdown**.

Examples

```
sonic(config) # errdisable recovery cause bpdukguard
```

```
sonic(config) # no errdisable recovery cause bpdukguard
```

Releases

3.1 or later

errdisable recovery interval

Configures the error disable recovery interval in seconds.

Command

```
errdisable recovery interval interval
```

Options

interval — Error disable recovery interval in seconds (30 to 65535; default 300)

Modes

CONFIGURATION

Usage

This command applies only to STP-enabled ports. The command takes effect only when the BPDU guard is configured on a port. The recovery timer value is applicable only for shutdown case. The recovery timer starts whenever there is a BPDU guard violation.

Examples

```
sonic(config) # errdisable recovery interval 200
```

```
sonic(config) # no errdisable recovery interval
```

Releases

3.1 or later

es-activation-delay

Configures the delay time used to enable packet forwarding on an Ethernet Segment port channel after the PortChannel comes up.

Command	<code>es-activation-delay milliseconds</code>
Options	<code>milliseconds</code> — Enter the delay time in milliseconds (0-1200000; default 0) for Ethernet segment activation.
Modes	EVPN ETHERNET-SEGMENT
Usage	By default, the ES activation time is disabled (default 0) for faster convergence. Configuring a higher ES activation value minimizes the risk of transient loops or packet duplication during DF election.
Examples	<pre>sonic(config) # evpn esi-multipathing sonic(config-evpn-esi-mh) # es-activation-delay 5000</pre>
Releases	4.4.0 or later

evpn esi-multipathing

Enters EVPN Multihoming mode to configure global multihoming settings.

Command	<code>evpn esi-multipathing</code>
Options	None
Modes	CONFIGURATION
Usage	In EVPN Multihoming mode, you can configure optional global multihoming settings, such as the startup delay time allowed during VTEP bootup (startup delay), hold-time for learned MAC addresses (mac-holdtime), and hold-time for learned ARP/ND entries (neigh-holdtime). To reset global multihoming settings to their default values, enter the <code>no evpn esi-multipathing</code> command.
Examples	<pre>sonic(config) # evpn esi-multipathing</pre>
Releases	4.2.0 or later

evpn ethernet-segment

Configures the Ethernet segment ID (ES-ID) on a multihomed VTEP.

Command	<code>evpn ethernet-segment {XX:XX:XX:XX:XX:XX:XX:XX:XX:XX} auto-lacp auto-system-mac</code>
Options	<ul style="list-style-type: none"><code>XX:XX:XX:XX:XX:XX:XX:XX:XX:XX</code> — Configures a Type-0 ES-ID. Enter a 9-byte ID with the type byte set to 0; for example, <code>00:00:00:00:00:00:00:0a:00:01</code>.<code>auto-lacp</code> — Automatically configures a Type-1 ES-ID from the LACP peer's MAC address.<code>auto-system-mac</code> — Automatically configures a Type-3 ES-ID by combining the system-mac address configured on the port-channel interface and the port-channel number.
Modes	PORT CHANNEL
Usage	Be sure to configure the same ES-ID on each VTEP in an Ethernet segment. Type-0, Type-1, and Type-3 ES-ID types are supported (see RFC 7432). To remove a configured Ethernet segment ID, enter the <code>no evpn ethernet-segment</code> command.
	(i) NOTE: A 10-byte Type-3 ES-ID is generated by concatenating the 1-byte Type=0x03, 6-byte System MAC, and the 3-byte Ethernet-segment number.

i **NOTE:** In addition to the Ethernet segment ID, a System MAC address is always required in an EVPN Ethernet segment configuration.

i **NOTE:** If MLAG is already configured on a multihomed VTEP, an EVPN Ethernet segment configuration is not supported. Similarly, if an EVPN Ethernet segment is already configured on one or more port-channel interfaces, MLAG configuration is not supported.

Examples

Type-0 ES-ID:

```
sonic(config) # interface PortChannel1
sonic(config-if-pol1) # evpn ethernet-segment 00:00:00:00:00:00:00:0a:00:01
sonic(config-if-pol1) # system-mac 00:00:00:0a:00:01
```

Type-1 ES-ID:

```
sonic(config) # interface PortChannel1
sonic(config-if-pol1) # evpn ethernet-segment auto-lACP
sonic(config-if-pol1) # system-mac 00:00:00:0a:00:01
```

Type-3 ES-ID:

```
sonic(config) # interface PortChannel1
sonic(config-if-pol1) # evpn ethernet-segment auto-system-mac
sonic(config-if-pol1) # system-mac 00:00:00:0a:00:01
```

Releases

4.2.0 or later

exit

Return to the next higher command mode.

Command

exit

Options

None

Modes

All

Usage

Use this command to navigate back to the primary mode from a submode. When you want to come out of configuration mode, enter the end command.

Examples

```
sonic# configure terminal
sonic(config) # bfd
sonic(config-bfd) # exit
sonic(config) #
```

Releases

3.0 or later

external-ip

Configures the external IPv4 address on a border leaf VTEP.

Command

external-ip {ipv4-address | Loopback number}

Options

- *ipv4-address* — Enter an IPv4 address in A.B.C.D format. An IPv6 address is not supported as an external IP address for multisite DCI.
- *Loopback number* — Enter a loopback ID number (0 - 16383). The loopback interface must be configured with an IPv4 address.

Modes

INTERFACE-VXLAN-VTEP

Usage

An external IP address is required when you configure a border leaf VTEP in multisite DCI. In a multisite DCI installation, configure a separate source and external IP address on each border leaf VTEP to

distinguish between internal and external VXLAN tunnels. If you specify a loopback number, the loopback interface must be configured with an IPv4 address. You cannot reconfigure or delete a loopback IP address if it is being used as the external IP address on a VXLAN VTEP. You can reconfigure or delete an external IP address "on the fly" on a border leaf VTEP if VLAN- or VRF-to-VNI mapping is configured.

Examples

```
sonic(config)# interface vxlan vtep1  
sonic(config-if-vxlan-vtep1)# external-ip 1.1.1.2
```

```
sonic(config)# interface vxlan vtep1  
sonic(config-if-vxlan-vtep1)# no external-ip 1.1.1.2
```

```
sonic(config)# interface vxlan vtep2  
sonic(config-if-vxlan-vtep2)# external-ip Loopback 10
```

Releases

4.1.0 or later

fabric-external

Configures a BGP neighbor as a fabric-external neighbor.

Command

fabric-external

Options

None

Modes

ADDRESS-FAMILY

Usage

Use this command to enable next-hop rewrite for a fabric-external neighbor in the case of a multi-site configuration.

Examples

Example configures neighbor 20.20.20.2 as fabric external

```
sonic# configure terminal  
sonic(config)# router bgp 100  
sonic(config-router-bgp)# neighbor 20.20.20.2  
sonic(config-router-bgp-neighbor)# remote-as 300  
sonic(config-router-bgp-neighbor)# address-family l2vpn evpn  
sonic(config-router-bgp-neighbor-af)# fabric-external
```

```
sonic(config-router-bgp-neighbor-af)# no fabric-external
```

Example configures peer-group neighbors as fabric external

```
sonic# configure terminal  
sonic(config)# router bgp 100  
sonic(config-router-bgp)# peer-group PG_Int  
sonic(config-router-bgp-pg)# address-family l2vpn evpn  
sonic(config-router-bgp-pg-af)# fabric-external
```

```
sonic(config-router-bgp-pg-af)# no fabric-external
```

Releases

4.0 or later

factory default profile

Sets the factory default configuration profile.

Command

factory default profile {12 | 13}

Options

- 12 — Apply the L2 switch configuration profile.
- 13 — Apply the L3 switch configuration profile (default).

Modes	CONFIGURATION
Usage	To optimize the switch for L2 and L3 deployments, Enterprise SONiC supports an L2 switch and an L3 router configuration profile. The <code>factory default profile</code> command removes the currently running switch configuration and creates a new startup configuration file, using the specified configuration profile. The newly created startup configuration is applied as part of this command. Entering the <code>factory default profile</code> command restarts all Enterprise SONiC application services and may result in a loss of switch connectivity.

Example

```
sonic# configure terminal
sonic(config)# factory default profile 12
Device configuration will be erased. You may lose connectivity.
Continue? [y/N]: y
Applying factory default configuration.
This may take 120--180 seconds and also result in a reboot.
sonic(config)#

```

Releases

3.1 or later

fast-convergence

Enables fast convergence between MLAG peers.

Command	<code>fast-convergence</code>
Options	None
Modes	MCLAG-DOMAIN
Usage	When the MLAG port channel is activated, traffic is enabled on the port channel only after an acknowledgment is received from another MLAG peer. This method prevents transient duplicate packets but introduces an additional delay in convergence. This command enables traffic on the port channel immediately after the port channel is initiated. This command can be used to speed up convergence process when bringing up the port channel, although it may result in transient duplicate packets for a short period. By default, it is disabled.

Examples

```
sonic(config-mlag-domain-100) # fast-convergence
```

Releases

4.2.0 or later

fast-external-failover

Causes BGP to take down eBGP peers immediately when a link flaps.

Command	<code>fast-external-failover</code>
Options	None
Modes	ROUTER-BGP
Usage	Use this command to control how sensitive eBGP neighborship is to the underlying link failure.
Examples	<pre>sonic(config) # router bgp 65300 sonic(config-router-bgp) # fast-external-failover</pre>

```
sonic(config-router-bgp) # no fast-external-failover
```

Releases

3.0 or later

fast-reboot

Enables a switch to reboot quickly with minimum disruptions to the data plane and packet forwarding.

Command	fast-reboot [options]
Options	None
Modes	EXEC
Usage	Use this command to minimize traffic disruption in data center networking operation during infrastructure maintenance and upgrades.
Examples	<pre>sonic# fast-reboot</pre>
Releases	3.1 or later

fec

Configures forward error correction (FEC).

Command	fec fec
Options	<code>fec</code> — FEC mode; select FC, RS, or off
Modes	<ul style="list-style-type: none">• FC — Enables FEC on supported interfaces. FC stands for fire code.• RS—Enables FEC on supported interfaces. RS stands for Reed-Solomon code.• none—Disables FEC on an interface.
Command mode	INTERFACE
Usage	By default, FEC is not enabled on an interface, except for 400G, 4x100G, 1x200G and 2x200G interfaces on which FEC RS is enabled. Use this command to configure FEC on 25G and 100G interfaces. The <code>no fec</code> command resets FEC to its default value.
Examples	<pre>sonic(config-if)# fec fc</pre> <pre>sonic(config-if)# no fec</pre>
Releases	3.1 or later

filter-list

Configures a filter list for a BGP neighbor or peer-group.

Command	filter-list <i>fname</i> {in out}
Options	<i>fname</i> — Filter-list name
Modes	<ul style="list-style-type: none">• NEIGHBOR-ADDRESS-FAMILY• PEER-GROUP-ADDRESS-FAMILY
Usage	Use this command to define policy (route filtering) for a BGP neighbor or peer-group in outbound or/and inbound direction.
Examples	<pre>sonic(config)# router bgp 100</pre> <pre>sonic(config-router-bgp)# neighbor 20.20.20.2</pre> <pre>sonic(config-router-bgp-neighbor)# remote-as 300</pre>

```

sonic(config-router-bgp-neighbor) # address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af) # filter-list fl_allow_remote in

sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # filter-list fl_allow_remote in

sonic(config-router-bgp-neighbor-af) # no filter-list fl_allow_remote in
sonic(config-router-bgp-pg-af) # no filter-list fl_allow_remote in

```

Releases

3.0 or later

flow-group

Configures flow group by specifying a set of match criteria that defines a set of flows.

Command `flow-group name [src-ip src_ip] [dst-ip dst_ip] [l4-src-port l4_src_port] [l4-dst-port l4_dst_port] [priority priority_value] [protocol protocol_value]`

Options

- *name* — Flow-group name
- *src_ip* — (Optional) Source IP in A.B.C.D/mask or A::B format
- *dst_ip* — (Optional) Destination IP in A.B.C.D/mask or A::B format
- *l4_src_port* — (Optional) L4 source port
- *l4_dst_port* — (Optional) L4 destination port
- *priority_value* — (Optional) Priority value to match
- *protocol_value* — (Optional) Protocol value to match; UDP or TCP

Command modes

- INTERFACE
- TAM

Usage

Use [show tam flowgroups](#) to view the TAM flow group configuration.

Examples

```

sonic(config-tam)# flow-group f9 type ipv4 src-ip 192.1.2.3 dst-ip 172.6.5.4
sonic# show tam flowgroups
Flow Group Name      : f9
  Id                 : 60
  Priority          : 100
  SRC IP            : 192.1.2.3/32
  DST IP            : 172.6.5.4/32
  Packet Count       : 5432
Flow Group Name      : DEMO
  Id                 : 1
  Priority          : 100
  SRC IP            : 1.1.1.1/32
  DST IP            : 4.4.4.4/32
  Packet Count       : 454

sonic(config)# interface Ethernet 46
sonic(config-if-Ethernet46)# flow-group f1
sonic(config-if-Ethernet46)# end
sonic# show tam flowgroups
Flow Group Name      : DEMO
  Id                 : 1
  Priority          : 100
  SRC MAC           : 11:22:33:44:55:66
  SRC IP            : 1.1.1.1/32
  DST IP            : 4.4.4.4/32
  Packet Count       :
Flow Group Name      : f88
  Id                 : 409
  Priority          : 100
  SRC IP            : 1.1.1.1/32
  DST IP            : 5.5.5.5/32
  Packet Count       :
Flow Group Name      : f1
  Id                 : 717
  Priority          : 100
  SRC MAC           : 00:00:00:00:00:01
  DST MAC           : 00:00:00:00:00:02

```

```
    SRC IP          : 3.3.3.3/32
    DST IP          : 4.4.4.4/32
    Ingress Intf   : Ethernet46
    Packet Count    :

sonic(config-tam)# no flow-group f9
```

Releases 3.1 or later

forwarding-fbs

Configures key-profile for forwarding flow-based-services.

Command `forwarding-fbs {egress | ingress} key-profile {ip | ipv4 | ipv6 | l2 | 12-ipv4}`

Options

- egress—egress direction
- ingress—ingress direction
- ip—IPv4 and IPv6 key-profile
- ipv4—IPv4 key-profile
- ipv6—IPv6 key-profile
- l2—L2 key-profile
- l2-ipv4—L2 and IPv4 key-profile

Modes TCAM

Usage This command enables a predefined set of keys for forwarding flow-based services. This preallocates the qualifiers required for hardware programming.

Examples

```
sonic# configure terminal
sonic(config)# hardware
sonic(config-hardware)# tcam
sonic(config-hardware-tcam)# forwarding-fbs ingress key-profile ip
```

Releases 4.0 or later

frequency

Configures the frequency of a probe for an IP SLA instance.

Command `frequency frequency-value`

Options `freq-value`—Frequency value.

Modes IP-SLA

Usage The range is from one to 300. The default value is 30 seconds.

Examples

```
sonic(config)# ip sla 10
sonic(config-ipsla-10)# frequency 45
```

```
sonic(config-ipsla-10)# no frequency
```

Releases 3.1 or later

graceful-restart

Configure Graceful Restart (RFC 3623) restarting support and the grace period on the device that has to be restarted.

Command	graceful-restart [grace-period <i>grace-period</i>]
Options	<i>grace-period</i> —The grace period before which the neighbors or helpers deem the restarting node dead. The range is from 1 to 1800 seconds. The default grace period is 120 seconds.
Modes	<ul style="list-style-type: none">• ROUTER-OSPF• ROUTER-BGP
Usage	By default, graceful restart is disabled on an OSPF and BGP router. This configuration enables or disables restart support on the router.
Examples	<pre>sonic(config)# router ospf 10 sonic(config-router-ospf)# graceful-restart grace-period 150</pre>
Releases	4.1.0 or later

graceful-restart enable

Enables graceful restart for an instance of BGP.

Command	graceful-restart enable
Options	None
Modes	ROUTER-BGP
Usage	Use this command to enable BGP graceful restart globally in an instance of BGP. Changing the graceful restart parameter will take effect only on the fly, and will not take effect immediately. It will require all the BGP neighbors to be reset to take effect. This is because graceful restart capability must be negotiated with neighbors to make this feature functional.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# graceful-restart enable</pre> <pre>sonic(config-router-bgp)# no graceful-restart enable</pre>
Releases	3.0 or later

graceful-restart helper enable

Configure graceful restart (RFC 3623) helper support on helping neighbor devices.

Command	graceful-restart helper enable [<i>router-id</i>]
Options	<i>router-id</i> —Configure graceful restart helper support for a specific neighbor using the router ID.
Modes	ROUTER-OSPF
Usage	By default, helper support is disabled for all neighbors. This configuration enables or disables helper support on this router for all neighbors.
Examples	<pre>sonic(config)# router ospf 10 sonic(config-router-ospf)# graceful-restart helper enable</pre> <pre>sonic(config-router-ospf)# graceful-restart helper enable 10.1.2.3</pre>

Releases	4.1.0 or later
-----------------	----------------

graceful-restart helper strict-lsa-checking

Configures strict LSA checking for the helper node.

Command	graceful-restart helper strict-lsa-checking
Modes	ROUTER-OSPF
Usage	If this command is configured, the helper cancels graceful restart when an LSA change occurs, which affects the restarting router. By default, strict LSA checking is enabled. To disable strict LSA checking, use the no form of the command.

Examples

```
sonic# configure terminal  
sonic(config)#router ospf  
sonic(config-router-ospf)# graceful-restart helper strict-lsa-checking
```

Releases	4.1.0 or later
-----------------	----------------

graceful-restart helper supported-grace-time

Configure the grace time on the helper node.

Command	graceful-restart helper supported-grace-time <i>grace-time</i>
Options	<i>grace-time</i> —Configure the grace time (10 to 1800 seconds; default is 120).
Modes	ROUTER-OSPF
Usage	This configuration determines the time bound for the helper node to support graceful restart.
Examples	<pre>sonic(config)# router ospf 10 sonic(config-router-ospf)# graceful-restart helper supported-grace-time</pre>

Releases	4.1.0 or later
-----------------	----------------

graceful-restart helper planned-only

Configure helper support for only planned restarts.

Command	graceful-restart helper planned-only
Modes	ROUTER-OSPF
Usage	By default, helper supports both planned and unplanned restarts.
Examples	<pre>sonic(config)# router ospf 10 sonic(config-router-ospf)# graceful-restart helper planned-only</pre>

Releases	4.1.0 or later
-----------------	----------------

graceful-restart preserve-fw-state

Configures BGP to preserve forwarding state during graceful restart for an instance of BGP.

Command	graceful-restart preserve-fw-state
Options	None

Modes	ROUTER-BGP
Usage	Use this command to enable BGP to preserve forwarding state of BGP during graceful restart.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# graceful-restart preserve-fw-state</pre> <pre>sonic(config-router-bgp)# no graceful-restart preserve-fw-state</pre>
Releases	3.0 or later

graceful-restart restart-time

Configures the restart timer interval for BGP.

Command	<code>graceful-restart restart-time <i>restart-time</i></code>
Options	<i>restart-time</i> — Restart time in seconds (default 120)
Modes	ROUTER-BGP
Usage	Use this command to configure the BGP restart timer interval in seconds. This is optional parameter and determines how long peer routers will wait to delete stale routes before a BGP open message is received. The default value is 120 seconds.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# graceful-restart restart-time 180</pre> <pre>sonic(config-router-bgp)# no graceful-restart restart-time 180</pre>
Releases	3.0 or later

graceful-restart stalepath-time

Configures the stale path timer interval for BGP.

Command	<code>graceful-restart stalepath-time <i>stalepath-time</i></code>
Options	<i>stalepath-time</i> — Stale path time in seconds (default 360)
Modes	ROUTER-BGP
Usage	Use this command to set the maximum time to hold on to the stale paths of a gracefully restarted peer. All stale paths are deleted after the expiration of this timer. This is an optional parameter, and the default is 360 seconds.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# graceful-restart stalepath-time 300</pre> <pre>sonic(config-router-bgp)# no graceful-restart stalepath-time 300</pre>
Releases	3.0 or later

graceful-shutdown (BGP)

Enables the graceful shutdown feature.

Command	<code>graceful shutdown</code>
----------------	--------------------------------

Options	None
Modes	ROUTER-BGP
Usage	Use this command to gracefully remove a BGP router from service. This command will instruct BGP to enter into graceful shutdown mode by resending routes with GSHUT community to all neighbors. This will enable all neighbors to route traffic around it so that the router can be taken out of service without impact data forwarding.
Examples	<pre>sonic(config) # router bgp 65300 sonic(config-router-bgp) # graceful-shutdown</pre> <pre>sonic(config-router-bgp) # no graceful-shutdown</pre>
Releases	3.0 or later

graceful-shutdown (Port Channel)

Enables graceful shutdown on a specified port channel.

Command	graceful-shutdown
Options	None
Modes	PORT-CHANNEL CONFIGURATION
Usage	If you enable graceful shutdown, the port channel is brought DOWN (operationally), regardless of the global port-channel graceful shutdown setting — see portchannel graceful-shutdown . If you disable graceful shutdown, the port channel exits graceful shutdown mode and no longer shuts down with no frame loss. To disable port-channel graceful shutdown, enter the no graceful-shutdown command.
Examples	<pre>sonic(config) # interface PortChannel 6 sonic(config-if-po6) # graceful-shutdown</pre>
Releases	4.0.3 or later

green

Configures the WRED minimum, maximum threshold, and drop probability for green color packets.

Command	green minimum-threshold {min-threshold {maximum-threshold max-threshold {drop-probability max-drop-rate}}}
Options	<ul style="list-style-type: none"> • <i>min-threshold</i>—Minimum threshold (1 to 12480) • <i>max-threshold</i>—Maximum threshold (1 to 12480) • <i>max-drop-rate</i>—Maximum drop rate (0 to 100)
Modes	WRED-GREEN
Usage	Use this command to set the bandwidth in KiloBytes (KB) per second allocated to the minimum and maximum threshold values, and the maximum drop rate for the green traffic class.
Example	<pre>sonic(config-wred-wred-green) # green minimum-threshold 100 maximum-threshold 200 drop- probability 50</pre>
Releases	3.1 or later

group

Add drop counter group.

Command	group <i>str</i>
Options	<i>str</i> —Group name of drop counter
Modes	DROPCOUNTERS
Usage	Use this command to add or delete a group to drop counters. For example, you could assign legitimate drop counters to a group named RX_LEGIT. This group is displayed in show dropcounters output. If required, you can assign nonlegitimate drops to a custom drop group.

Examples

```
sonic# configure terminal
sonic(config)# dropcounters drop
sonic(config-dropcounters-drop)# group group1

sonic# configure terminal
sonic(config)# dropcounters drop
sonic(config-dropcounters-drop)# no group
```

Releases

4.0 or later

H and I commands

Topics:

- hardware
- hostname
- icmp-echo
- idle-time
- ifa
- ignore server-key
- ignore session-key
- image firmware install
- image gpg-key key-server key-id
- image install
- image patch install
- image patch rollback
- image remove
- image set-default
- image verify gpg signature
- image verify pki signature
- import vrf
- instance
- interface
- interface CPU
- interface breakout
- interface Loopback
- interface Management
- interface media-fec
- interface-naming
- interface PortChannel
- interface port-locator
- interface range
- interface transceiver diagnostics loopback
- interface transceiver diagnostics pattern
- interface vxlan
- ip access-group
- ip access-list
- ip-acl
- ip address
- ip anycast-address
- ip anycast-address
- ip anycast-mac-address
- ip anycast-mac-address router-mac-for-forwarding
- ip arp
- ip dhcp-relay
- ip dhcp-relay circuit-id
- ip dhcp-relay link-select
- ip dhcp-relay max-hop-count
- ip dhcp-relay policy-action
- ip dhcp-relay source-interface
- ip dhcp-relay vrf-select

- ip dhcp snooping
- ip dhcp snooping trust
- ip dhcp snooping verify mac-address
- ip dhcp snooping vlan
- ip drop-neighbor
- ip drop-neighbor aging-time
- ip forward-protocol udp enable
- ip forward-protocol udp exclude
- ip forward-protocol udp include
- ip forward-protocol udp rate-limit
- ip helper-address
- ip igmp
- ip igmp join
- ip igmp last-member-query-count
- ip igmp last-member-query-interval
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp snooping
- ip igmp version
- ip load-share hash algorithm
- ip load-share hash ingress-port
- ip load-share hash ipv4
- ip load-share hash ipv6
- ip load-share hash offset
- ip load-share hash roce qpn
- ip load-share hash seed
- ip name-server
- ip name-server source-interface
- ip nht
- ip ospf
- ip ospf area
- ip ospf authentication
- ip ospf authentication-key
- ip ospf bfd
- ip ospf bfd profile
- ip ospf cost
- ip ospf dead-interval
- ip ospf hello-interval
- ip ospf message-digest-key
- ip ospf mtu-ignore
- ip ospf network
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- ip pim
- ip pim bfd
- ip pim bfd profile
- ip pim drpriority
- ip pim hello
- ip pim sparse-mode
- ip prefix-list
- ip protocol
- ipv6 protocol
- ip reserve local-neigh
- ip rest
- ip rest authentication

- ip rest cipher-suite
- ip rest security-profile
- ip route
- ip sla
- ip source binding
- ip ssh
- ip ssh client ciphers
- ip ssh client kexalgorithms
- ip ssh client macs
- ip telemetry
- ip telemetry authentication
- ip telemetry security-profile
- ip unnumbered
- ip vrf
- ip vrf forwarding
- ip vrf mgmt
- ipv6 access-group
- ipv6 access-list
- ipv6-acl
- ipv6 address
- ipv6 anycast-address
- ipv6 anycast-address enable
- ipv6 dhcp snooping
- ipv6 dhcp snooping trust
- ipv6 dhcp snooping verify mac-address
- ipv6 dhcp snooping vlan
- ipv6 dhcp-relay
- ipv6 dhcp-relay max-hop-count
- ipv6 dhcp-relay source-interface
- ipv6 dhcp-relay vrf-select
- ipv6 drop-neighbor
- ipv6 enable
- ipv6 nd adv-interval-option
- ipv6 nd cache
- ipv6 nd dnssl
- ipv6 nd home-agent-config-flag
- ipv6 nd home-agent-lifetime
- ipv6 nd home-agent-preference
- ipv6 nd managed-config-flag
- ipv6 nd mtu
- ipv6 nd other-config-flag
- ipv6 nd prefix
- ipv6 nd ra-fast-retrans
- ipv6 nd ra-hop-limit
- ipv6 nd ra-interval
- ipv6 nd ra-lifetime
- ipv6 nd ra-retrans-interval
- ipv6 nd rdnss
- ipv6 nd reachable-time
- ipv6 nd router-preference
- ipv6 nd suppress-ra
- ipv6 neighbor
- ipv6 nht
- ipv6 prefix-list
- ipv6 route
- ipv6 source binding

hardware

Enters hardware mode to change ACL counter parameters and TCAM Key-profile parameters.

Command hardware

Options None

Modes CONFIGURATION

Usage Use this command to enter hardware configuration mode to configure ACL counter parameters and TCAM key-profile parameters for different flow-based-services.

Example

```
sonic# configure terminal  
sonic(config)# hardware
```

Releases 3.1 or later

hostname

Configures the switch hostname.

Command hostname *hostname*

Options *hostname*—Hostname of the switch

Modes CONFIGURATION

Usage Use this command to set the hostname for the switch. For the hostname to get reflected on the CLI prompt, you must log out from Exec mode (sonic) and log in again.

Examples

```
sonic(config)# hostname sonic  
  
sonic(config)# no hostname
```

Releases 3.1 or later

icmp-echo

Configures the operation type as ICMP, and the target IP address for an IP SLA instance.

Command icmp-echo *target-ip-address*

Options *target-ip-address*—Enter the target IP address to track with ICMP IP SLA.

Modes IP-SLA

Usage For default VRF, do not use the vrf option.

Examples

```
sonic(config)# ip sla 10  
sonic(config-ipsla-10)# icmp-echo 10.30.1.2  
  
sonic(config-ipsla-10)# no icmp-echo
```

Releases 3.1 or later

idle-time

Configures the idle duration in microseconds and classify a flow-let in a macro flow.

Command `idle-time idle-time-value`

Options *idle-time-value*—Enter the idle time value (16 to 32767; default is 80).

Modes ARS-OBJECT

Usage The idle time configuration is not supported in packet-random ARS mode.

Examples

```
sonic(config)# ars object default  
sonic(config-ars-object)# idle-time 5000
```

Releases 4.4.0 or later

ifa

Configures the inband flow analyzer.

Command `ifa`

Options None

Command mode TAM

Usage Use this command to enter the IFA configuration mode to configure and enable IFA on the switch. IFA is used to record flow-specific information from switches across the network for specified flows.

Example

```
sonic(config-tam)# ifa
```

Releases 3.1 or later

ignore server-key

Configure the device to ignore the server key.

Command `ignore server-key`

Modes RADIUS-DA

Usage Use this command to ignore the server-key and accept packet from an untrusted DAC.

Examples

```
sonic(config)# aaa server radius dynamic-author  
sonic(config-radius-da)# ignore server-key
```

Releases 4.1.0 or later

ignore session-key

Configure the device to ignore the session key.

Command `ignore session-key`

Modes RADIUS-DA

Usage This command fails to run when the authentication type using the auth-type command is set to session-key as the authentication can happen only based on the session-key attribute.

Examples

```
sonic(config) # aaa server radius dynamic-author
sonic(config-radius-da) # ignore session-key
```

Releases

4.1.0 or later

image firmware install

Stages a firmware package.

Command

```
image firmware install file-url
```

Options

- *http[s]://hostip:/filepath*—Install the image from a remote HTTP or HTTPS server.
- *file://filepath*—Install the image from the local or a USB file system.

Modes

EXEC

Usage

Although you can use the `image firmware install` command to stage a firmware file, ONIE installs the firmware package after you reload the switch.

Example

```
sonic# image firmware install file://home/admin/onie-update-full-x86_64-
dell EMC_Z9400_c3758-r0.3.51.5.1-15.tar
%Info: Check 'show image firmware status' for firmware package staging
progress.
```

Releases

4.2.0 or later

image gpg-key key-server key-id

Installs a GNU Privacy Guard (GPG) key file that is used to verify an Enterprise SONiC image.

Command

```
image gpg-key key-server key-server-address key-id key-id
```

Options

- *key-server key-server-address* — Enter the text string of the hostname address of the key server from which you want to download a GPG key.
- *key-id key-id* — Enter the ID of the GPG public key to retrieve from the key server (64 bits minimum).

Modes

EXEC

Usage

To check the data integrity of an Enterprise SONiC image, you can use GPG verification. You must first download a GPG key file and then verify the image with the [image verify gpg signature](#) command. The GPG verification method requires the image URL and GPG key-file path to be in a remote or local directory.

Examples

```
sonic# image gpg-key key-server hkp://keyserver.ubuntu.com:80 key-id
9FD5A00009E251BF
```

Releases

4.4.1 or later

image install

Installs an Enterprise SONiC image.

Command

```
image install {cancel | filepath}
```

Options

Path/url—Enter the location of the image file:

- *http[s]://hostip:/filepath*—Install the image from a remote HTTP or HTTPS server.
- *file://filepath*—Install the image from the local or a USB file system.

Modes	EXEC
Usage	Use the <code>image install</code> command to install an Enterprise SONiC image in the standby partition. If the active partition contains any modified text files or installed custom packages, they are not available in the standby partition. Back up the modified files and reinstall the packages after downloading the image. To interrupt and cancel an active image installation, use the <code>image install cancel</code> command.
Example	<pre>sonic# image install http://10.199.210.159/tftpboot/SONiC/broadcom_releases/4.4.0/Build106/_Enterprise SONiC OS_4.4.0_Cloud_Premium.bin %Info: Check 'show image status' for image install progress.</pre> <pre>sonic# image install cancel Cancel the image install process, continue? [y/N]:</pre>
Releases	3.0 or later

image patch install

Installs a patch.

Command	<code>image patch install {file:local-path file-url}</code>
Options	<ul style="list-style-type: none"> • <code>http[s]://host-ip/filepath</code> — Install the image from a remote HTTP or HTTPS server. • <code>file: filepath</code> — Install a patch image from a local or USB file path.
Modes	EXEC
Usage	A patch automatically performs a system reboot or container restart, if required. To display the list of patches already applied or installed on the switch, use the <code>show image patch list</code> command.
Example	<pre>sonic# image patch install file:///home/admin/sonic-broadcom-enterprise-advanced.bin.01.patch %Info: Check 'show image patch status' for patch install progress.</pre>
Releases	4.1.0 or later

image patch rollback

Removes an installed patch.

Command	<code>image patch rollback patch-tag-name</code>
Options	<code>patch-tag-name</code> — Specifies the patch Tag value displayed in <code>show image patch list</code> output.
Modes	EXEC
Usage	During patch installation, if a patch fails to install properly, any part that was applied is removed and the image is restored to its previous state. To install a patch, use the <code>image patch install</code> command.
Example	<pre>sonic# image patch rollback "22.11.22-0001-patch-framework-verification-patch" %Info: Check 'show image patch status' for patch rollback progress.</pre>
Releases	4.1.0 or later

image remove

Removes all or a specific image file.

Command	<code>image remove {all <i>image</i>}</code>
Options	<ul style="list-style-type: none">• <code>all</code> — Removes all image files• <code><i>image</i></code> — Removes a specific image file
Modes	EXEC
Usage	Use this command to delete an unused SONiC image. You cannot remove the current running image.
Example	<pre>sonic# image remove SONiC-OS-HEAD.140-20200105.093102 Remove image SONiC-OS-HEAD.138-20200103.154042? [y/N]:y</pre>
Releases	3.0 or later

image set-default

Sets the default boot image.

Command	<code>image set-default <i>img-name</i></code>
Options	<code><i>img-name</i></code> —Image name
Modes	EXEC
Usage	Use this command to set the default boot image that will be used during the next reboot.
Example	<pre>sonic# image set-default SONiC-OS-3.2.0-Enterprise_Base sonic# show image list Current: SONiC-OS-3.1.0-Enterprise_Base Next: SONiC-OS-3.2.0-Enterprise_Base Available: SONiC-OS-3.2.0-Enterprise_Base SONiC-OS-3.2.0_RC10-Enterprise_Base</pre>
Releases	3.0 or later

image verify gpg signature

Verifies an Enterprise SONiC image using the GNU Privacy Guard (GPG) verification method.

Command	<code>image verify <i>image-file-url</i> gpg signature <i>signature-file-url</i></code>
Options	<ul style="list-style-type: none">• <code><i>image-file-url</i></code> — Enter the location of the image file in one of the following formats:<ul style="list-style-type: none">◦ <code>ftp://userid:passwd@hostip/filepath</code> — Verifies an image file from a remote FTP server.◦ <code>home://filename</code> — Verifies an image file from a local directory.◦ <code>http://hostip/filepath</code> — Verifies an image file from a remote HTTP server.◦ <code>https://hostip/filepath</code> — Verifies an image file from a remote HTTPS server.◦ <code>scp://userid:passwd@hostip/filepath</code> — Verifies an image file from a remote SCP server.◦ <code>usb://filepath</code> — Verifies an image file on an attached USB device.• <code>gpg</code> — Use a GPG key to verify the downloaded image file.• <code><i>signature-file-url</i></code> — Enter the location of the signature file to download from a local directory, attached USB media or a remote server using FTP, HTTP, HTTPS, or SCP.
Modes	EXEC

Usage To check the data integrity of an Enterprise SONiC image, you can use GPG verification. You must first download a GPG key file with the `image gpg-key key-server key-id` command and then verify the image. The GPG verification method requires the image URL, and the GPG key-file and signature file paths to be all in a remote or local directory.

Examples

```
sonic# image verify http://1.1.1.1/image.bin gpg signature home://sign.gpg
```

Releases 4.4.1 or later

image verify pki signature

Verifies an Enterprise SONiC image using the Public Key Infrastructure (PKI) verification method.

Command `image verify image-file-url pki signature signature-file-url`

Options

- *image-file-url* — Enter the location of the image file in one of the following formats:
 - `ftp://userid:passwd@hostip/filepath` — Verifies an image file from a remote FTP server.
 - `home://filename` — Verifies an image file from a local directory.
 - `http://hostip/filepath` — Verifies an image file from a remote HTTP server.
 - `https://hostip/filepath` — Verifies an image file from a remote HTTPS server.
 - `scp://userid:passwd@hostip/filepath` — Verifies an image file from a remote SCP server.
 - `usb://filepath` — Verifies an image file on an attached USB device.
- *pki* — Use an x509 certificate to verify the downloaded image file.
- *signature signature-file-url* — Enter the location of the signature file to download from a local directory, attached USB media or a remote server using FTP, HTTP, HTTPS, or SCP.
- *public-key public-key-url* — Enter the location of the public key file to download from a local directory, attached USB media or a remote server using FTP, HTTP, HTTPS, or SCP.

Modes EXEC

Usage To check the data integrity of an Enterprise SONiC image, you can use PKI verification. The PKI verification method requires the image URL, and the PKI signature and public key-file paths to be all in a remote or local directory.

Examples

```
sonic# image verify http://1.1.1.1/image.bin pki signature http://1.1.1.1/sign.sig public-key home://Dellcert.pem
```

Releases 4.4.1 or later

import vrf

Imports all routes or selected routes, using a route map, from another VRF.

Command `import vrf {route-map route-map-name | import-vrf-name}`

Options

- *route-map-name*—Route-map name
- *import-vrf-name*—VRF name to import (up to 15 characters)

Modes ROUTER-BGP

Usage Use the `import vrf` command to leak all routes from a specified VRF to the current VRF. Use a route map to leak selected routes.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family ipv4 unicast
sonic(config-router-bgp-af)# import vrf Vrf1
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family ipv4 unicast
sonic(config-router-bgp-af)# import vrf route-map map1
```

```
sonic(config-router-bgp-af)# no import vrf
```

Releases

3.1 or later

instance

Configures VLANs to an MST instance.

Command `instance inst-id {vlan id/id-range}`

Options • *inst-id*—MST interface ID (0 to 4094)

• *vlan id/id range*—Individual VLAN IDs or ID range (1 to 4094)

Modes SPANNING-TREE MST

Usage

To separate individual VLAN IDs or VLAN ranges, use a comma; for example, 20, 70-100, 142. In the no version of the command, if you specify a VLAN ID or range, the VLANs are removed from the corresponding MST instance. If you do not specify a VLAN ID or range, all VLANs in the MST instance are removed. By default, all VLANs are assigned to MST instance 0.

 **NOTE:**

- Changing a VLAN to MST instance mapping can indeed result in protocol convergence. Be sure to configure the mapping before you enable MSTP to avoid traffic disruption.
- Assign a VLAN to an MST instance before you create the VLAN in order to preconfigure VLAN-to-MST instance mapping.

Examples

```
sonic(config)# spanning-tree mst configuration
sonic(config-mst)# instance 1 vlan 100
```

```
sonic(config)# spanning-tree mst configuration
sonic(config-mst)# no instance 1 vlan 100
```

Releases

4.0 or later

interface

Enters interface configuration mode, and adds a physical or VLAN interface.

Command `interface {phy-if-name | vlan-if-name | phy-sub-if-name}`

Options • *phy-if-name* — Ethernet, PortChannel, Management, or Loopback interface name

• *vlan-if-name* — VLAN interface name

• *phy-sub-if-name* — Ethernet, PortChannel, Management, or Loopback subinterface name

Modes CONFIGURATION

Usage

Use this command to select a physical interface (Ethernet, PortChannel, Management, or Loopback) or VLAN interface to configure. Use [show interface](#) to view the currently configured interfaces. To add Ethernet and PortChannel interfaces to an access or trunk VLAN, use [switchport access](#) and [switchport trunk](#).

Examples

```
sonic(config) # interface Ethernet 28
sonic(config-if-Ethernet28) #

sonic(config) # interface Vlan 10
sonic(config-if-Vlan10) #

sonic (config) # interface Ethernet 80.1
sonic (config-subif-Ethernet80.1) encapsulation dot1q vlan-id 10

sonic(config) # no interface Vlan 10
```

Releases

3.2 or later

interface CPU

Enters CPU interface configuration mode.

Command

interface CPU

Options

None

Modes

CONFIGURATION

Usage

Use this command to enter CPU interface configuration mode to apply the ACL-based CoPP policy to change the queue assignment and policer rate for CPU traffic.

Example

```
sonic(config) # interface CPU
sonic(config-if-cpu) #
```

Releases

3.1 or later

interface breakout

Splits a port into breakout interfaces.

Commandinterface breakout port *slot/port* mode *breakout_mode***Options**

- *slot/port mode*—Front-panel port (slot/port)
- *breakout_mode*—Port breakout mode. The options are:
 - 1x100G
 - 1x40G
 - 2x100G
 - 2x50G
 - 4x100G
 - 4x25G
 - 4x10G
 - 1x400G
 - 2x200G
 - 4x50G
 - 8x50G
 - 8x25G
 - 8x10G
 - 1x800G
 - 2x400G

Modes

CONFIGURATION

Usage	Use the <code>show interface breakout modes</code> command to verify the configured breakout interfaces. The <code>no interface breakout port slot/port mode</code> command resets a port to its default mode.
Examples	<pre>sonic(config)# interface breakout port 1/1 mode 4x25 Dynamic Port Breakout in-progress, use 'show interface breakout port 1/1' to check status.</pre> <pre>sonic(config)# no interface breakout port 1/1 Dynamic Port Breakout in-progress, use 'show interface breakout port 1/1' to check status.</pre>
Releases	3.1 or later

interface Loopback

Enters Loopback interface configuration mode.

Command	<code>interface Loopback lo-id</code>
Options	<code>lo-id</code> — Loopback interface ID number (0 to 16383)
Modes	CONFIGURATION
Usage	Use this command to configure a Loopback interface.
Examples	<pre>sonic(config)# interface loopback 100 sonic(config-if-lo100) #</pre> <pre>sonic(config)# no interface loopback 100</pre>
Releases	3.0 or later

interface Management

Enters Management interface configuration mode.

Command	<code>interface Management mgmt-if-id</code>
Options	<code>mgmt-if-id</code> — Management interface ID
Modes	CONFIGURATION
Usage	Use this command to configure the Management interface. You cannot delete a Management interface port.
Example	<pre>sonic(config)# interface Management 0 sonic(config-if-Management0) #</pre>
Releases	3.0 or later

interface media-fec

Configures interface media FEC on a port.

Command	<code>interface media-fec slot/port mode {ieee custom}</code>
Options	<ul style="list-style-type: none"> <code>ieee</code> — Enables the IEEE KP/KP4 RS FEC mode <code>custom</code> — Enables a proprietary or custom FEC mode; for example, the BRCM proprietary KP/KP4 RS FEC mode on the Q56DD-400G-SR4.2 transceiver.

Modes	CONFIGURATION
Usage	Use this command if the FEC runs on an installed transceiver instead of the port interface. To verify the FEC mode on breakout interfaces, use the <code>show interface</code> command.
Example	<pre>sonic(config)# interface media-fec port 1/6 mode ieee</pre>
Releases	4.0 or later

interface-naming

Enables standard or standard extended interface naming.

Command	<code>interface-naming standard [extended]</code>
Options	<ul style="list-style-type: none"> <code>standard</code>—Enables interface naming in standard mode. <code>standard-extended</code>—Enables interface naming in standard extended mode.
Modes	CONFIGURATION
Usage	To identify the front-panel ports associated with an interface, enable <i>standard</i> interface-naming mode. Standard port interlace naming applies only to CLI configuration commands, REST API requests, gNMI remote procedure calls, Syslog messages, and SNMP views. The nonbreakout interfaces and breakout subinterfaces are identified and displayed as <code>Ethslot/port[/breakout-port]</code> . The <code>no</code> version of this command returns to the default native interface naming. Use <code>show interface-naming</code> to view the configured naming mode.

```
sonic(config)# interface Eth1/2/4
sonic(config-if-Eth1/2/4) #
```

Starting in 4.1.0 and later releases, you can use standard extended mode to extend standard interface naming to SONiC-specific applications (such as FRR), internal databases (such as `config_db`), and Linux commands (such as `ifconfig` and `tcpdump`) from the kernel name and kernel alias.

Examples	<pre>sonic(config)# interface-naming standard</pre>
	<pre>sonic(config)# interface-naming standard-extended</pre>
	<pre>sonic(config)# no interface-naming standard</pre>

Releases	3.1 or later
-----------------	--------------

interface PortChannel

Creates a port channel interface.

Command	<code>interface PortChannel {{lag-id {[mode PoMode]} {[min-links min-links-value]} [fallback] [fast_rate]} lag-id-subid}</code>
Options	<ul style="list-style-type: none"> <code>lag-id</code> — PortChannel ID (1 to 256) <code>PoMode</code> — (Optional) All interfaces in the port channel start up with LACP enabled, and active ports dynamically negotiate with peer ports; configured ports are bundled as members of an active port channel (default <code>active on</code>) <code>min-links-value</code> — (Optional) Minimum links (1 to 255; default 0) <code>fallback</code> — (Optional) Places the port channel in fallback mode <code>fast_rate</code> — (Optional) Places the port channel in fast_rate mode <code>lag-id-subid</code> — (Optional) PortChannel subinterface ID
Modes	CONFIGURATION

Usage

By default, the admin status is UP, the MTU is 9100 bytes, fallback and fast rate are disabled, and the LACP mode is active. The LACP fallback feature allows an active member interface to establish a connection with a peer interface before the port channel receives the LACP protocol negotiation from the peer. When `fast_rate` is disabled, an LACP port channel is in SLOW mode, and Ethernet port members send LACP protocol data unit (LACPDU) packets to connected neighbors with the state of the link every 30 seconds. If you enable `fast_rate`, the port channel operates in FAST mode, and Ethernet members send LACPDUs every second. Use `channel-group` to create a static port channel LAG, and manually assign member interfaces. Use `show interface PortChannel` or `show PortChannel summary` to view the currently configured port channels.

Examples

```
sonic(config)# interface PortChannel 10
sonic(config-if-po10)#
sonic (config)# interface PortChannel 1.1
sonic (config-subif-PortChannel1.1)# encapsulation dot1q vlan-id 10
sonic(config)# no interface PortChannel 10
sonic(config)# interface PortChannel 4
sonic(config-if-po4)# min-links 4
sonic(config-if-po4)# fallback
sonic(config-if-po4)# fast-rate
```

Releases

3.1 or later

interface port-locator

Enables the port locator LED.

Command

```
interface port-locator [timer timer_value] [Ethernet port-port]
```

Options

- *timer_value*—Timer value in minutes (1 to 120)
- *port-port*—Interface or interface range

Modes

EXEC

Usage

This feature does not interact with the application and hence any port-locator settings are not saved across a reset and also do not be displayed in running-configuration.

Examples

```
sonic# interface port-locator Ethernet 2
sonic# interface port-locator timer 60
sonic# interface port-locator Ethernet 4,9-12
```

Releases

4.0 or later

interface range

Configures a range of Ethernet, port-channel or VLAN interfaces for bulk configuration.

Command

```
interface range {iface_range_num | vlan_range_num | po_range_num | {create
{ivlan_range_num | {po_range_num {[mode PoMode] } {[min-links min-links-value] } [fallback] [fast_rate]}}}
```

Options

- *iface_range_num*—Range of Ethernet interfaces
- *vlan_range_num*—Range of VLAN interfaces
- *po_range_num*—Range of PortChannel interfaces

- *PoMode* — Selects PortChannel mode; select active on
- *min-links-value* — Minimum links

Modes

CONFIGURATION

Usage

Enter up to six comma-separated interface ranges without spaces between commas. When creating an interface range, interfaces are not sorted and appear in the order entered. You cannot mix interface configuration such as Ethernet ports with VLANs.

- A bulk configuration is created if at least one interface is valid
- Non-existing interfaces are excluded from the bulk configuration with a warning message
- Command has multiple port ranges, and the prompt excludes the smaller port range
- If you enter overlapping port ranges, the port range extends to the smallest port and the largest end port
- You can only use VLAN and port-channel interfaces created with [interface](#) or [interface PortChannel](#)

Examples

```
sonic(config) # interface range Ethernet 1-4,6,8-10
sonic(config-if-range-eth**)#
```



```
sonic(config) # no interface range
```

Releases

3.1 or later

interface transceiver diagnostics loopback

Enables the loopback test mode of the transceiver.

Command

```
interface transceiver diagnostics loopback {host-side-input | host-side-output | media-side-input | media-side-output} [Ethernet port-port]
```

Options

- *host-side-input*—Host or System side input
- *host-side-output* —Host or System side output
- *media-side-output*—Media or Line side output
- *media-side-input* —Media or Line side input
- *port-port*—(Optional) Ethernet port number or port range

Modes

CONFIGURATION

Usage

If the interface details are not specified, this command is applied to all the switch ports.

Examples

Enable or disable all the loopback controls:

```
sonic-clc(config) # interface transceiver diagnostics loopback Ethernet 0
sonic-clc(config) # no interface transceiver diagnostics loopback
Ethernet 0
```

Enable or disable one specific loopback controls:

```
sonic(config) # interface transceiver diagnostics loopback media-side-
input
sonic(config) # no interface transceiver diagnostics loopback media-side-
input
```

Releases

4.0 or later

interface transceiver diagnostics pattern

Enables the pattern generation and checking mode.

Command

```
interface transceiver diagnostics pattern { checker-host | checker-media |
generator-host | generator-media } [ Ethernet port-port ]
```

Options	<ul style="list-style-type: none"> • <code>checker-host</code> — Enable PRBS pattern checking at the system/host side • <code>checker-media</code> — Enable PRBS pattern checking at the media/line side • <code>generator-host</code> — Enable PRBS pattern generation at the system/host side • <code>generator-media</code> — Enable PRBS pattern generation at the media/line side • <code>port-port</code> — (Optional) Ethernet port number or port range
Modes	CONFIGURATION
Usage	If the interface information is not specified, this command is applied to all the switch ports.
Examples	Enable or disable all the pattern controls:
	<pre>sonic-cl(i(config)# interface transceiver diagnostics pattern Ethernet 0 sonic-cl(i(config)# no interface transceiver diagnostics pattern Ethernet 0</pre>
	Enable or disable one specific pattern control:
	<pre>sonic(config)# interface transceiver diagnostics pattern checker-host Ethernet 0 sonic(config)# no interface transceiver diagnostics pattern checker-host Ethernet 0</pre>
Releases	4.0 or later

interface vxlan

Enters VXLAN interface configuration mode.

Command	<code>interface vxlan vtep-name</code>
Options	<code>vtep-name</code> —Text string prefixed with <code>vtep</code> ; 10 characters maximum; for example, <code>vtep25</code> .
Modes	CONFIGURATION
Usage	Use this command to configure a VXLAN interface. A virtual extensible LAN (VXLAN) extends Layer 2 (L2) server connectivity over an underlying Layer 3 (L3) transport network in a virtualized data center. A virtualized data center consists of virtual machines (VMs) in a multi-tenant environment.
Examples	<pre>sonic(config)# interface vxlan vtep1 sonic(config-if-vxlan-vtep1)# sonic(config)# no interface vxlan vtep1</pre>
Releases	3.0 or later

ip access-group

Specifies access control for packets.

Command	<code>ip access-group access-list-name {in out}</code>
Options	<code>access-list-name</code> — IPv4 access-list name (up to 63 characters)
Modes	INTERFACE
Usage	Use this command to create an ingress (in) or egress (out) access-list on an interface. ACL must be created first and must be IPv4 to be applied. Only one ACL of a given type can be applied per interface and per direction.

Examples

```
sonic(config-if-Ethernet28)# ip access-group abcd in  
  
sonic(config-if-pol1)# ip access-group ipacl-example out  
  
sonic(config-if-Ethernet28)# no ip access-group abcd in
```

Releases

3.0 or later

ip access-list

Creates an IP access-list to filter based on an IP address.

Command `ip access-list access-list-name`**Options** `access-list-name` — Name of an IPv4 access-list (up to 63 characters)**Modes** CONFIGURATION**Usage** Use this command to assign an access-list to match the route-map. ACL names must begin with A-Z, a-z or 0-9. Underscore and hyphens can be used except as the first character. ACL name must be unique across all ACL types.**Examples**

```
sonic(config)# ip access-list ipacl-example  
  
sonic(config)# no ip access-list ipacl-example
```

Releases

3.0 or later

ip-acl

Configures key-profile for PAC-related IP ACLs.

Command `ip-acl {egress | ingress} key-profile pac`**Options**

- egress—egress direction
- ingress—ingress direction
- pac—key-profile for PAC-related ACLs

Modes TCAM**Usage** Use this command to configure key-profile for PAC-related IP ACLs. This command is supported only in the Lite bundles.**Examples**

```
sonic# configure terminal  
sonic(config)# hardware  
sonic(config-hardware)# tcam  
sonic(config-hardware-tcam)# ip-acl egress key-profile pac
```

Releases

4.0 or later

ip address

Configures an IPv4 address to an interface.

Command `ip address addr {{[gwaddr gw_addr]}} | {[secondary]}`**Options**

- *addr* — IPv4 address in A.B.C.D/mask format

- *gw_addr* — (Optional) Gateway address in A.B.C.D format
- *secondary* — (Optional) Secondary IP address

Modes

INTERFACE

Usage

Use this command to configure an IPv4 address to an Ethernet, Management, VLAN, PortChannel, or Loopback interface. The *gwaddr* option is only used in Management interface mode.

Examples

```
sonic(config)# interface Ethernet 28
sonic(config-if-Ethernet28)# ip address 10.1.1.0/24
```

```
sonic(config-if-Ethernet28)# no ip address 10.1.1.0/24
```

Releases

3.0 or later

ip anycast-address

Configures an IPv4 static anycast gateway address for an interface.

Command

`ip anycast-address anycast-addr`

Options

anycast-addr—IPv4 anycast address in A.B.C.D/mask format

Modes

INTERFACE-VLAN

Usage

Use this command to configure an IPv4 static anycast gateway address for a VLAN interface. Configure anycast MAC address globally using `ip anycast-mac-address` command for this static anycast address.

Examples

```
sonic(config-if-Vlan5)# ip anycast-address 50.0.0.1/24
```

```
sonic(config-if-Vlan5)# no ip anycast-address 50.0.0.1/24
```

Releases

3.0 or later

ip anycast-address

Enables or disables IPv4 static anycast gateway functionality.

Command

`ip anycast-address {enable | disable}`

Options

- *enable*—Enables anycast gateway (default)
- *disable*—Disables anycast gateway

Modes

CONFIGURATION

Usage

Use this command to enable or disable IPv4 static anycast-address globally. But default, IP anycast-address functionality is enabled.

Examples

```
sonic(config)# ip anycast-address enable
```

```
sonic(config)# ip anycast-address disable
```

Releases

3.1 or later

ip anycast-mac-address

Configures an IPv4 or IPv6 MAC address for all static anycast gateway addresses.

Command	<code>ip anycast-mac-address <i>anycast-mac</i></code>
Options	<code><i>anycast-mac</i></code> — Anycast MAC address in nn:nn:nn:nn:nn:nn format
Modes	INTERFACE-VLAN
Usage	Use this command to configure the MAC address used for all IPv4 and IPv6 static anycast gateway addresses.
Examples	<pre>sonic(config)# interface Vlan 5 sonic(config-if-Vlan5)# ip anycast-mac-address 00:22:33:44:55:66 sonic(config-if-Vlan5)# no ip anycast-mac-address 00:22:33:44:55:66</pre>
Releases	3.0 or later

ip anycast-mac-address router-mac-for-forwarding

Configures the router HW MAC address to be set as the source MAC address in routed packets in VLANs which have a configured static anycast address.

Command	<code>ip anycast-mac-address router-mac-for-forwarding</code>
Options	None
Modes	CONFIGURATION
Usage	In a data center, the same static anycast MAC address is used in all pods - see ip anycast-mac-address . This MAC address acts as the gateway MAC that is set as the source MAC address in routed packets in VLANs, which have a configured static anycast address. If the network fabric uses filters to drop packets which have the static anycast MAC address as the source MAC address, configure the router HW MAC address to be set as the source MAC address in routed packets.
Examples	<pre>sonic(config)# ip anycast-mac-address router-mac-for-forwarding sonic(config)# no ip anycast-mac-address router-mac-for-forwarding</pre>
Releases	4.4.0 or later

ip arp

Configures static ARP.

Command	<code>ip arp <i>static_ip</i> <i>mac-address</i></code>
Options	<ul style="list-style-type: none"><code><i>static_ip</i></code>—Static IP address in A.B.C.D or A::B format<code><i>mac-address</i></code>—MAC address in nn:nn:nn:nn:nn:nn format
Modes	INTERFACE
Usage	Use this command to configure a static ARP entry in an interface.
Examples	<pre>sonic(config)# interface Ethernet28 sonic(config-if-Ethernet28)# ip arp 10.10.10.1 00:22:33:44:55:66 sonic(config-if-Ethernet28)# no ip arp 10.10.10.1 00:22:33:44:55:66</pre>

Releases	3.1 or later
-----------------	--------------

ip dhcp-relay

Adds DHCP-relay on a physical (Ethernet), PortChannel, or VLAN interface.

Command	<code>ip dhcp-relay ipaddr1 {{[vrf vrf_name]} {[ipaddr2 {[ipaddr3 [ipaddr4]}]}}}</code>
----------------	---

Options	<ul style="list-style-type: none"> • <i>ipaddr1</i> — IP address in A.B.C.D format • <i>vrf_name</i> — (Optional) Name of the VRF (up to 15 characters) • <i>ipaddr2</i> — IP address in A.B.C.D format • <i>ipaddr3</i> — IP address in A.B.C.D format • <i>ipaddr4</i> — IP address in A.B.C.D format
----------------	--

Modes	INTERFACE
--------------	-----------

Usage	Use this command to add or remove IPv4 DHCP relay addresses on the given interface. You can specify up to four addresses at a time (separated by space).
--------------	--

Examples	<code>sonic(config-if-pol1)# ip dhcp-relay 100.10.14.200 vrf vrf1</code>
-----------------	--

```
sonic# configure terminal
  sonic(config)# interface Ethernet 0
    sonic(config-if-Ethernet0)# ip dhcp-relay 11.0.0.1
    sonic(config-if-Ethernet0)# no ip dhcp-relay 11.0.0.1
```

```
sonic(config-if-pol1)# no ip dhcp-relay 100.10.14.200
```

Releases	3.1 or later
-----------------	--------------

ip dhcp-relay circuit-id

Configures the circuit-id format for option 82 in DHCPv4 relay packets.

Command	<code>ip dhcp-relay circuit-id [%p %h:%p %i]</code>
----------------	---

Options	<ul style="list-style-type: none"> • <i>%p</i> — Send the name of the interface on which the request was received; for example, <code>vlan100</code> (default). • <i>%h:%p</i> — Send the hostname of the switch followed by the interface name; for example, <code>sonic-acc-sw-01:Vlan100</code>. • <i>%i</i> — Send the name of the physical interface on which the request was received; for example, <code>Eth1/2</code>. Use this option to identify the physical interface when multiple clients are connected in a VLAN. The DHCP server can then assign DHCP leases according to individual client interfaces. If a VLAN name is sent in the circuit ID information, all clients will have the same circuit ID.
----------------	---

Modes	INTERFACE
--------------	-----------

Usage	When a DHCP relay agent forwards DHCP requests from a client to a DHCP server, it can include encoded circuit ID information based on the interface on which the DHCP client packet is received. The circuit ID is used to relay DHCP server response packets back to the originating client interface. To delete the configured circuit-ID format and return to the default, enter the <code>no ip dhcp-relay circuit-id</code> command. DHCP option 82 is applied only on DHCPv4 packets.
--------------	---

Example	<code>sonic(config-if-Eth1/2)# ip dhcp-relay circuit-id %h:%p</code>
----------------	--

An example of the resulting circuit-ID (option 82) information in DHCPv4 relay packets is:

```
Agent-Information Option 82, length 43:  
  Circuit-ID SubOption 1, length 22: "sonic-acc-sw-01:Vlan100"  
  Remote-ID SubOption 2, length 17: 52:54:00:c1:65:6b
```

Releases	4.0.1 or later
-----------------	----------------

ip dhcp-relay link-select

Enables link selection.

Command	<code>ip dhcp-relay link-select</code>
Options	None
Modes	INTERFACE
Usage	Use this command to configure the link-selection suboption on an Ethernet, PortChannel, or VLAN interface.
Examples	<pre>sonic(config-if-Vlan1)# ip dhcp-relay link-select sonic(config-if-Vlan1)# no ip dhcp-relay link-select</pre>
Releases	3.1 or later

ip dhcp-relay max-hop-count

Sets the maximum hop count for DHCP-relay packets.

Command	<code>ip dhcp-relay max-hop-count <i>hop_count</i></code>
Options	<i>hop_count</i> — Maximum number of hops (0 to 16; default is 10)
Modes	INTERFACE
Usage	Use this command to set the maximum hop count for an Ethernet, PortChannel, or VLAN interface.
Examples	<pre>sonic(config-if-pol1)# ip dhcp-relay max-hop-count 10 sonic(config-if-Ethernet12)# ip dhcp-relay max-hop-count 9 sonic(config-if-pol1)# no ip dhcp-relay max-hop-count</pre>
Releases	3.1 or later

ip dhcp-relay policy-action

Configures the policy for handling DHCPv4 relay options.

Command	<code>ip dhcp-relay policy-action <i>PolicyAction</i></code>
Options	<i>PolicyAction</i> — Policy action (up to 8 characters)
Modes	INTERFACE
Usage	Use this command to configure a DHCP-relay policy for an Ethernet, PortChannel, or VLAN interface.

Examples

```
sonic(config-if-pol1)# ip dhcp-relay policy-action REPLACE  
sonic(config-if-Ethernet12)# ip dhcp-relay policy-action REPLACE  
sonic(config-if-pol1)# no ip dhcp-relay policy-action
```

Releases

3.1 or later

ip dhcp-relay source-interface

Configures the source IP address used for relaying DHCP packets.

Command ip dhcp-relay source-interface {intfName | pchName | vlanName | loName}**Options**

- *intfName*—Interface name
- *pchName*—PortChannel number
- *vlanName*—VLAN number
- *loName*—Loopback number

Modes

INTERFACE

Usage

Use this command to set the giaddr in the DHCP relay packet to the IP address from the source-interface. DHCP server sends a reply to this IP address. This IP address should be reachable from the DHCP server. This command should be used along with ip dhcp-relay link-select command.

Examples

```
sonic(config)# interface PortChannel 1  
sonic(config-if-pol1)# ip dhcp-relay source-interface po3  
  
sonic(config-if-Ethernet12)# ip dhcp-relay source-interface Ethernet36  
  
sonic(config-if-pol1)# no ip dhcp-relay source-interface
```

Releases

3.2 or later

ip dhcp-relay vrf-select

Enables VRF selection.

Command ip dhcp-relay vrf-select**Options**

None

Modes

INTERFACE

Usage

Use this command to enable VRF selection suboption (Virtual Subnet Selection - VSS) in DHCP relay. If the DHCP server supports this suboption, it uses the VRF information along with other information to assign IP to the DHCP client.

Examples

```
sonic(config)# interface PortChannel 1  
sonic(config-if-pol1)# ip dhcp-relay vrf-select  
  
sonic(config)# interface Ethernet 12  
sonic(config-if-Ethernet12)# ip dhcp-relay vrf-select  
  
sonic(config-if-pol1)# no ip dhcp-relay vrf-select
```

Releases

3.1 or later

ip dhcp snooping

Enables DHCPv4 snooping globally.

Command	ip dhcp snooping
Options	None
Modes	CONFIGURATION
Usage	DHCP snooping is applicable only to physical interfaces and port channels. Use the no form of this command to disable DHCPv4 snooping.
Examples	Enable DHCPv4 snooping: <pre>sonic-cli# configure terminal sonic-cli(config)# ip dhcp snooping sonic-cli(config)#</pre> Disable DHCPv4 snooping: <pre>sonic-cli# configure terminal sonic-cli(config)# no ip dhcp snooping sonic-cli(config)#</pre>
Releases	4.0 or later

ip dhcp snooping trust

Sets Trust mode for DHCPv4 snooping on an interface or multiple interfaces.

Command	ip dhcp snooping trust
Options	None
Modes	INTERFACE
Usage	Use the no form of this command to disable DHCPv4 snooping trust.
Examples	To enable DHCPv4 snooping trust <pre>sonic(config)#interface Ethernet10 sonic(config-if-Ethernet10)#ip dhcp snooping trust</pre>
Releases	4.0 or later

ip dhcp snooping verify mac-address

Enables or disables DHCPv4 snooping MAC address verification.

Command	ip dhcp snooping verify mac-address
Options	None
Modes	CONFIGURATION
Usage	With DHCP snooping MAC address verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports. The source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet. Where there is a mismatch, DHCP snooping logs and drops the packet.

Examples	Enable DHCPv4 snooping MAC address verification: sonic> configure terminal sonic>(config)# ip dhcp snooping verify mac-address sonic>(config)#
	Disable DHCPv4 snooping MAC address verification: sonic> configure terminal sonic>(config)# no ip dhcp snooping verify mac-address sonic>(config)#

Releases	4.0 or later
-----------------	--------------

ip dhcp snooping vlan

Enables or disables DHCPv4 snooping on a VLAN or multiple VLANs.

Command	ip dhcp snooping vlan <i>vlan-id</i>
Options	<i>vlan-id</i> — VLAN ID (1 to 4094)
Modes	CONFIGURATION
Usage	Enter an individual VLAN ID or a range of VLAN IDs separated by hyphen. For example, 20, 142, 7-100.
Examples	Enable DHCP snooping on a VLAN: sonic# configure terminal sonic# ip dhcp snooping vlan 100

Enable DHCP snooping on a VLAN range:

```
sonic(config)# ip dhcp snooping vlan 70-100
```

Disable DHCP snooping on a VLAN:

```
sonic# configure terminal  
sonic# no ip dhcp snooping vlan 100
```

Releases	4.0 or later
-----------------	--------------

ip drop-neighbor

Configures time in seconds for IPv4 drop-neighbor aging.

Command	ip drop-neighbor aging-time <i>time</i>
Options	<i>time</i> —Specify aging-time in seconds (60 to 14400; default is 300)
Modes	CONFIGURATION
Usage	To protect the CPU from IP attacks using unresolvable IPv4 packets, enable ARP protection to create a blackhole route destined for an unresolved IPv4 address. The switch drops all matching IPv4 packets until the blackhole route is deleted. A blackhole route is deleted when the route becomes reachable or the configured blackhole aging timer expires. To protect the CPU from IP attacks using unresolvable IPv6 packets, use the ipv6 drop-neighbor aging-time command.
Examples	sonic(config)# ip drop-neighbor aging-time 12000

Releases	4.1.0 or later
-----------------	----------------

ip drop-neighbor aging-time

Enables ARP protection for unresolved IPv4 subnet traffic and applies a blackhole aging interval.

Command	<code>ip drop-neighbor aging-time <i>seconds</i></code>
Options	<code>aging-time <i>seconds</i></code> —Enter the blackhole aging interval for unresolved IPv4 traffic (60-14400; default 300).
Modes	EXEC
Usage	To protect the CPU from IP attacks using unresolvable IPv4 packets, enable ARP protection to create a blackhole route destined for an unresolved IPv4 address. The switch drops all matching IPv4 packets until the blackhole route is deleted. A blackhole route is deleted when the route becomes reachable or the configured blackhole aging timer expires. To protect the CPU from IP attacks using unresolvable IPv6 packets, use the <code>ipv6 drop-neighbor aging-time</code> command.
Examples	<pre>sonic# ip drop-neighbor aging-time 12000</pre>
Releases	4.1.0 or later

ip forward-protocol udp enable

Enables the IP helper globally.

Command	<code>ip forward-protocol udp enable</code>
Options	None
Modes	CONFIGURATION
Usage	Use this command to enable UDP broadcast forwarding. Use the <code>no</code> form to disable UDP broadcast forwarding. By default, it is disabled.
Examples	<pre>sonic(config)# ip forward-protocol udp enable</pre> <pre>sonic(config)# no ip forward-protocol udp enable</pre>
Releases	3.1 or later

ip forward-protocol udp exclude

Excludes UDP ports to forward.

Command	<code>ip forward-protocol udp exclude {<i>port</i> <i>port</i>}</code>
Options	<code><i>port</i></code> —Port to exclude <ul style="list-style-type: none">● <code>tftp</code>—Port 69● <code>dns</code>—Port 53● <code>ntp</code>—Port 37● <code>netbios-name-server</code>—Port 137● <code>netbios-datagram-server</code>—Port 138● <code>tacacs</code>—Port 49
Modes	CONFIGURATION
Usage	Use this command to exclude specified UDP ports from the list of forwarding ports in UDP broadcast forwarding.

Examples

```
sonic(config) # ip forward-protocol udp exclude 12200
```

```
sonic(config) # ip forward-protocol udp exclude tftp
```

Releases

3.1 or later

ip forward-protocol udp include

Includes UDP ports to forward.

Command

```
ip forward-protocol udp include {port | port}
```

Options

port—Port to include

- tftp—Port 69
- dns—Port 53
- ntp—Port 37
- netbios-name-server—Port 137
- netbios-datagram-server—Port 138
- tacacs—Port 49

Modes

CONFIGURATION

Usage

Use this command to include specified UDP ports to the list of forwarding ports in UDP broadcast forwarding.

Examples

```
sonic(config) # ip forward-protocol udp include 12200
```

```
sonic(config) # ip forward-protocol udp include tftp
```

Releases

3.1 or later

ip forward-protocol udp rate-limit

Configures the incoming UDP rate limit.

Command

```
ip forward-protocol udp rate-limit rate
```

Options

rate—Enter a value (600 to 10000 pps; default is 600)

Modes

CONFIGURATION

Usage

Use this command to configure the rate limiting value for UDP broadcast packets.

Examples

```
sonic(config) # ip forward-protocol udp rate-limit 1000
```

```
sonic(config) # no ip forward-protocol udp rate-limit
```

Releases

3.1 or later

ip helper-address

Configures an IP helper server address for an interface.

Command

```
ip helper-address addr [vrf vrf-name]
```

Options

- *addr*—IP address in A.B.C.D format

- *vrfname*—VRF name prefixed by Vrf (up to 15 characters)

Modes

INTERFACE

Usage

Use this command to relay UDP broadcast packets as unicast packets to the configured server address (helper address).

Examples

```
sonic(config)# interface Ethernet12
sonic(config-if-Ethernet12)# ip helper-address 3.3.3.3
```

```
sonic(config)# interface PortChannel 10
sonic(config-if-po10)# ip helper-address 3.3.3.3
```

```
sonic(config-if-Vlan10)# ip helper-address 3.3.3.3
```

```
sonic(config-if-Ethernet12)# no ip helper-address 3.3.3.3
```

Releases

3.1 or later

ip igmp

Enables IGMP operation.

Command

ip igmp

Options

None

Modes

INTERFACE

Usage

Enables IGMP operation.

Examples

```
sonic(config-if-Vlan200)# ip igmp
```

```
sonic(config-if-Vlan200)# no ip igmp
```

Releases

3.2 or later

ip igmp join

Configures a static IGMP join for a multicast group.

Command

ip igmp join *mcastgrpaddr srcaddr*

Options

- *mcastgrpaddr*—Multicast group address in A.B.C.D format
- *srcaddr*—Source address in A.B.C.D format

Modes

INTERFACE

Usage

Use this command to configure a static IGMP join for a multicast group. Also, specify the source address from which the traffic has to be received.

Examples

```
sonic(config-if-Ethernet0)# ip igmp join 232.1.1.1 90.0.0.2
```

```
sonic(config-if-Ethernet0)# no ip igmp join 232.1.1.1 90.0.0.2
```

Releases

3.2 or later

ip igmp last-member-query-count

Configure IGMP last member query count.

Command	<code>ip igmp last-member-query-count <i>count</i></code>
Options	<i>count</i> —IGMP count (1 to 7; default is 2)
Modes	INTERFACE
Usage	Use this command to set the number of group-specific queries to send after an IGMP leave is received.
Examples	<pre>sonic(config) # interface Ethernet0 sonic(config-if-Ethernet0) # ip igmp last-member-query-count 5 sonic(config-if-Ethernet0) # no ip igmp last-member-query-count</pre>
Releases	3.2 or later

ip igmp last-member-query-interval

Configures IGMP last member query interval.

Command	<code>ip igmp last-member-query-interval <i>lmqueryinterval</i></code>
Options	<i>lmqueryinterval</i> —Interval (1 to 255; default is 10 deciseconds)
Modes	INTERFACE
Usage	Use this command to set the interval at which group-specific queries are sent. This value is used to set the maximum response code in IGMP group-specific queries.
Examples	<pre>sonic(config) # interface Ethernet0 sonic(config-if-Ethernet0) # ip igmp last-member-query-interval 50 sonic(config-if-Ethernet0) # no ip igmp last-member-query-interval</pre>
Releases	3.2 or later

ip igmp query-interval

Configures the IGMP query interval.

Command	<code>ip igmp query-interval <i>queryinterval</i></code>
Options	<i>queryinterval</i> —Query interval (1 to 1024; default is 125 seconds)
Modes	INTERFACE
Usage	Use this command to set the IGMP query interval. IGMP querier periodically sends queries at this interval to discover active multicast groups.
Examples	<pre>sonic(config) # interface Ethernet0 sonic(config-if-Ethernet0) # ip igmp query-interval 75 sonic(config-if-Ethernet0) # no ip igmp query-interval</pre>
Releases	3.2 or later

ip igmp query-max-response-time

Configures the IGMP query maximum response time.

Command	<code>ip igmp query-max-response-time <i>querymaxrestime</i></code>
Options	<code><i>querymaxrestime</i></code> —Time in seconds (1 to 250; default is 10)
Modes	INTERFACE
Usage	Use this command to set the IGMP query response time. This value is used to set the maximum response code in an IGMP query. On receiving a query, the hosts delay the response by a random time between 0 and maximum response time and send an IGMP join.
Examples	<pre>sonic(config-if-Ethernet0)# ip igmp query-max-response-time 5</pre> <pre>sonic(config-if-Ethernet0)# no ip igmp query-max-response-time</pre>
Releases	3.2 or later

ip igmp snooping

Configures or unconfigures IGMP snooping parameters on a VLAN.

Command	<code>ip igmp snooping {[querier] [fast-leave] {[query-interval <i>query-interval-val</i>] {[last-member-query-interval <i>last-mem-query-interval-val</i>] {[query-max-response-time <i>query-max-response-val</i>] {[version <i>igmp-version-val</i>] {[mrouter {interface <i>mrouter-if-name</i>}]} {[static-group {group-addr {interface <i>grp-if-name</i>}]}}}}}</code>
Options	<ul style="list-style-type: none">• <code>querier</code> — (Optional) Enables IGMP querier processing for the specified VLAN interface• <code>fast-leave</code> — (Optional) Enables fast-leave snooping for the specified VLAN interface• <code>query-interval-val</code> — (Optional) Query interval time in seconds (default 125)• <code>last-mem-query-interval-val</code> — (Optional) Last memory query value in millisecond (default 1000)• <code>query-max-response-val</code> — (Optional) Query maximum response time in seconds (default 10)• <code>igmp-version-val</code> — (Optional) IGMP version; 1 or 2 or 3 (default 2)• <code>mrouter-if-name</code> — (Optional) Interface name• <code>group-addr</code> — (Optional) IPv4 address in A.B.C.D format• <code>grp-if-name</code> — (Optional) Group interface name
Modes	INTERFACE-VLAN
Usage	The IGMP querier periodically sends a general query to discover which multicast groups are active. A group must have at least one host to be active. By default, the periodic query messages are sent every 60 seconds. When the IGMP querier receives a leave message, it sends a group-specific query message to ensure if any other host in the network is interested in the multicast flow. By default, the group-specific query messages are sent every 125 milliseconds. The maximum response time is the amount of time that the querier waits for a response to a query before taking action. When a host receives a query, it does not respond immediately, but rather starts a delay timer. The delay time is set to a random value between 0 and the maximum response time. The host sends a response when the timer expires; in IGMP version 2, if another host responds before the timer expires, the timer nullifies, and no response is sent. The querier advertises the maximum response time in the query. Lowering this value decreases leave latency but increases response burstiness because all host membership reports are sent before the maximum response time expires. Increasing this value decreases burstiness, but increases leave latency.

Examples

```
sonic(config-if-Vlan200)# ip igmp snooping  
  
sonic(config-if-Vlan200)# ip igmp snooping querier  
  
sonic(config-if-Vlan200)# ip igmp snooping fast-leave  
  
sonic(config-if-Vlan200)# no ip igmp snooping fast-leave  
  
sonic(config-if-Vlan200)# ip igmp snooping query-interval 20  
  
sonic(config-if-Vlan200)# no ip igmp snooping query-interval  
  
sonic(config-if-Vlan200)# ip igmp snooping last-member-query-interval 2000  
  
sonic(config-if-Vlan200)# no ip igmp snooping last-member-query-interval  
  
sonic(config-if-Vlan200)# ip igmp snooping query-max-response-time 12  
  
sonic(config-if-Vlan200)# no ip igmp snooping query-max-response-time  
  
sonic(config-if-Vlan200)# ip igmp snooping version 3  
  
sonic(config-if-Vlan200)# no ip igmp snooping version  
  
sonic(config-if-Vlan200)# ip igmp snooping mrouter interface Ethernet4  
  
sonic(config-if-Vlan200)# no ip igmp snooping mrouter interface Ethernet4  
  
sonic(config-if-Vlan200)# ip igmp snooping static-group 225.0.0.1 interface PortChannel2  
  
sonic(config-if-Vlan200)# no ip igmp snooping static-group 225.0.0.1 interface PortChannel2
```

Releases

3.2 or later

ip igmp version

Configures the IGMP version.

Command

```
ip igmp version version
```

Options

version—IGMP version (2 or 3; default is 3)

Modes

INTERFACE

Usage

Use this command to change the IGMP version.

Examples

```
sonic(config)# interface Ethernet0  
sonic(config-if-Ethernet0)# ip igmp version 2  
  
sonic(config-if-Ethernet0)# no ip igmp version
```

Releases

3.2 or later

ip load-share hash algorithm

Configures the hash algorithm used on a switch for ECMP load sharing.

Command ip load-share hash algorithm {CRC | XOR | CRC_32LO | CRC_32HI | CRC_CCITT | CRC_XOR | JENKINS_HASH_LO | JENKINS_HASH_HI}

Options *algorithm* — Enter the name of the supported hash algorithm. The default hash algorithm is displayed in show ip load-share output.

Modes CONFIGURATION

Usage To remove the configured hash algorithm and restore the default, use the no ip load-share hash algorithm command. To reconfigure the parameters used by the hash algorithm to determine ECMP load sharing over multiple routes to a destination, use the ip load-share hash {ipv4 | ipv6} command.

i **NOTE:** The JENKINS_HASH_LO and JENKINS_HASH_HI hash algorithms used for ECMP load-share hashing are only supported on Tomahawk4 (TH4) and Tomahawk5 (TH5) switches; they are not supported on other Enterprise SONiC platforms.

Examples

```
sonic(config)# ip load-share hash algorithm JENKINS_HASH_LO
```

Releases

4.4.0 or later

ip load-share hash ingress-port

Configures the IP ECMP hash seed.

Command ip load-share hash ingress-port

Options None

Modes CONFIGURATION

Usage To make ECMP hashing on IPv4, IPv6, and ROCE traffic flows more efficient, enable the ingress port to be used in the hashing calculation. To remove the configured ingress port parameter from the hashing calculation, use the no ip load-share hash ingress-port command. To reconfigure the parameters that are used by the hash algorithm to determine ECMP load sharing over multiple routes to a destination, use the ip load-share hash {ipv4 | ipv6} command.

Examples

```
sonic(config)# ip load-share hash ingress-port
```

Releases

4.4.0 or later

ip load-share hash ipv4

Configures the parameters that are used by the hash algorithm to determine ECMP load sharing over multiple IPv4 routes to a destination.

Command ip load-share hash ipv4 {ipv4-src-ip | ipv4-dst-ip | ipv4-ip-proto | ipv4-14-src-port | ipv4-14-dst-port | symmetric}

Options

- *ipv4-src-ip* — Use the source address in IPv4 packet headers.
- *ipv4-dst-ip* — Use the destination address in IPv4 packet headers.
- *ipv4-ip-proto* — Use the protocol specified by the IANA number in the Protocol field of IPv4 packet headers.
- *ipv4-14-src-port* — Use the L4 source port in IPv4 packet headers.
- *ipv4-14-dst-port* — Use the L4 destination port in IPv4 packet headers.
- *symmetric* — Enable symmetric hashing in IPv4 flows.

Modes	CONFIGURATION
Usage	<p>Use this command to modify the IPv4 load-share hashing parameters used by the hash algorithm that is specified with the <code>ip load-share hash</code> algorithm command. To remove a configured hash parameter, use the <code>no ip load-share hash ipv4 value</code> command. To enable symmetric hashing to ensure that bidirectional IPv4 flows always use the same port in an ECMP port group, use the <code>ip load-share hash ipv4 symmetric</code> command.</p>
Examples	<pre>sonic(config) # ip load-share hash ipv4 ipv4-src-ip</pre> <pre>sonic(config) # no ip load-share hash ipv4 ipv4-src-ip</pre>
Releases	3.2 or later

ip load-share hash ipv6

Configures the parameters that are used by the hash algorithm to determine ECMP load sharing over multiple IPv6 routes to a destination.

Command	<code>ip load-share hash ipv6 {ipv6-src-ip ipv6-dst-ip ipv6-next-hdr ipv6-14-src-port ipv6-14-dst-port symmetric}</code>
Options	<ul style="list-style-type: none"> <code>ipv6-src-ip</code> — Use the source address in IPv6 packet headers. <code>ipv6-dst-ip</code> — Use the destination address in IPv6 packet headers. <code>ipv6-next-hdr</code> — Use the protocol specified by the IANA number in the Next Header field of IPv6 packet headers. <code>ipv6-14-src-port</code> — Use the L4 source port in IPv6 packet headers. <code>ipv6-14-dst-port</code> — Use the L4 destination port in IPv6 packet headers. <code>symmetric</code> — Enable symmetric hashing in IPv6 flows.
Modes	CONFIGURATION
Usage	<p>Use this command to modify the IPv6 load-share hashing parameters used by the hash algorithm that is specified with the <code>ip load-share hash</code> algorithm command. To remove a configured hash parameter, use the <code>no ip load-share hash ipv6 value</code> command. To enable symmetric hashing to ensure that bidirectional IPv6 flows always use the same port in an ECMP port group, use the <code>ip load-share hash ipv6 symmetric</code> command.</p>
Examples	<pre>sonic(config) # ip load-share hash ipv6 ipv6-src-ip</pre> <pre>sonic(config) # no ip load-share hash ipv6 ipv6-src-ip</pre>
Releases	3.1 or later

ip load-share hash offset

Reconfigures the hash offset used by the ECMP hash algorithm.

Command	<code>ip load-share hash offset {offset-value flow-based}</code>
Options	<ul style="list-style-type: none"> <code>offset-value</code> — Offset value (0 to 15; the default is the last four bits of the system MAC address) <code>flow-based</code> — Enable the switch to dynamically set the offset value per flow.
Modes	CONFIGURATION
Usage	<p>The hash offset modifies the generated hash value by specifying the number of times that the hash value is clockwise-rotated. Customizing the offset is particularly effective in changing the traffic distribution for a set of source-destination flows and the configured hash algorithm. To remove the configured hash offset value and restore the default, use the <code>no ip load-share hash offset</code> command.</p>

i **NOTE:** The flow-based parameter for ECMP hashing is only supported on Tomahawk4 (TH4) and Tomahawk5 (TH5) switches; it is not supported on other Enterprise SONiC platforms. The JENKINS hash algorithm cannot be enabled with flow-based offset.

Examples

```
sonic(config)# ip load-share hash offset 200
```

```
sonic(config)# no ip load-share hash offset 200
```

Releases

3.1 or later

ip load-share hash roce qpn

Enables QPN hashing for ROCEv2 lossless flows.

Command `ip load-share hash roce qpn`**Options** None**Modes** CONFIGURATION**Usage**

For RoCE traffic flows, the configured ECMP load-share hashing parameters may result in a skewed distribution of traffic among available paths. To ensure even traffic distribution in lossless flows after you enable RoCEv2, Dell Technologies recommends that you also enable the QPN hashing option.

i **NOTE:** The `qpn` parameter for load-share hashing of RoCE traffic flows is only supported on Z9864F-ON, Z9664F-ON, and Z9432F-ON switches. QPN hashing is not supported on other Enterprise SONiC platforms. If you enable both the `qpn` and `ingress-port` options to be used in the hashing calculation, only two least significant bits (LSBs) of QPN are used for hashing.

Examples

```
sonic(config)# ip load-share hash roce qpn
```

Releases

4.4.0 or later

ip load-share hash seed

Reconfigures the seed value that is used in ECMP hash calculation for IPv4 and IPv6 traffic flows.

Command `ip load-share hash seed seed-value`**Options** `seed-value` — Seed value (0 to 16777215; the default seed value is derived from the last three octets of the system MAC address)**Modes** CONFIGURATION**Usage**

Configures a unique hash seed for each device to avoid hash polarization which may result in network congestion. The default value is derived from the last three octets of the system MAC address of the switch.

Examples

```
sonic(config)# ip load-share hash seed 200
```

```
sonic(config)# no ip load-share hash seed 200
```

Releases

3.1 or later

ip name-server

Configures the DNS name server.

Command	ip name-server <i>nameserver</i> {[vrf {mgmt}]} { <i>name_server</i> — Name server in A.B.D.C or A::B format}
Options	
Modes	CONFIGURATION
Usage	Use this command to configure the IPv4 or IPv6 name server.
Examples	<pre>sonic(config)# ip name server 100.10.4.20</pre> <pre>sonic(config)# no ip name server 100.10.4.20</pre>
Releases	3.2 or later

ip name-server source-interface

Configures the source interface to select the source IP for a DNS query.

Command	ip name-server source-interface {Ethernet <i>port-number</i> Loopback <i>number</i> Management 0 PortChannel <i>number</i> Vlan <i>vlan-id</i> }
Options	<ul style="list-style-type: none">• Ethernet <i>port-number</i> — Port number (1 to 65535)• Loopback <i>number</i> — Loopback interface ID (0 to 16383)• Management 0 — Management interface number• PortChannel <i>number</i> — PortChannel ID (1 to 128)• <i>vlan-id</i> — VLAN ID (1 to 4094)
Modes	CONFIGURATION
Usage	The DNS service is not enabled by default. You must configure a source interface and one or more DNS servers from which the switch receives IP addresses.
Examples	<pre>sonic(config)# ip name-server source-interface Loopback 0</pre> <pre>sonic(config)# ip name-server 2001:4860:4860::8888</pre> <pre>sonic(config)# ip name-server 8.8.8.8</pre> <pre>sonic(config)# no ip name-server source-interface Loopback 0</pre>
Releases	3.1 or later

ip nht

Configures next hop resolution and tracking parameters using default route.

Command	ip [vrf <i>vrf-name</i>] nht resolve-via-default
Options	<i>vrf-name</i> —(Optional) VRF name prefixed by Vrf
Modes	CONFIGURATION
Usage	Use this command to enable IPv4 next hop tracking to resolve through the default route.
Examples	<pre>sonic# configure terminal</pre> <pre>sonic(config)# ip vrf Vrf-Blue nht resolve-via-default</pre>
Releases	4.0 or later

ip ospf

Configures OSPFv2 parameters within an IPv4 interface.

Command	<code>ip ospf [ip-address]</code>
Options	<code>ip_address</code> — (Optional) IP address in A.B.C.D format
Command mode	INTERFACE
Usage	Use this command to configure OSPFv2 parameters under an IPv4 interface. IPv4 interface can be Ethernet, PortChannel, VLAN, or Loopback. Every OSPFv2 parameter on an interface can be associated with its specific IPv4 address by specifying the IPv4 address after the parameter.
Examples	<pre>sonic(config-if-Ethernet12)# ip ospf</pre> <pre>sonic(config-if-po10)# ip ospf</pre> <pre>sonic(config-if-Vlan10)# ip ospf</pre> <pre>sonic(config-if-Vlan10)# no ip ospf</pre>

Releases	3.1 or later
-----------------	--------------

ip ospf area

Configures an OSPFv2 interface area identifier.

Command	<code>ip ospf area area-id [ip-address]</code>
Options	<ul style="list-style-type: none"><code>area-id</code> — Area ID in A.B.C.D or 0..4294967295 format<code>ip-address</code> — (Optional) IP address in A.B.C.D format
Modes	INTERFACE
Usage	Use this command to associate an interface into an OSPFv2 area. Area identifier can be configured only when there is an already configured OSPFv2 switch within the interface VRF, and there are no network commands that are configured within that switch. Area identifier configuration on an interface is auto unconfigured while OSPFv2 switch is unconfigured from the VRF.
Examples	<pre>sonic(config-if-Ethernet12)# ip ospf area 19</pre> <pre>sonic(config-if-po10)# ip ospf area 19</pre> <pre>sonic(config-if-Vlan10)# ip ospf area 19 19.0.0.1</pre> <pre>sonic(config-if-Ethernet12)# no ip ospf area</pre>

Releases	3.1 or later
-----------------	--------------

ip ospf authentication

Specifies the authentication type for an interface.

Command	<code>ip ospf authentication {{[message-digest [ip-address]]}} {[null [ip-address]]}} [ip-address]</code>
Options	<ul style="list-style-type: none"><code>message-digest</code> — (Optional) Specifies that message-digest authentication is used

- `null` — (Optional) Specifies that no authentication is used
- `ip-address` — IP address in A.B.C.D format

Modes

INTERFACE

Usage

Use this command to enable OSPFv2 authentication type for OSPFv2 messages. Authentication types can be clear-text, message-digest, or no authentication. Interface mode authentication type overrides switch mode area authentication type. Based on the configured authentication type, corresponding configured authentication key is used for OPSFV2 message authentication.

Examples

```
sonic(config-if-Ethernet12)# ip ospf authentication message-digest
sonic(config-if-po10)# ip ospf authentication message-digest
sonic(config-if-Vlan10)# ip ospf authentication message-digest
sonic(config-if-Ethernet12)# no ip ospf authentication
```

Releases

3.1 or later

ip ospf authentication-key

Assigns a password to be used by neighboring routes that are using OSPF simple password authentication.

Command

```
ip ospf authentication-key authkey {{[encrypted [ip-address]]}} [ip-address]
```

Options

- `authkey` — Eight-character string for the authentication key
- `ip-address` — (Optional) IP address in A.B.C.D format

Modes

INTERFACE

Usage

Use this command to configure OSPFv2 clear text authentication key. Clear-text authentication key can be up to eight characters long. The provided password displays as an encrypted string and is also saved as an encrypted string in configuration file. It is recommended to use the password and not to use the encrypted string as the password.

Examples

```
sonic(config-if-Ethernet12)# ip ospf authentication-key pa$$woRd
sonic(config-if-Ethernet12)# no ip ospf authentication-key
```

Releases

3.2 or later

ip ospf bfd

Enables bidirectional forwarding detection (BFD) on a specific interface configured for OSPF.

Command

```
ip ospf bfd
```

Options

None

Modes

INTERFACE

Usage

Use this command to configure an OSPFv2 interface to use BFD for failure detection. Enabling BFD establishes a BFD session between the OSPF neighbors. Any failure in the BFD session brings down the OSPFv2 session.

Examples

```
sonic(config-if-Ethernet12)# ip ospf bfd  
sonic(config-if-Ethernet12)# no ip ospf bfd
```

Releases

3.1 or later

ip ospf bfd profile

Configures BFD profile on OSPFv2 interface.

Command

```
ip ospf bfd profile profile-name
```

Options

profile-name — BFD profile name (up to 63 characters)

Modes

INTERFACE

Usage

Use this command to enable on an Ethernet, PortChannel, or VLAN interface.

Examples

```
sonic(config)# interface Ethernet 1  
sonic(config-if-Ethernet1)# ip ospf bfd profile profile1  
sonic(config-if-Ethernet1)#
```

Releases

4.0 or later

ip ospf cost

Specifies the cost of sending a packet on an interface.

Command

```
ip ospf cost interface-cost [ip-address]
```

Options

- *interface-cost*—OSPF cost for the interface (1 to 65335; default is 10)
- *ip-address*—(Optional) IP address in A.B.C.D format

Modes

INTERFACE

Usage

If not configured, the interface cost is based on [auto-cost](#). This command configures OSPF over multiple vendors to ensure that all routers use the same cost. If you manually configure the cost, the calculated cost based on the reference bandwidth does not apply to an Ethernet, PortChannel, Loopback, or VLAN interface.

Examples

```
sonic(config)# interface Ethernet 1/2  
sonic(config-if-Ethernet1/2)# ip ospf cost 10  
  
sonic(config-if-Ethernet1/2)# no ip ospf cost
```

Releases

3.1 or later

ip ospf dead-interval

Sets the time period for hello packets must not have been seen before neighbors declare the router down.

Command

```
ip ospf dead-interval {{[deadinterval [ip-address]]) | {[minimal {[hello-  
multiplier {helломultiplier [ip-address]}}]}}}}
```

Options

- *deadinterval*—(Optional) Interval in seconds during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list, and does not participate in routing (1 to 65535; default is 40); this value must be the same for all nodes on the network

- *ip-address*—(Optional) IP address in A.B.C.D format
- *minimal*—(Optional) Sets the dead interval to 1 second; using this keyword requires that the *hello-multiplier* also be configured
- *hellomultiplier*—(Optional) Hello multiplier value representing the number of hello packets sent during one second (3 to 20)

Modes

INTERFACE

Usage

The dead interval is advertised in OSPF hello packets, and this value must be the same for all devices on the network. Specifying a smaller dead interval provides faster detection of a neighbor being down and improve convergence, but may cause routing instability. The dead interval is four times the default hello-interval by default. After the interval elapses, the neighboring router declares the router dead.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf dead-interval 10

sonic(config-if-Ethernet1/2)# no ip ospf dead-interval
```

Releases

3.1 or later

ip ospf hello-interval

Sets the interval between hello packets that are sent on an interface.

Commandip ospf hello-interval {*hellointerval* [*ip-address*]}**Options**

- *hellointerval*—Hello-interval value in seconds (1 to 65535; default 10)
- *ip-address*—(Optional) IP address in A.B.C.D format

Modes

INTERFACE

Usage

When you configure hello-interval for OSPF, the OSPF dead-interval value is implicitly set to a value four times greater than the hello-interval value. This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes are detected, but more routing traffic ensues. The value must be the same for all routers on the network. To return to the default time, use the no form of this command.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf hello-interval 30

sonic(config-if-Ethernet1/2)# no ip ospf hello-interval
```

Releases

3.1 or later

ip ospf message-digest-key

Enables OSPF MD5 authentication and sends an OSPF message digest key on an interface.

Commandip ospf message-digest-key *keyid* {md5 {*md5key* {[*encrypted ip-address*]}} [*ip-address*]}}**Options**

- *keyid*—MD5 key ID for the interface (1 to 255)
- *md5key*—MD5 password (up to 16 characters)
- *ip-address*—(Optional) IP address in A.B.C.D format

Modes

INTERFACE

Usage

One key per interface is used to generate authentication information when sending packets, and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value. The system assumes that its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated in different ways. Rollover

allows neighboring routers to continue to communicate while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor that is authenticated by the new key. After all neighbors have been updated with the new key, use the `no` form of this command to remove the old key.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf message-digest-key 10 md5 mDpa$S
$woRd

sonic(config-if-Ethernet1/2)# no ip ospf message-digest-key
```

Releases

3.2 or later

ip ospf mtu-ignore

Disables maximum transmission unit (MTU) mismatch detection on receiving packets when forming OSPFv3 adjacency.

Command

`ip ospf mtu-ignore [ip-address]`

Options

`ip-address`—(Optional) IP address in A.B.C.D format

Modes

INTERFACE

Usage

OSPF checks if neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange packets. If the MTU size of the peer interface is greater than the local interface, devices that run OSPF do not form adjacencies with neighbors. Use this command to override this behavior and form adjacency. If you try to disable neighborship with the `no` form of this command after a neighborship is formed, the neighborship continues. MTU mismatch detection is enabled by default.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf mtu-ignore

sonic(config-if-Ethernet1/2)# no ip ospf mtu-ignore
```

Releases

3.1 or later

ip ospf network

Sets the network type for an interface.

Command

`ip ospf network {broadcast | point-to-point}`

Options

- `broadcast`—Sets the interface as part of a broadcast network (default)
- `point-to-point`—Sets the interface as part of a point-to-point network

Modes

INTERFACE

Usage

Use this command to configure the OSPFv2 interface network type. Configuring networks as broadcast assumes that there are virtual circuits from every router to every router. Routing between two routers that are not directly connected go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature. If this command is issued on an interface that does not allow it, this command is ignored.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf network point-to-point
```

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf network broadcast
```

```
sonic(config-if-Ethernet1/2)# no ip ospf network
```

Releases

3.1 or later

ip ospf priority

Sets the router priority which helps determine the designated router (DR) for this network.

Command

```
ip ospf priority priorityval [ip-address]
```

Options

- *priorityval*—Router priority number (0 to 255; default 1)
- *ip-address*—(Optional) IP address in A.B.C.D format

Modes

INTERFACE

Usage

Use this command to set the priority of the interface to determine the DR for the OSPF network. When two routers that are attached to a network attempt to become the DR, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the DR or backup DR.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf priority 19
```

```
sonic(config-if-Ethernet1/2)# no ip ospf priority
```

Releases

3.1 or later

ip ospf retransmit-interval

Specifies the time between link-state advertisement (LSA) transmissions for adjacencies belonging to an interface.

Command

```
ip ospf retransmit-interval retransmitinterval [ip-address]
```

Options

- *retransmitinterval*—Value in seconds as the interval between retransmission (1 to 3600; default is 5)
- *ip-address*—(Optional) IP address in A.B.C.D format

Modes

INTERFACE

Usage

Use this command to set the time interval to a number large enough to avoid unnecessary retransmission. When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it resends the LSA. The *seconds* value should be greater than the expected round-trip delay between any two routers on the attached network. The setting of this option should also be conservative, or needless LSA retransmissions may occur.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip ospf retransmit-interval 35
```

```
sonic(config-if-Ethernet1/2)# no ip ospf retransmit-interval
```

Releases

3.1 or later

ip ospf transmit-delay

Sets the estimated time that is required to set a link state update packet on an interface.

Command	<code>ip ospf transmit-delay <i>transmitdelay</i> [<i>ip-address</i>]</code>
Options	<ul style="list-style-type: none">• <i>transmitdelay</i>—Time in seconds required to send a link state update (1 to 3600; default is 1)• <i>ip-address</i>—(Optional) IP address in A.B.C.D format
Modes	INTERFACE
Usage	When you set the transmit delay value, take into account the transmission and propagation delays for the interface.
Examples	<pre>sonic(config)# interface Ethernet 1/2 sonic(config-if-Ethernet1/2)# ip ospf transmit-delay 35</pre> <pre>sonic(config-if-Ethernet1/2)# no ip ospf transmit-delay</pre>
Releases	3.1 or later

ip pim

Configures global protocol-independent multicast (PIM) parameters.

Command	<code>ip pim [vrf <i>vrf-name</i>] {{ecmp [rebalance]} {join-prune-interval <i>jpi</i>} {keep-alive-timer <i>kat</i>} {ssm {prefix-list <i>pln</i>}}}</code>
Options	<ul style="list-style-type: none">• <i>vrf-name</i> — (Optional) VRF name prefixed by Vrf• <i>jpi</i> — Join prune interval value (60 to 600 seconds)• <i>kat</i> — Keepalive timer value (31 to 60000 seconds)• <i>pln</i> — Prefix-list number
Command mode	CONFIG
Usage	All commands are run per VRF. If the VRF is not specified, the command is run in default VRF context. Once PIM global configurations are done on a specified non-default VRF, that VRF cannot be deleted from the system until relevant PIM configurations are cleared. <ul style="list-style-type: none">• <i>join-prune-interval</i> — Configures the frequency of join/prune messages on the specified interface.• <i>keep-alive-timer</i> — Configures the keepalive timer for the period after the last (S,G) data packets during which (S,G) join state is even in the absence of (S,G) join messages• <i>ssm prefix-list</i> — Configures other multicast group addresses as the PIM-SSM range using the IP prefix-list. You can create the corresponding ip prefix-list using ip prefix-list, then associate that prefix-list to the PIM. The IP prefix-list cannot be deleted from the system until after removal of any PIM global configuration which refers to the prefix-list.• <i>ecmp</i> — Configures rebalancing of ECMP next-hops; if this option is not specified, the first next-hop found is used

Examples

```
sonic(config)# ip pim join-prune-interval 75  
sonic(config)# ip pim vrf Vrf1 join-prune-interval 70  
sonic(config)# ip pim keep-alive-timer 35  
sonic(config)# ip pim vrf Vrf1 keep-alive-timer 45  
sonic(config)# ip pim prefix-list pim_ssm_pfx_list  
sonic(config)# ip pim vrf Vrf1 prefix-list pim_ssm_pfx_list  
sonic(config)# ip pim ecmp  
sonic(config)# ip pim vrf Vrf1 ecmp  
sonic(config)# ip pim ecmp rebalance  
sonic(config)# ip pim vrf Vrf1 ecmp rebalance  
sonic(config)# no ip pim
```

Releases

3.2 or later

ip pim bfd

Enables BFD processing for PIM on a specified interface.

Command ip pim bfd**Options** None**Command mode** INTERFACE**Usage** Use this command to enable BFD on an Ethernet, PortChannel, or VLAN interface.**Examples**

```
sonic(config-if-Ethernet12)# ip pim bfd  
sonic(config-if-Vlan10)# ip pim bfd  
sonic(config-if-Ethernet12)# no ip pim bfd
```

Releases

3.2 or later

ip pim bfd profile

Enables BFD profile for PIM on the given interface.

Command ip pim bfd profile *profile-name***Options** *profile-name* — BFD profile name (up to 63 characters)**Modes** INTERFACE**Usage** Use this command to enable on an Ethernet, PortChannel, or VLAN interface.

Examples

```
sonic(config)# interface Ethernet 1
sonic(config-if-Ethernet1)# ip pim bfd profile bgp
sonic(config-if-Ethernet1)#{
```

Releases

4.0 or later

ip pim drpriority

Sets the designated router (DR) priority.

Command ip pim drpriority *drprio*

Options *drprio*—Designated router priority (1 to 4294967295)

Command mode INTERFACE

Usage Use this command to set the DR priority on an Ethernet, PortChannel, or VLAN interface. This command sets the priority of a node for becoming the DR on a network to which the interface is attached. A higher value means a higher chance of being elected.

Examples

```
sonic(config)# interface Ethernet 1/2
sonic(config-if-Ethernet1/2)# ip pim drpriority 100

sonic(config-if-po10)# ip pim drpriority 10

sonic(config-if-Vlan100)# ip pim drpriority 10

sonic(config-if-Ethernet1/2)# no ip pim drpriority
```

Releases

3.2 or later

ip pim hello

Sets the periodic interval for hello messages to keep the PIM neighbor session alive.

Command ip pim hello *hello*

Options *hello* — Hello interval (1 to 255 seconds)

Command mode INTERFACE

Usage Use this command to set the hello interval on an Ethernet, PortChannel, or VLAN interface. This configuration internally configures the default hold-time (3.5 * hello-interval); the period to keep the PIM neighbor session alive without receiving hello messages from that particular neighbor.

Examples

```
sonic(config-if-Ethernet12)# ip pim hello 30

sonic(config-if-po10)# ip pim hello 30

sonic(config-if-Vlan100)# ip pim hello 30

sonic(config-if-Ethernet12)# no ip pim hello
```

Releases

3.2 or later

ip pim sparse-mode

Enables PIM sparse mode.

Command	ip pim sparse-mode
Options	None
Command mode	INTERFACE
Usage	Use this command to enable PIM sparse mode on an Ethernet, PortChannel, or VLAN interface.
Examples	<pre>sonic(config-if-Ethernet12)# ip pim sparse-mode</pre> <pre>sonic(config-if-po10)# ip pim sparse-mode</pre> <pre>sonic(config-if-Vlan100)# ip pim sparse-mode</pre> <pre>sonic(config-if-Ethernet12)# no ip pim sparse-mode</pre>
Releases	3.2 or later

ip prefix-list

Builds a prefix-list.

Command	ip prefix-list <i>prefix-name</i> {seq { <i>seq-no</i> {{permit { <i>ipv4-prefix</i> {[ge <i>ge-min-prefix-length</i>] } {[le <i>le-max-prefix-length</i>] }}} {deny { <i>ipv4-prefix</i> {[ge <i>ge-min-prefix-length</i>] } {[le <i>le-max-prefix-length</i>] }}}}}}
Options	<ul style="list-style-type: none">• <i>prefix-name</i>—Name of the prefix-name• <i>seq-no</i>—Sequence number (1 to 4294967295)• <i>ipv4-prefix</i>—Source network address and mask in A.B.C.D/mask format• <i>ge-min-prefix-length</i>—Greater than or equal to the range specified• <i>le-max-prefix-length</i>—Less than or equal to the range specified
Command mode	CONFIGURATION
Usage	Use this command to create a prefix list with permit and deny statements for matching routes.
Examples	<pre>sonic(config)# ip prefix-list allowprefix seq 10 permit 10.10.10.1/16 ge 10</pre> <pre>sonic(config)# no ip prefix-list allowprefix seq 10 permit 10.10.10.1/16 ge 10</pre>
Releases	3.1 or later

ip protocol

Sets the route-map in the routing filter configuration for ARS.

Command	ip protocol any route-map <i>map-name</i> [vrf <i>vrf-name</i>]
Options	<ul style="list-style-type: none">• <i>map-name</i>—Enter a route-map name.• <i>vrf-name</i>—(Optional) Enter the VRF name.
Modes	CONFIGURATION
Usage	After you apply this filter, the routes have an ARS object that is bound to the NHG.

Example

```
sonic(config) # ip protocol any route-map ars-map
```

Releases

4.4.0 or later

ipv6 protocol

Sets the route-map in the routing filter configuration for ARS.

Command

```
ipv6 protocol any route-map map-name [vrf vrf-name]
```

Options

- *map-name*—Enter a route-map name.
- *vrf-name*—(Optional) Enter the VRF name.

Modes

CONFIGURATION

Usage

After you apply this filter, the routes have an ARS object that is bound to the NHG.

Example

```
sonic(config) # ipv6 protocol any route-map ars-map
```

Releases

4.4.0 or later

ip reserve local-neigh

Configures value to reserve host table entries for local hosts.

Command

```
ip reserve local-neigh num
```

Options

num—Number of local neighbors to be reserved (0 to 32000; default is 0)

Modes

CONFIGURATION

Usage

Use this command to preconfigure the host table capacity for ARP entries from local hosts.

(i) NOTE: Reserving host table space for ARP entries from local hosts is a software-based limit check.
There is no hardware partitioning.

Examples

```
sonic# configure terminal  
sonic(config) # ip reserve local-neigh 655
```

Releases

4.0 or later

ip rest

Configures authentication settings for the REST API.

Command

```
ip rest {log-level severity-level | port {number | shutdown} | read-timeout seconds | request-limit number | security-profile profile-name | vrf vrf-name}
```

Options

- *log-level severity-level* — Enter the severity level of messages to be logged for debugging (1-7), where lower numbers indicate more severe conditions: alerts for immediate action (1), critical conditions (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7); no default.
- *port number* — Enter the TCP port number used by the REST server to receive REST requests (1-65535; default 443).
- *port shutdown* — Disable the REST server listening port.
- *read-timeout seconds* — Enter the time (in seconds) that the REST server waits for a valid HTTP request to reach a switch resource on a REST API connection (0 for disabled; no maximum; default 0).

- `request-limit number` — Enter the number of concurrent requests allowed by the REST server (from 0 for disabled to any positive number for the number of concurrent requests supported; no maximum; default 0).
- `security-profile profile-name` — Enter the name of a security profile used by the REST API.
- `vrf vrf-name` — Enable REST API service in the specified VRF. If you do not configure a VRF, the REST service listens on all VRF instances.

Modes

CONFIGURATION

UsageTo reconfigure REST API authentication modes, use the [ip rest authentication](#) command.**Examples**

```
sonic(config)# ip rest log-level 4 request-limit 20
```

Releases

4.1.0 or later

ip rest authentication

Configures authentication modes for the REST API.

Command`ip rest authentication auth_mode`**Options**`auth_mode` — Where `auth_mode` is one or more of the following values that are separated by commas:

- `password` — Enable HTTP password authentication.
- `jwt` — Enable JWT token-based authentication.
- `cert` — Enable certificate-based authentication.
- `none` — Remove the configured authentication modes, and restore the defaults: HTTP password and JWT authentication.

Modes

CONFIGURATION

UsageEnter multiple values for `auth_mode` by separating them with a comma. To configure various settings used in REST API authentication, use the [ip rest](#) command.**Examples**

```
sonic(config)# ip rest authentication password,jwt,cert
```

Releases

4.1.0 or later

ip rest cipher-suite

Configures the REST server cipher suite with the cryptographic algorithms used for secure communication between the REST server running in an Enterprise SONiC switch and REST clients that are external to the switch, such as Swagger.

Command`ip rest cipher-suite {[ecdhe-ecdsa-with-aes-256-gcm-SHA384] [ecdhe-ecdsa-withchacha20-poly1305-SHA256] [ecdhe-ecdsa-with-aes-128-gcm-SHA256]}`**Options**

- `cipher-suite {[ecdhe-ecdsa-with-aes-256-gcm-SHA384] [ecdhe-ecdsa-withchacha20-poly1305-SHA256] [ecdhe-ecdsa-with-aes-128-gcm-SHA256]}` — Enter the REST cipher algorithms supported for encrypted REST server connections with external clients. Separate cipher-suite entries with a comma. By default, all three cipher suites are enabled.

Mode

CONFIGURATION

UsageThe Enterprise SONiC REST server typically negotiates the cipher suite with a REST client during the SSL/TLS handshake process. The server then selects the most secure cipher suite (TLSv1.2) that is supported by both the server and the client. To unconfigure SSH client cipher algorithms, enter the `no ip rest cipher-suite` command.

Examples

```
sonic(config)# ip rest cipher-suite ecdhe-ecdsa-with-aes-256-gcm-
SHA384,ecdhe-ec
dsa-with-chacha20-poly1305-SHA256
```

```
sonic(config)# no ip rest cipher-suite
```

Releases

4.4.1 or later

ip rest security-profile

Enables a security profile for the REST service.

Command

```
ip rest security-profile profile-name
```

Options

profile-name — Enter the name of a security profile.

Modes

CONFIGURATION

Usage

When the REST server restarts, it uses the new certificate. To create a security profile, use the [crypto security-profile](#) command. To associate a certificate/key pair with the security profile, use the [crypto security-profile certificate](#) command.

Examples

```
sonic(config)# ip rest security-profile myserver
```

Releases

4.1.0 or later

ip route

Assigns a static route on the network device.

Command

```
ip route [vrf {mgmt | vrf-name}] prefix {{interface {ifname {[nexthop-vrf
{next-hop-vrf {[tag {tag-val [pref]}]} [pref]}]} | {[tag {tag-val [pref]}]} |
[pref]}]}} | {[blackhole {[tag {tag-val [pref]}]} [pref]} | {[nexthop-addr
{{[interface {ifname {[{nexthop-vrf {next-hop-vrf {[tag {tag-val {[track
{trackid [pref]}]} [pref]}]} [pref]}]} {[track {trackid [pref]}]}]} | {[track
{trackid [pref]}]} | {[tag {tag-val {[track {trackid [pref]}]} [pref]}]} | {[tag
{tag-val {[track {trackid [pref]}]} [pref]}]} | {[pref] | {[track {trackid [pref]}]} | {[nexthop-vrf {next-hop-vrf {[tag
{tag-val {[track {trackid [pref]}]} [pref]}]} [pref]}]} {[track {trackid
[pref]}]}]}]}}}}}
```

Options

- *prefix*—Destination IP prefix in A.B.C.D/mask format
- *ifname*—Interface type; select Ethernet, PortChannel, Vlan, or null
- *next-hop-vrf*—(Optional) Next-hop VRF (up to 15 characters)
- *tag-val*—(Optional) Tag value (1 to 4294967295)
- *pref*—(Optional) Preference range (1 to 255)
- *next-hop-addr*—(Optional) Next-hop IP address in A.B.C.D format
- *trackid*—(Optional) Track ID

Modes

CONFIGURATION

Usage

Use this command to configure a static IPv4 route on the network device.

Examples

```
sonic(config)# ip route 200.200.200.0/24 interface Ethernet next-hop-vrf Vrf1 10
```

```
sonic(config)# no ip route 200.200.200.0/24 interface Ethernet next-hop-vrf Vrf1 10
```

Releases

3.1 or later

ip sla

Configures Internet protocol service level agreement (IP SLA).

Command ip sla *sla-id*

Options *sla-id* — Enter the SLA ID. The range is from one to 255.

Modes CONFIGURATION

Usage Use the ip sla command to configure ICMP or TCP-based IP SLA.

Examples

```
sonic(config)# ip sla 10
```

```
sonic(config)# no ip sla
```

Releases 3.1 or later

ip source binding

Create a static DHCPv4 snooping binding entry.

Command ip source binding *ip-addressmac-address vlan vlan-id {Ethernet phy-if-name | PortChannel port-channel-id}*

Options

- *ip-address*—IP address in A.B.C.D format
- *mac-address*—MAC address in nn:nn:nn:nn:nn:nn format
- *phy-if-name*—Ethernet interface name
- *port-channel-id*—PortChannel ID (1 to 256)

Modes CONFIGURATION

Usage

Use this command to create a static DHCPv4 snooping binding entry.

Examples

```
sonic# configure terminal
sonic(config)# ip source binding 10.1.1.1 00:00:00:00:00:01 Vlan 100
Ethernet15
```

Releases 4.0 or later

ip ssh

Configures Secure Shell (SSH) settings.

Command ip ssh {[disable-forwarding {true | false}] [ciphers {[aes128-ctr] [aes192-ctr] [aes256-ctr] [chacha20-poly1305@openssh.com] [aes128-gcm@openssh.com] [aes256-gcm@openssh.com]}] [macs {[umac-128-etm@openssh.com] [hmac-sha2-256-etm@openssh.com] [hmac-sha2-512-etm@openssh.com] [umac-128@openssh.com] [hmac-sha2-256] [hmac-sha2-51]}] [kexalgorithms {[curve25519-sha256] [curve25519-sha256@libssh.org] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group14-sha256]}] [] [x11-forwarding {true | false}] [permit-root-login {true | false}] [permit-user-rc {true | false}] [permit-user-environment{true | false}] [max-auth-retries *number*] }

Options

- *disable-forwarding {true | false}* — Enter true to globally disable all forwarding features, including TCP, local, dynamic, and remote forwarding. The default is false).
- *ciphers {[aes128-ctr] [aes192-ctr] [aes256-ctr] [chacha20-poly1305@openssh.com] [aes128-gcm@openssh.com] [aes256-gcm@openssh.com]}*

- the ciphers supported for encrypted connections with remote servers. Separate cipher entries with a comma. Default: aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305@openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com.
- macs {[umac-128-etm@openssh.com] [hmac-sha2-256-etm@openssh.com] [hmac-sha2-512-etm@openssh.com] [umac-128@openssh.com] [hmac-sha2-256] [hmac-sha2-51]} — Enter the MAC algorithms supported for connections with remote servers. Separate MAC algorithm entries with a comma. Default: umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-51.
- kexalgorithms {[curve25519-sha256] [curve25519-sha256@libssh.org] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group14-sha256]} — Enter the key exchange algorithms supported by SSH to exchange a shared session key in remote connections. Separate kexalgorithm entries with a comma. Default: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256.
- x11-forwarding {true | false} — Enter true to support X11 forwarding that allows graphical applications running on a remote server to be displayed on the switch. The default is false.
- permit-root-login {true | false} — Enter true to allow a root user to log on to the switch using SSH. The default is false.
- permit-user-rc {true | false} — Enter true to allow users to execute the commands in the SSH startup file (~/.ssh/rc file). The default is true.
- permit-user-environment{true | false} — Enter true to allow users to set environment variables in the SSH ~/ssh/environment file. The default is false.
- max-auth-retries number — Enter the maximum number of authentication attempts allowed per SSH connection (0 to 10; default 3).

Mode

CONFIGURATION

Usage

Enterprise SONiC uses SSHv2 as its connection protocol for secure connectivity over a network. SSH functions in both IPv4 and IPv6 connections. SSH supports terminal connections, tunneling, and user authentication using RADIUS or TACACS+ servers. Enter the no version of a command to unconfigure the parameter and return it to its default setting.

Examples

```
sonic(config)# sonic(config)# ip ssh disable-forwarding true
sonic(config)# ip ssh ciphers aes128-ctr,aes256-ctr,aes256-gcm@openssh.com
sonic(config)# ip ssh macs umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com
sonic(config)# ip ssh kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256
sonic(config)# ip ssh x11-forwarding true
sonic(config)# ip ssh permit-root-login true
sonic(config)# ip ssh permit-user-rc false
sonic(config)# ip ssh permit-user-environment true
sonic(config)# ip ssh max-auth-retries 7

sonic(config)# no ip ssh ciphers
```

Releases

4.4.0 or later

ip ssh client ciphers

Configures SSH client cipher algorithms.

Command

```
ip ssh client ciphers {[aes128-ctr] [aes192-ctr] [aes256-ctr] [chacha20-poly1305@openssh.com] [aes128-gcm@openssh.com] [aes256-gcm@openssh.com]}
```

Options

- ciphers {[aes128-ctr] [aes192-ctr] [aes256-ctr] [chacha20-poly1305@openssh.com] [aes128-gcm@openssh.com] [aes256-gcm@openssh.com]} — Enter the cipher algorithms supported for encrypted SSH client connections with remote servers. Separate cipher entries with a comma. There is no default value.

Mode	CONFIGURATION
Usage	<p>The SSH client feature provides secure, encrypted connections to a remote SSH server, and consists of SSH keys and SSH client algorithms. Configure the SSH cipher algorithms used to encrypt data transmitted over SSH connections, such as AES. Configure algorithms that provide strong encryption security and performance. Consider factors such as key size, block size, and resistance to attacks. By default, SSH client ciphers are not configured. To unconfigure SSH client cipher algorithms, enter the no ip ssh client ciphers command.</p>
Examples	<pre>sonic(config)# ip ssh client ciphers aes256-ctr,chacha20- poly1305@openssh.com</pre> <pre>sonic(config)# no ip ssh client ciphers</pre>
Releases	4.4.1 or later

ip ssh client kexalgorithms

Configures key exchange algorithms (kexalgorithms) used by SSH to exchange a shared-session key in remote connections.

Command	ip ssh client kexalgorithms {[curve25519-sha256] [curve25519-sha256@libssh.org] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group14-sha256]}
Options	<ul style="list-style-type: none"> • kexalgorithms {[curve25519-sha256] [curve25519-sha256@libssh.org] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group14-sha256]} — Enter the kexalgorithms supported for encrypted SSH client connections with remote servers. Separate kexalgorithm entries with a comma. There is no default value.
Mode	CONFIGURATION
Usage	<p>The SSH client feature provides secure, encrypted connections to a remote SSH server, and consists of SSH keys and SSH client algorithms. When you configure the SSH key exchange algorithms that are used to encrypt data transmitted over SSH connections, consider factors such as key size, computational complexity, and resistance to attacks. By default, SSH client kexalgorithms are not configured. Enter the no ip ssh client kexalgorithms command to unconfigure SSH client kexalgorithms.</p>
Examples	<pre>sonic(config)# ip ssh client kexalgorithms ecdh-sha2-nistp256,diffie- hellman-group-exchange-sha256</pre> <pre>sonic(config)# no ip ssh client kexalgorithms</pre>
Releases	4.4.1 or later

ip ssh client macs

Configures the message authentication code (MAC) algorithms that are used in SSH connections.

Command	ip ssh client macs {[curve25519-sha256] [curve25519-sha256@libssh.org] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group14-sha256]}
Options	<ul style="list-style-type: none"> • macs {[umac-128-etm@openssh.com] [hmac-sha2-256-etm@openssh.com] [hmac-sha2-512-etm@openssh.com] [umac-128@openssh.com] [hmac-sha2-256] [hmac-sha2-512]} — Enter the MAC algorithms supported for encrypted SSH client connections with remote servers. Separate cipher entries with a comma. There is no default value.
Mode	CONFIGURATION

Usage	A MAC algorithm generates and verifies MAC codes (MACs) that ensure the integrity of SSH messages. By default, SSH client MAC algorithms are not configured. To unconfigure SSH MAC algorithms, enter the no ip ssh client macs command.
Examples	<pre>sonic(config)# ip ssh client macs hmac-sha2-256- etm@openssh.com,umac-128@openssh.com</pre> <pre>sonic(config)# no ip ssh client macs</pre>
Releases	4.4.1 or later

ip telemetry

Configures authentication settings for gNMI and the Telemetry service.

Command	ip telemetry {jwt-refresh <i>seconds</i> jwt-valid <i>seconds</i> log-level <i>severity-level</i> port <i>number</i> security-profile <i>profile-name</i> vrf <i>vrf-name</i> }
Options	<ul style="list-style-type: none"> • <i>jwt-refresh seconds</i> — Enter the time (in seconds) before a JWT token can be refreshed (minimum 0; no maximum; default 3600). • <i>jwt-valid seconds</i> — Enter the time (in seconds) that a JWT token is valid (minimum 0; no maximum; default 3600). • <i>log-level severity-level</i> — Enter the severity level of messages to be logged for debugging (1-7), where lower numbers indicate more severe conditions: alerts for immediate action (1), critical conditions (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7); no default. • <i>port number</i> — Enter the TCP port number used by the telemetry server to receive gNMI requests (1-65535; default 8080). • <i>security-profile profile-name</i> — Enter the name of a security profile used by gNMI. • <i>vrf vrf-name</i> — Enable gNMI and telemetry services in the specified VRF. If you do not configure a VRF, the gNMI Telemetry service listens on all VRF instances.
Modes	CONFIGURATION
Usage	To reconfigure gNMI authentication modes, use the ip telemetry authentication command.
Examples	<pre>sonic(config)# ip telemetry jwt-refresh 6000 jwt-valid 6000 log-level 4 request-limit 20</pre> <pre>sonic(config)# ip telemetry port 1234</pre>
Releases	4.1.0 or later

ip telemetry authentication

Configures authentication modes for telemetry services.

Command	ip telemetry authentication <i>auth_mode</i>
Options	<i>auth_mode</i> — Where <i>auth-mode</i> is one or more of the following values that are separated by commas: <ul style="list-style-type: none"> • <i>password</i> — Enable HTTP password authentication. • <i>jwt</i> — Enable JWT token-based authentication. • <i>cert</i> — Enable certificate-based authentication. • <i>none</i> — Disable all authentication modes.
Modes	CONFIGURATION
Usage	Use this command to configure the authentication modes used for gNMI. Enter multiple values for <i>auth-mode</i> by separating them with a comma.

Examples

```
sonic(config) # ip telemetry authentication password,jwt,cert
```

Releases

4.1.0 or later

ip telemetry security-profile

Enables a security profile for Telemetry services, such as gNMI.

Command `ip telemetry security-profile profile-name`

Options *profile-name* — Enter the name of a security profile.

Modes CONFIGURATION

Usage When the Telemetry server restarts, it uses the new security profile. To create a security profile, use the [crypto security-profile](#) command. To associate a certificate/key pair with the security profile, use the [crypto security-profile certificate](#) command.

Examples

```
sonic(config) # ip telemetry security-profile telemserver
```

Releases

4.1.0 or later

ip unnumbered

Configures an IPv4 unnumbered interface from an Ethernet or PortChannel donor interface.

Command `ip unnumbered donor-interface`

Options *donor-interface* — IPv4 interface name

Modes INTERFACE

Usage Use this command to configure an IPv4 unnumbered interface at the interface level.

Examples

```
sonic(config-if-Ethernet12) # ip unnumbered Loopback1
```

```
sonic(config-if-pol) # ip unnumbered Loopback1
```

```
sonic(config-if-Ethernet12) # no ip unnumbered  
sonic(config-if-pol) # no ip unnumbered
```

Releases

3.0 or later

ip vrf

Creates a non-default VRF instance.

Command `ip vrf vrf-name`

Options *vrf-name* — VRF name instance (up to 15 characters) prefixed with Vrf.

Modes CONFIGURATION

Usage Use this command to create a VRF instance to leak routes in one VRF instance to another using route targets.

Examples

```
sonic(config)# ip vrf Vrf1  
sonic(config)#  
  
sonic(config)# no ip vrf Vrf1
```

Releases

3.0 or later

ip vrf forwarding

Configures the interface forwarding table.

Command ip vrf forwarding {mgmt | vrf-name}

Options vrf-name — VRF name instance (up to 15 characters)

Modes INTERFACE

Usage Use this command to assign an Ethernet, PortChannel, VLAN, or Loopback interface to the source VRF instance.

Examples

```
sonic(config-if-Ethernet12)# ip vrf forwarding Vrf_red  
  
sonic(config-if-po10)# ip vrf forwarding Vrf_red  
  
sonic(config-if-Vlan100)# ip vrf forwarding Vrf_red  
  
sonic(config-if-Vlan100)# ip vrf forwarding mgmt  
  
sonic(config-if-Ethernet12)# no ip vrf forwarding Vrf_red
```

Releases

3.0 or later

ip vrf mgmt

Configures a Management interface VRF instance.

Command ip vrf mgmt

Options None

Modes CONFIGURATION

Usage Use this command to configure a management VRF instance. Management interface becomes automatically part of this instance.

Examples

```
sonic(config)# ip vrf mgmt  
  
sonic(config)# no ip vrf mgmt
```

Releases

3.0 or later

ipv6 access-group

Configures an IPv6 access-group.

Command ipv6 access-group access-list-name {in | out}

Options	<ul style="list-style-type: none"> • <i>access-list-name</i> — IPv6 ACL name (up to 63 characters) • <i>in</i> — Apply the ACL to incoming traffic • <i>out</i> — Apply the ACL to outgoing traffic
Modes	CONFIGURATION
Usage	IPv6 ACL must be created first to be applied. Only one ACL of a given type can be applied per interface, and per direction.
Examples	<pre>sonic(config)# ipv6 access-group ipv6acl-example in</pre> <pre>sonic(config)# no ipv6 access-group ipv6acl-example in</pre>
Releases	3.1 or later

ipv6 access-list

Configures an IPv6 access-list.

Command	<code>ipv6 access-list <i>access-list-name</i></code>
Options	<i>access-list-name</i> — IPv6 ACL name (up to 63 characters)
Modes	CONFIGURATION
Usage	ACL name must begin with A-Z, a-z or 0-9. Underscore and hyphens can be used except as the first character. ACL name must be unique across all ACL types.
Examples	<pre>sonic(config)# ipv6 access-list acl6</pre> <pre>sonic(config)# no ipv6 access-list acl6</pre>
Releases	3.1 or later

ipv6-acl

Configures key-profile for PAC-related IP ACLs.

Command	<code>ipv6-acl {egress ingress} key-profile pac</code>
Options	<ul style="list-style-type: none"> • <i>egress</i>—egress direction • <i>ingress</i>—ingress direction • <i>pac</i>—key-profile for PAC-related ACLs
Modes	TCAM
Usage	Use this command to configure key-profile for PAC-related IP ACLs. This command is supported only in the Lite bundles.
Examples	<pre>sonic# configure terminal</pre> <pre>sonic(config)# hardware</pre> <pre>sonic(config-hardware)# tcam</pre> <pre>sonic(config-hardware-tcam)# ipv6-acl egress key-profile pac</pre>
Releases	4.0 or later

ipv6 address

Configures a global unicast IPv6 address on an interface.

Command	<code>ipv6 address <i>addr</i></code>
Options	<code><i>addr</i></code> — IPv6 address in A::B/mask format
Modes	INTERFACE
Usage	Use this command to configure an IPv6 address for a physical, Loopback, PortChannel, VLAN, or Management interface.
Examples	<pre>sonic(config-if-Ethernet28) # ipv6 address 2111:dddd:0eee::22/64</pre> <pre>sonic(config-if-Ethernet28) # no ipv6 address 2111:dddd:0eee::22/64</pre>
Releases	3.0 or later

ipv6 anycast-address

Configures an IPv6 static anycast gateway address for an interface.

Command	<code>ipv6 anycast-address <i>anycast-addr</i></code>
Options	<code><i>anycast-addr</i></code> —IPv6 address in A::B/mask format
Modes	INTERFACE
Usage	Use the <code>ipv6 anycast-address</code> command to configure an IPv6 static anycast gateway address for a VLAN interface. To globally configure an anycast MAC address for the IPv6 static anycast address, use the <code>ipv6 anycast-mac-address</code> command.
Examples	<pre>sonic(config)# interface Vlan 5</pre> <pre>sonic(config-if-Vlan5) # ipv6 anycast-address 50::1/64</pre> <pre>sonic(config-if-Vlan5) # no ipv6 anycast-address 50::1/64</pre>
Releases	3.0 or later

ipv6 anycast-address enable

Enables or disabled IPv6 static anycast gateway functionality.

Command	<code>ipv6 anycast-address {enable disable}</code>
Options	<ul style="list-style-type: none"><code>enable</code>—Enables static anycast gateway functionality (default)<code>disable</code>—Disables static anycast gateway functionality
Modes	CONFIGURATION
Usage	Use this command to enable or disable IPv6 static anycast-address globally. By default, IPv6 anycast-address functionality is enabled.
Examples	<pre>sonic(config) # ipv6 anycast-address enable</pre> <pre>sonic(config) # no ipv6 anycast-address disable</pre>
Releases	3.1 or later

ipv6 dhcp snooping

Enables DHCPv6 snooping globally.

Command	ipv6 dhcp snooping
Options	None
Modes	CONFIGURATION
Usage	DHCP snooping is applicable only on physical interfaces and port channels.
Examples	Enable DHCPv6 snooping:

```
sonic-cl# configure terminal  
sonic-cl(config)# ipv6 dhcp snooping  
sonic-cl(config)#
```

Disable DHCPv6 snooping:

```
sonic-cl# configure terminal  
sonic-cl(config)# no ipv6 dhcp snooping  
sonic-cl(config)#
```

Releases	4.0 or later
-----------------	--------------

ipv6 dhcp snooping trust

Sets Trust mode for DHCPv6 snooping on an interface or interface range.

Command	ipv6 dhcp snooping trust
Options	None
Modes	INTERFACE
Usage	Use the no version of this command to disable DHCPv6 snooping trust.
Examples	<pre>sonic(config)#interface Ethernet10 sonic(config-if-Ethernet10)#ipv6 dhcp snooping trust</pre> <pre>sonic(config)#interface Ethernet10 sonic(config-if-Ethernet10)# no ipv6 dhcp snooping trust</pre>

Releases	4.0 or later
-----------------	--------------

ipv6 dhcp snooping verify mac-address

Enables or disables DHCPv6 snooping MAC address verification.

Command	ipv6 dhcp snooping verify mac-address
Options	None
Modes	CONFIGURATION
Usage	With DHCP snooping MAC address verification enabled, DHCP snooping verifies whether the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports. The source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet. Where there is a mismatch, DHCP snooping logs and drops the packet.

Examples	Enable DHCPv6 snooping MAC address verification:
<pre>sonic-cl# configure terminal sonic-cl(config)# ipv6 dhcp snooping verify mac-address sonic-cl(config)#{/pre></pre>	
	Disable DHCPv6 snooping MAC address verification:
<pre>sonic-cl# configure terminal sonic-cl(config)# no ipv6 dhcp snooping verify mac-address sonic-cl(config)#{/pre></pre>	

Releases	4.0 or later
-----------------	--------------

ipv6 dhcp snooping vlan

Enables or disables DHCPv6 snooping on a VLAN or multiple VLANs.

Command	<code>ipv6 dhcp snooping vlan <i>vlan-id</i></code>
Options	<i>vlan-id</i> — VLAN ID number or range (1 to 4094)
Modes	CONFIGURATION
Usage	Enter an individual VLAN ID or a range of VLAN IDs separated by hyphen. For example, 20, 142, 7-100.
Examples	Enable IPv6 DHCP snooping on a VLAN:

```
sonic# configure terminal
sonic(config)#ipv6 dhcp snooping vlan 100
```

Enable IPv6 DHCP snooping on a VLAN list:

```
sonic(config)# ipv6 dhcp snooping vlan 70-100
```

Disable IPv6 DHCP snooping on a VLAN:

```
sonic# configure terminal
sonic(config)#no ipv6 dhcp snooping vlan 100
```

Releases	4.0 or later
-----------------	--------------

ipv6 dhcp-relay

Adds DHCP-relay to an IPv6 interface.

Command	<code>ipv6 dhcp-relay <i>ipaddr1</i> {{{[vrf <i>vrfName</i>]}} {[[<i>ipaddr2</i> {[<i>ipaddr3</i> [<i>ipaddr4</i>]}]]]}}</code>
Options	<ul style="list-style-type: none"> • <i>ipaddr1</i> — IPv6 address in A::B format • <i>vrfName</i> — (Optional) VRF name (up to 32 characters) • <i>ipaddr2</i> — IPv6 address in A::B format • <i>ipaddr3</i> — IPv6 address in A::B format • <i>ipaddr4</i> — IPv6 address in A::B format
Modes	INTERFACE
Usage	Use this command to add DHCP-relay to an Ethernet, PortChannel, or VLAN IPv6 interface.
Examples	<pre>sonic(config-if-Ethernet28)# ipv6 dhcp-relay 2111:dddd:0eee::22/64</pre> <pre>sonic(config-if-Ethernet28)# no ipv6 dhcp-relay 2111:dddd:0eee::22/64</pre>

Releases	3.1 or later
-----------------	--------------

ipv6 dhcp-relay max-hop-count

Sets the maximum hop count for DHCPv6 relay packets.

Command	<code>ipv6 dhcp-relay max-hop-count <i>hop-count</i></code>
Options	<i>hop-count</i> —Maximum hop count (0 to 16; default is 10)
Modes	INTERFACE
Usage	Use this command to set the maximum hop count for an Ethernet, PortChannel, or VLAN interface.
Examples	<pre>sonic(config) # interface Ethernet28 sonic(config-if-Ethernet28) # ipv6 dhcp-relay max-hop-count 10 sonic(config-if-Ethernet28) # no ipv6 dhcp-relay max-hop-count</pre>

Releases	3.1 or later
-----------------	--------------

ipv6 dhcp-relay source-interface

Configures the source IPv6 address used for relaying DHCPv6 packets.

Command	<code>ipv6 dhcp-relay source-interface {<i>intfName</i> <i>pchName</i> <i>vlanName</i> <i>loName</i>}</code>
Options	<ul style="list-style-type: none">• <i>intfName</i>—Interface name• <i>pchName</i>—PortChannel number• <i>vlanName</i>—VLAN number• <i>loName</i>—Loopback number
Modes	INTERFACE
Usage	Use this command to set the IPv6 address on the specified interface as the source IPv6 address on relayed DHCPv6 packets. DHCPv6 server sends replies to this IPv6 address. This address should be reachable from the DHCPv6 server.
Examples	<pre>sonic(config) # interface Ethernet 28 sonic(config-if-Eth28) # ipv6 dhcp-relay source-interface Ethernet 12 sonic(config-if-Ethernet28) # no ipv6 dhcp-relay source-interface</pre>

Releases	3.2 or later
-----------------	--------------

ipv6 dhcp-relay vrf-select

Enables VRF selection.

Command	<code>ipv6 dhcp-relay vrf-select</code>
Options	None
Modes	INTERFACE
Usage	Use this command to enable VRF selection suboption (Virtual Subnet Selection - VSS) in DHCP relay. If the DHCP server supports this suboption, it uses this VRF information along with other information to assign IP to the DHCP client.

Examples

```
sonic(config) # interface Ethernet28
sonic(config-if-Ethernet28) # ipv6 dhcp-relay vrf-select

sonic(config-if-Ethernet28) # no ipv6 dhcp-relay vrf-select
```

Releases

3.1 or later

ipv6 drop-neighbor

Configures time in seconds for IPv6 drop-neighbor aging.

Command `ipv6 drop-neighbor aging-time time`**Options** *time*—Specify aging-time in seconds (60 to 14400; default is 300)**Modes** CONFIGURATION**Usage** Use this command to configure the aging interval for drop entry to enable ND protection for unresolved neighbors to protect the CPU.**Examples**

```
sonic(config) # ipv6 drop-neighbor aging-time 200
```

Releases

4.1.0 or later

ipv6 enable

Enables or disables IPv6 forwarding on an interface configured with an IPv6 address.

Command `ipv6 enable`**Options** None**Modes** INTERFACE**Usage** Use this command to disable and re-enable IPv6 forwarding on an Ethernet, PortChannel, Loopback or VLAN interface for security purposes, or to recover from a duplicate address discovery (DAD) failure.**Examples**

```
sonic(config-if-Ethernet28) # ipv6 enable
```

```
sonic(config-if-Ethernet28) # no ipv6 enable
```

Releases

3.1 or later

ipv6 nd adv-interval-option

Enables the advertisement interval option in router advertisements so that an IPv6 mobile device that joins the network knows that it can receive router advertisements.

Command `ipv6 nd adv-interval-option`**Options** None**Modes** INTERFACE**Usage** This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config) # interface Ethernet1/4
sonic(config-if-Eth1/4) # ipv6 nd adv-interval-option
```

```
sonic(config) # interface Vlan 10
sonic(config-if-Vlan10) # ipv6 nd adv-interval-option
```

```
sonic(config) # interface PortChannel 2
sonic(config-if-po2) # ipv6 nd adv-interval-option
```

Releases

4.0.3 or later

ipv6 nd cache

Configures the time in seconds for an IPv6 ND cache entry to expire.

Command `ipv6 nd cache {expire value}`**Options** `value`—Time in seconds for the cache entry to expire**Modes** CONFIGURATION**Usage** Use this command to change the expiry timer for IPv6 neighbor entries.**Examples**

```
sonic(config) # ipv6 nd cache expire 500
```

```
sonic(config) # no ipv6 nd cache expire
```

Releases

3.1 or later

ipv6 nd dnssl

Advertise the DNS search list in neighbor discovery messages, using the DNSSL (type 31) option as described in RFC8106.

Command `ipv6 nd dnssl domain-name-suffix [seconds | infinite]`**Options**

- `domain-name-suffix` — Enter a text string for a domain name suffix to identify DNS servers.
- `seconds | infinite` — (Optional) Enter the maximum time in seconds for which the specified domain suffix is used for domain name resolution (0-4294967295; default is three times the RA interval configured with the `ipv6 nd ra-interval` command). Enter 0 to specify that the domain name suffix is no longer used. Enter infinite to advertise the list of DNS servers for an infinite time.

Modes INTERFACE**Usage**

This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces. Re-enter the command to configure an additional DNS server list.

Examples

```
sonic(config-if-Eth1/4) # ipv6 nd dnssl powerswitch1 infinite
```

```
sonic(config-if-Vlan10) # ipv6 nd dnssl broadcom1 2000
```

```
sonic(config-if-po2) # ipv6 nd dnssl broadcom1 4000
```

Releases

4.0.3 or later

ipv6 nd home-agent-config-flag

Sets the home agent configuration flag in IPv6 router advertisements so that the router is identified by the same IPv6 address (mobile IP) even if it moves from one network to another.

Command `ipv6 nd home-agent-config-flag`

Options None

Modes INTERFACE

Usage When moving the router to a different network, connectivity is maintained seamlessly without user intervention. This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config-if-Eth1/4)# ipv6 nd home-agent-config-flag
```

```
sonic(config-if-Vlan10)# ipv6 nd home-agent-config-flag
```

```
sonic(config-if-po2)# ipv6 nd home-agent-config-flag
```

Releases

4.0.3 or later

ipv6 nd home-agent-lifetime

Sets the time that the router is considered as the home agent on the network.

Command `ipv6 nd home-agent-lifetime seconds`

Options *seconds* — Enter a time in seconds (0-65535; default 0).

Modes INTERFACE

Usage This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces. The value you set is applied only if the router has been configured as the home agent using the `ipv6 nd home-agent-config-flag` command.

Examples

```
sonic(config-if-Eth1/4)# ipv6 nd home-agent-lifetime 50000
```

```
sonic(config-if-Vlan10)# ipv6 nd home-agent-lifetime 50000
```

```
sonic(config-if-po2)# ipv6 nd home-agent-lifetime 50000
```

Releases

4.0.3 or later

ipv6 nd home-agent-preference

Sets the time that the router may have preferred home agent status.

Command `ipv6 nd home-agent-preference seconds`

Options *seconds* — Enter a time in seconds (0-65535; default 0).

Modes INTERFACE

Usage This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces. The value you set is applied only if the router has been configured as a home agent using the `ipv6 nd home-agent-config-flag` command.

Examples

```
sonic(config-if-Eth1/4)# ipv6 nd home-agent-preference 50000  
sonic(config-if-Vlan10)# ipv6 nd home-agent-preference 50000  
sonic(config-if-po2)# ipv6 nd home-agent-preference 50000
```

Releases

4.0.3 or later

ipv6 nd managed-config-flag

Sets the managed address configuration flag in IPv6 router advertisements so that host devices know to use stateful autoconfiguration to receive IPv6 addresses.

Command `ipv6 nd managed-config-flag`

Options None

Modes INTERFACE

Usage This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config-if-Eth1/4)# ipv6 nd managed-config-flag  
sonic(config-if-Vlan10)# ipv6 nd managed-config-flag  
sonic(config-if-po2)# ipv6 nd managed-config-flag
```

Releases

4.0.3 or later

ipv6 nd mtu

Sets the maximum transmission unit (MTU) size of IPv6 messages transmitted by the router.

Command `ipv6 nd mtu bytes`

Options *bytes* — Enter the maximum MTU size (1 to 65535; default 0).

Modes INTERFACE

Usage This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces. By default, no MTU size is advertised in IPv6 messages (default value 0).

Examples

```
sonic(config-if-Eth1/4)# ipv6 mtu bytes 25000  
sonic(config-if-Vlan10)# ipv6 nd mtu bytes 25000  
sonic(config-if-po2)# ipv6 nd mtu bytes 25000
```

Releases

4.0.3 or later

ipv6 nd other-config-flag

Sets the "other stateful configuration flag" in IPv6 router advertisements so that host devices can receive autoconfiguration information besides IPv6 addresses.

Command `ipv6 nd other-config-flag`

Options	None
Modes	INTERFACE
Usage	To receive non-address information, host devices should use stateful autoconfiguration. This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.
Examples	<pre>sonic(config-if-Eth1/4) # ipv6 nd other-config-flag</pre> <pre>sonic(config-if-Vlan10) # ipv6 nd other-config-flag</pre> <pre>sonic(config-if-po2) # ipv6 nd other-config-flag</pre>
Releases	4.0.3 or later

ipv6 nd prefix

Configures the IPv6 prefixes to be included in router advertisements for IPv6 neighbor discovery.

Command	<code>ipv6 nd prefix <i>ipv6-prefix/prefix-length</i> [<i>valid-lifetime</i>] [<i>preferred-lifetime</i>] [<i>off-link</i>] [<i>no-autoconfig</i>] [<i>router-address</i>]</code>
Options	<ul style="list-style-type: none"> • <i>ipv6-prefix/prefix-length</i> — Enter the IPv6 prefix in hexadecimal format with a prefix-length value. • <i>valid-lifetime</i> — (Optional) Enter the lifetime (in seconds) that the IPv6 prefix is advertised as a valid address (0 to 4294967295). • <i>preferred-lifetime</i> — (Optional) Enter the time (in seconds) that the IPv6 prefix is advertised as a preferred address (0 to 4294967295). • <i>off-link</i> — (Optional) Advertises the IPv6 prefix with the L-bit clear, and not add the prefix to the routing table as a Connected prefix. If the prefix was statically configured in the routing table, it is removed. • <i>no-autoconfig</i> — (Optional) Advertises the IPv6 prefix with the A-bit clear, and prevent hosts on the local link from using the prefix for IPv6 autoconfiguration. • <i>router-address</i> — (Optional) Sets the R flag to communicate to hosts on the local link that the specified prefix contains a complete IPv6 address.
Modes	INTERFACE
Usage	This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.
Examples	<pre>sonic(config-if-Eth1/4) # ipv6 nd prefix 20::2/64</pre> <pre>sonic(config-if-Vlan10) # ipv6 nd prefix off-link</pre> <pre>sonic(config-if-po2) # ipv6 nd prefix no-autoconfig router-address</pre>
Releases	4.0.3 or later

ipv6 nd ra-fast-retrans

Enables faster transmissions of RA packets to accelerate convergence and neighbor establishment, particularly for unnumbered peering.

Command	<code>ipv6 nd ra-fast-retrans</code>
Options	None
Modes	INTERFACE

Usage

RA fast retransmission is enabled by default. To disable it, enter the `no ipv6 nd ra-fast-retrans` command. Disabling RA fast retransmission is sometimes necessary to have IPv6 neighbor discovery compliant with the RFC by having slower convergence and neighbor establishment. To re-enable, RA fast retransmission, enter the `ipv6 nd ra-fast-retrans` command. This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config-if-Eth1/4)# no ipv6 nd ra-fast-retrans  
sonic(config-if-Vlan10)# no ipv6 nd ra-fast-retrans  
sonic(config-if-po2)# no ipv6 nd ra-fast-retrans  
sonic(config-if-Eth1/4)# ipv6 nd ra-fast-retrans
```

Releases

4.0.3 or later

ipv6 nd ra-hop-limit

Configures the maximum number of next hops supported in router advertisements.

Command

`ipv6 nd ra-hop-limit number`

Options

number — Enter a number of next hops (0-255; default 0).

Modes

INTERFACE

Usage

This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config-if-Eth1/4)# ipv6 nd ra-hop-limit 10  
  
sonic(config-if-Vlan10)# ipv6 nd ra-hop-limit 10  
  
sonic(config-if-po2)# ipv6 nd ra-hop-limit 10
```

Releases

4.0.3 or later

ipv6 nd ra-interval

Configures the interval that is used to send router advertisement messages for IPv6 neighbor discovery.

Command

`ipv6 nd ra-interval {seconds | msec milliseconds}`

Options

- *seconds* — Enter a time in seconds (1-1800; default 600).
- *msec milliseconds* — Enter a time in milliseconds (70-1800000).

Modes

INTERFACE

Usage

Specify a time in seconds (1-1800; default 600) or milliseconds (**msec** 70-1800000). This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config-if-Eth1/4)# ipv6 nd ra-interval 1200  
  
sonic(config-if-Vlan10)# ipv6 nd ra-interval 1200  
  
sonic(config-if-po2)# ipv6 nd ra-interval msec 1000000
```

Releases

4.0.3 or later

ipv6 nd ra-lifetime

Configures the time that the router is advertised as the default router.

Command	<code>ipv6 nd ra-lifetime <i>seconds</i></code>
Options	<i>seconds</i> — Enter a time in seconds (0-9000; default is 0).
Modes	INTERFACE
Usage	Enter 0 to configure the router as a nondefault router. The RA lifetime value should be greater than the RA interval time (ipv6 nd ra-interval). This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.
Examples	<pre>sonic(config-if-Eth1/4)# ipv6 nd ra-lifetime 1000</pre> <pre>sonic(config-if-Vlan10)# ipv6 nd ra-lifetime 1000</pre> <pre>sonic(config-if-po2)# ipv6 nd ra-lifetime 1000</pre>
Releases	4.0.3 or later

ipv6 nd ra-retrans-interval

Configures the time interval for resending consecutive Advertisement Retransmit messages.

Command	<code>ipv6 nd ra-retrans-interval <i>milliseconds</i></code>
Options	<i>milliseconds</i> — Enter a time in milliseconds (0-4294967295; default 0).
Modes	INTERFACE
Usage	Setting the value to zero indicates that the RA retransmission time is not specified by the router. This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.
Examples	<pre>sonic(config-if-Eth1/4)# ipv6 nd ra-retrans-interval 1000000</pre> <pre>sonic(config-if-Vlan10)# ipv6 nd ra-retrans-interval 1000000</pre> <pre>sonic(config-if-po2)# ipv6 nd ra-retrans-interval 1000000</pre>
Releases	4.0.3 or later

ipv6 nd rdnss

Configures a recursive domain name server to advertise in neighbor discovery messages using the RDNSS (type 25) option described in RFC8106.

Command	<code>ipv6 nd rdnss <i>ipv6-address</i> [<i>seconds</i> infinite]</code>
Options	<ul style="list-style-type: none">• <i>ipv6-address</i> — Enter an IPv6 address in hexadecimal format.• <i>seconds</i> infinite — (Optional) Enter the maximum time in seconds for which the specified IPv6 server address is used for domain name resolution (0-4294967295; default is three times the RA interval configured with the ipv6 nd ra-interval command). Enter 0 to specify that the IPv6 address is no longer used. Enter infinite to advertise a DNS server for an infinite time.
Modes	INTERFACE

Usage

This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces. Re-enter the command to configure additional recursive DNS servers. By default, no recursive domain name server is advertised.

Examples

```
sonic(config-if-Eth1/4) # ipv6 nd rdnss  
2001:0DB8:AC10:FE01:0000:0000:0000:0001
```

```
sonic(config-if-Vlan10) # ipv6 nd rdnss  
2001:0DB8:AC10:FE01:0000:0000:0000:0001 3000
```

```
sonic(config-if-po2) # ipv6 nd rdnss  
2001:0DB8:AC10:FE01:0000:0000:0000:0001
```

```
sonic(config-if-Eth1/4) # ipv6 nd rdnss 2001::1 infinite
```

Releases

4.0.3 or later

ipv6 nd reachable-time

Configures the time that an IPv6 neighbor is considered to be reachable after a reachability confirmation is received.

Command

`ipv6 nd reachable-time seconds`

Options

`seconds`—Enter a time in seconds (0-3600000; default 0).

Modes

INTERFACE

Usage

This command is supported on Ethernet, which is routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config)# interface Ethernet 1/4  
sonic(config-if-Eth1/4) # ipv6 nd reachable-time 1800000
```

```
sonic(config)# interface Vlan 10  
sonic(config-if-Vlan10) # ipv6 nd reachable-time 1800000
```

```
sonic(config)# interface PortChannel 10  
sonic(config-if-po2) # ipv6 nd reachable-time 1800000
```

Releases

4.0.3 or later

ipv6 nd router-preference

Configures the default router preference that is sent in router advertisements.

Command

`ipv6 nd router-preference value`

Options

`value` — Enter high, medium, or low to specify the default router preference (default medium).

Modes

INTERFACE

Usage

The default router preference is used by host devices to select the destination for IPv6 routing when two routers on a link provide equal next-hop routing. This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic(config-if-Eth1/4)# ipv6 nd router-preference high  
  
sonic(config-if-Vlan10)# ipv6 nd router-preference low  
  
sonic(config-if-po2)# ipv6 nd router-preference high
```

Releases

4.0.3 or later

ipv6 nd suppress-ra

Stops the router from sending router advertisement messages for IPv6 neighbor discovery.

Command `ipv6 nd suppress-ra`**Options** None**Modes** INTERFACE**Usage** This command is supported on Ethernet, routed VLAN, port channel interfaces and on subinterfaces. By default, sending router advertisement messages is disabled. You can enable sending router advertisements using the `no ipv6 nd suppress-ra` command.**Examples**

```
sonic(config-if-Eth1/4)# no ipv6 nd suppress-ra  
  
sonic(config-if-Vlan10)# no ipv6 nd suppress-ra  
  
sonic(config-if-po2)# no ipv6 nd suppress-ra  
  
sonic(config-if-Eth1/4)# ipv6 nd suppress-ra
```

Releases

4.0.3 or later

ipv6 neighbor

Configures a static ND.

Command `ipv6 neighbor static-ip mac-address`

- Options**
- *static-ip*—Static IPv6 address in A.B.C.D or A::B format
 - *mac-address*—Neighbor address in nn::nn format

Modes INTERFACE**Usage** Use this command to configure a static IPv6 neighbor entry in an interface.**Examples**

```
sonic(config)# interface Eth28  
sonic(config-if-Ethernet28)# ipv6 neighbor 1001:db8:a1::2  
00:22:33:44:55:66
```

```
sonic(config-if-Ethernet28)# no ipv6 neighbor 1001:db8:a1::2  
00:22:33:44:55:66
```

Releases

3.1 or later

ipv6 nht

Configures next hop resolution and tracking parameters using default route.

Command	ipv6 [vrf <i>vrf-name</i>] nht resolve-via-default
Options	<i>vrf-name</i> —(Optional) VRF name prefixed by Vrf
Modes	CONFIGURATION
Usage	Use this command to enable IPv6 next hop tracking to resolve using the default route.
Examples	<pre>sonic# configure terminal sonic(config)# ipv6 vrf Vrf-Blue nht resolve-via-default</pre>
Releases	4.0 or later

ipv6 prefix-list

Builds an IPv6 prefix-list.

Command	ipv6 prefix-list <i>prefix-name</i> {seq {seq-no {{permit { <i>ipv6-prefix</i> {[ge <i>ge-min-prefix-length</i>] } {[le <i>le-max-prefix-length</i>] }}} {deny { <i>ipv6-prefix</i> {[ge <i>ge-min-prefix-length</i>] } {[le <i>le-max-prefix-length</i>] }}}}}}
Options	<ul style="list-style-type: none"><i>prefix-name</i> — New prefix-list name<i>seq-no</i> — Sequence number (1 to 4294967295)<i>ipv6-prefix</i> — IPv6 prefix-list to permit or deny<i>ge-min-prefix-length</i> — (Optional) Indicates the prefix-list is greater than or equal to the range specified<i>le-max-prefix-length</i> — (Optional) Indicates the prefix-list is less than or equal to the range specified
Modes	CONFIGURATION
Usage	Use this command to create an IPv6 prefix-list to permit or deny route filtering from a specified prefix-list.
Examples	<pre>sonic(config)# ipv6 prefix-list TEST deny AB10::1/128 ge 10 le 30</pre> <pre>sonic(config)# no ipv6 prefix-list TEST deny AB10::1/128 ge 10 le 30</pre>
Releases	3.2 or later

ipv6 route

Specifies an IPv6 static route.

Command	ipv6 route [vrf {mgmt vrfname}] {prefix {{interface {ifname {[nexthop-vrf {[next-hop-vrf {[tag {tag-val [pref]}]} [pref]}]} {[tag {tag-val [pref]}]} {[pref]}]} {blackhole {[tag {tag-val [pref]}]} [pref]} {next-hop-addr {[interface {ifname {[nexthop-vrf {next-hop-vrf {[tag {tag-val {[track {trackid [pref]}]} [pref]}]} [pref]}]} {[track {trackid [pref]}]}]} {[track {trackid [pref]}]} {[tag {tag-val {[track {trackid [pref]}]} [pref]}]} {[pref]}]} {[tag {tag-val {[track {trackid [pref]}]} [pref]}]} {[track {trackid [pref]}]} {[nexthop-vrf {next-hop-vrf {[tag {tag-val {[track {trackid [pref]}]} [pref]}]} [pref]}]} {[track {trackid [pref]}]}]} {[tag {tag-val {[track {trackid [pref]}]} [pref]}]} {[track {trackid [pref]}]} {[nexthop-vrf {next-hop-vrf {[tag {tag-val {[track {trackid [pref]}]} [pref]}]} [pref]}]} {[track {trackid [pref]}]}]}}}
Options	<ul style="list-style-type: none"><i>vrfname</i>—VRF name starting with Vrf (up to 15 characters)

- *prefix*—IPv6 route prefix in A::B/mask format
- *ifname*—Interface type; select Ethernet, PortChannel, Loopback, or Vlan
- *next-hop-vrf*—(Optional) VRF name prefixed by Vrf (up to 15 characters)
- *tag-val*—(Optional) Tag value (1 to 4294967295)
- *pref*—(Optional) Preference range (1 to 255)
- *next-hop-addr*—(Optional) Next-hop address in A::B format
- *trackid*—(Optional) Track ID

Modes

CONFIGURATION

Usage

Use this command to configure a static IPv6 route on the network device.

Examples

```
sonic(config)# ipv6 route 2111:dddd:0eee::22/128 interface Ethernet nexthop-vrf Vrf1 10

sonic(config)# no ipv6 route 2111:dddd:0eee::22/128 interface Ethernet nexthop-vrf Vrf1 10
```

Releases

3.1 or later

ipv6 source binding

Create a static DHCPv6 snooping binding entry.

Command

```
ipv6 source binding ipv6-addressmac-address vlan vlan-id {Ethernet phy-if-name | PortChannel port-channel-id}
```

Options

- *ipv6-address*—IPv6 address in A::B format
- *mac-address*—MAC address in nn:nn:nn:nn:nn:nn format
- *phy-if-name*—Ethernet interface name
- *port-channel-id*—PortChannel ID (1 to 256)

Modes

CONFIGURATION

Usage

Use this command to create a static DHCPv6 snooping binding entry.

Examples

```
sonic# configure terminal
sonic(config)#ipv6 source binding 3001:1001:2001::2009 aa:bb:aa:bb:aa:08
Vlan2025 Eth1/3
```

Releases

4.0 or later

K, L, and M commands

Topics:

- kdump enable
- kdump memory
- kdump num-dumps
- keepalive-interval
- key config-key password-encrypt
- l2-nexthop-group
- lacp individual
- ldap-server
- ldap-server host
- ldap-server map
- ldap-server nss
- ldap-server pam
- ldap-server security-profile
- ldap-server source-interface
- ldap-server sudo
- ldap-server vrf
- line vty
- link state track
- link-error-disable
- listen limit
- listen range
- lldp
- lldp enable
- lldp med-tlv-select
- lldp multiplier
- lldp system-description
- lldp system-name
- lldp timer
- lldp tlv-select
- lldp tlv-set
- lldp vlan-name-tlv allowed vlan
- lldp vlan-name-tlv max-tlv-count
- load-current-max-val
- load-current-min-val
- load-future-max-val
- load-future-min-val
- load-future-weight
- load-past-max-val
- load-past-min-val
- load-past-weight
- load-scaling-factor
- local-as
- locator-led chassis
- log-adjacency-changes
- log-neighbor-changes
- logger
- logging security-profile

- logging server
- login exec-timeout
- login lockout
- login password-attributes
- mab
- mab request format
- mab timeout
- mac access-group
- mac access-list
- mac address-table
- mac address-table aging-time
- mac address-table dampening-interval
- mac address-table dampening-threshold
- mac-holdtime
- map
- match access-group
- match as-path
- match community
- match dei
- match destination-address
- match dscp
- match ethertype
- match evpn
- match ext-community
- match interface
- match ip protocol
- match ip address prefix-list
- match ip next-hop prefix-list
- match ipv6 address prefix-list
- match l4-port
- match local-preference
- match metric
- match origin
- match pcp
- match peer
- match protocol
- match source-address
- match source-protocol
- match source-vrf
- match tag
- match tcp-flags
- match vlan
- max-flows
- max-med
- max-metric
- maximum-paths
- maximum-paths ibgp
- maximum-prefix
- mclag
- mclag domain
- mclag gateway-mac
- mclag-peer-gateway
- mclag-separate-ip
- mclag-system-mac
- meter-type
- minimum-ttl

- mirror
- mirror-session
- mode
- monitoring-fbs
- mtu

kdump enable

Enables or disables the kernel core dump configuration in the startup configuration file.

Command `kdump enable`

Options None

Modes CONFIGURATION

Usage This command typically require a reboot to complete.

Examples

```
sonic(config) # kdump enable
KDUMP configuration has been updated in the startup configuration
Kdump configuration changes will be applied after the system reboots
```

```
sonic(config) # no kdump
KDUMP configuration has been updated in the startup configuration
ALERT! A system reboot is highly recommended.
Kdump configuration changes will be applied after the system reboots
```

Releases 3.0 or later

kdump memory

Sets or resets the amount of memory reserved for the kernel core dump files.

Command `kdump memory kdump_memory`

Options `kdump_memory` — Amount of memory reserved for kdump

Modes CONFIGURATION

Usage This command typically require a reboot to complete.

Examples

```
sonic(config) # kdump memory 512M
KDUMP configuration has been updated in the startup configuration
kdump updated memory will be only operational after the system reboots
```

```
sonic(config) # no kdump memory
```

Releases 3.0 or later

kdump num-dumps

Sets or resets the maximum number of kernel core files stored locally.

Command `kdump num-dumps kdump_num.dumps`

Options `kdump_num.dumps` — Maximum number of kdump files to store locally

Modes CONFIGURATION

Usage This command typically require a reboot to complete.

Examples

```
sonic(config) # kdump num-dump 5  
  
sonic(config) # no kdump num-dump
```

Releases

3.1 or later

keepalive-interval

Configures MCLAG session keepalive intervals.

Command

keepalive-interval *KA*

Options

KA — Keepalive time interval in seconds

Modes

CONFIGURATION

Usage

Use this command to configure the time interval between keepalive messages sent to the neighbor routers.

Example

```
sonic(config) # keepalive-interval 20
```

Releases

3.0 or later

key config-key password-encrypt

Configures a user-selected passphrase that is used to derive the primary encryption key.

Command

key config-key password-encrypt

Options

password-encrypt — Encryption key configuration

Modes

CONFIGURATION

Usage

Use the `key config-key password-encrypt` command to configure a user-configured primary encryption key (PEK). A TACACS+ server configuration cannot be copied from one switch to another unless the same PEK passphrase is configured on both devices. If you do not configure a primary encryption key, the switch uses the default PEK.

Examples

```
sonic# configure terminal  
sonic(config) # key config-key password-encrypt  
Primary encryption key update will re-encrypt protocol passwords and  
save the system configuration to be persistent. [confirm Y/N]: y  
New key:  
Confirm key:
```

```
sonic(config) # no key config-key password-encrypt  
WARNING: System will default to device specific primary encryption key.  
[confirm Y/N]:
```

Releases

4.0 or later

l2-nexthop-group

Sets the forwarding database (FDB) table in wide mode.

Command

l2-nexthop-group

Options

None

Modes	SWITCH-RESOURCE
Usage	<p>When EVPN Multihoming is enabled in a network, the MAC addresses of downstream devices can point to a L2 next-hop group so that known unicast traffic is load-balanced between the switches in a L2 next-hop group using tunnels. The 12-nexthop-group setting in Switch-Resource mode is required to enable this functionality on EVPN multihomed TD4-based switches, such as Z9432-ON and S5448-ON. The L2 next-hop group setting is applied immediately and does not require a reboot to take effect. Enabling the L2 next-hop group setting reduces the capacity of the FDB and ARP tables by 50%.</p>
Examples	<pre>sonic(config)# switch-resource sonic(config-switch-resource)# 12-nexthop-group</pre>
Releases	4.2.0 or later

lacp individual

Enables LACP individual mode on port channel members.

Command	lacp individual [timeout seconds]
Options	<p><i>timeout seconds</i>—Enter the timeout period (in seconds) used to transition member interfaces in a dynamic port channel from Inactive to LACP individual mode if they do not receive an LACPDU for the configured timeout period.</p>
Modes	PORt-CHANNEL CONFIGURATION
Usage	<p>If a port channel member port becomes link UP and does not receive an LACPDU for the configured LACP individual timeout period, the port transitions to individual LACP mode. If a port channel member port, which is LACP active, receives no LACPDU for the LACP timeout plus the configured LACP individual timeout period, the port transitions to individual LACP individual mode. To remove the configured LACP individual timeout value and return to the default timeout, enter the <code>no lacp individual timeout</code> command.</p>
Examples	<pre>sonic(config)# interface PortChannel 6 sonic(config-if-po6)# lacp individual sonic(config-if-po6)# lacp individual timeout 60</pre>
Releases	4.4.0 or later

ldap-server

Configures the LDAP server.

Command	<pre>ldap-server {{timelimit timelimit_val} {bind-timelimit bind_timelimit_val} {idle-timelimit idle_timelimit_val} {retry retry_val} {port port_val} {scope scope_val} {version ldap_version_val} {base ldap_base_val} {ssl ssl_val} {binddn binddn_val} {bindpw bindpw_val} {pam-filter pam_filter_val} {pam-login-attribute pam_login_val} {pam-group-dn pam_group_val} {pam-member-attribute pam_member_val} {sudoers-base sudoers_val} {nss-base-passwd nss_base_passwd_val} {nss-base-group nss_base_group_val} {nss-base-shadow nss_base_shadow_val} {nss-base- netgroup nss_base_netgroup_val} {nss-base-sudoers nss_sudoers_val} {nss-initgroups-ignoreusers nss-initgroups_val} {nss-skipmembers {true false}} } [Vrf vrf-name]</pre>
Options	<ul style="list-style-type: none"> • <i>timelimit timelimit_val</i>—Time limit • <i>bind-timelimit bind_timelimit_val</i>—Bind time limit • <i>idle-timelimit idle_timelimit_val</i>—Idle time limit • <i>retry retry_val</i>—Retry

- `port port_val`—Port
- `scope scope_val`—Scope; select sub or base
- `version ldap_version_val`—LDAP version
- `base ldap_base_val`—LDAP base
- `ssl ssl_val`—SSL; select on, off, or start_tls
- `binddn binddn_val`—Distinguished name to bind
- `bindpw bindpw_val`—Credentials to bind; valid characters include ASCII printable except space
- `pam-filter pam_filter_val`—PAM filter name
- `pam-login-attribute pam_login_val`—PAM login attribute (default uid)
- `pam-group-dn pam_group_val`—PAM group distinguished name
- `pam-member-attribute pam_member_val`—PAM member attribute value
- `sudoers-base sudoers_val`—Sudo base distinguished name
- `nss-base-passwd nss_base_passwd_val`—NSS search base password
- `nss-base-group nss_base_group_val`—NSS search base group
- `nss-base-shadow nss_base_shadow_val`—NSS search base for shadow map
- `nss-base-netgroup nss_base_netgroup_val`—NSS search base for netgroup map
- `nss-base-sudoers nss_sudoers_val`—NSS search base for sudoers map
- `nss-initgroups-ignoreusers nss_initgroups_val`—NSS initialization groups ignore users value
- `nss-skipmembers {true | false}`—Specifies whether or not to populate the members list in the group structure for group lookups (Default: False).

Modes

CONFIGURATION

Usage

Use this command to configure the LDAP server and its parameters.

Examples

```
sonic(config) # ldap-server timelimit 13  
sonic(config) # ldap-server bind-timelimit 10  
sonic(config) # ldap-server idle-timelimit 12  
sonic(config) # ldap-server retry 8  
sonic(config) # ldap-server port 389  
sonic(config) # ldap-server scope sub  
sonic(config) # ldap-server version 2  
sonic(config) # ldap-server base basetest  
sonic(config) # ldap-server ssl on  
sonic(config) # ldap-server binddn dnname  
sonic(config) # ldap-server bindpw testpasswd  
sonic(config) # ldap-server pam-filter testfilter  
sonic(config) # ldap-server pam-login-attribute loginattrstring  
sonic(config) # ldap-server pam-group-dn grpdn  
sonic(config) # ldap-server pam-member-attribute attrstring  
sonic(config) # ldap-server sudoers-base dnqrystr  
sonic(config) # ldap-server nss-base-passwd dnsearchstr  
sonic(config) # ldap-server nss-base-group grpmap  
sonic(config) # ldap-server nss-base-shadow grpmap  
sonic(config) # ldap-server nss-base-netgroup netgrpstr  
sonic(config) # ldap-server nss-base-sudoers sudomap  
sonic(config) # ldap-server nss-initgroups-ignoreusers grpstr  
sonic(config) # no ldap-server nss-initgroups-ignoreusers grpstr
```

Releases

3.1 or later

ldap-server host

Configures the LDAP server hostname.

Command	ldap-server host <i>host_val</i> [<i>use-type use_type_val</i>] [<i>port server_port_val</i>] [<i>priority priority_val</i>] [<i>ssl ssl_val</i>] [<i>retry retry_val</i>]
Options	<ul style="list-style-type: none">• <i>host_val</i>—Host IP address in A.B.C.D or A::B format• <i>use_type_val</i>—(Optional) Use type; select all, nss, sudo, pam, nss_sudo, nss_pam, or sudo_pam• <i>server_port_val</i>—(Optional) Server port number• <i>priority_val</i>—(Optional) Port priority• <i>ssl_val</i>—(Optional) SSL; select on, off, or start_tls• <i>retry_val</i>—(Optional) Retries
Modes	CONFIGURATION
Usage	Use this command to configure the IP address or the hostname of the LDAP server. You can configure up to eight LDAP servers.
Examples	<pre>sonic(config)# ldap-server host 4.5.6.7 use-type nss port 300 priority 12 ssl on retry 5</pre> <pre>sonic(config)# no ldap-server host 4.5.6.7 use-type</pre>
Releases	3.1 or later

ldap-server map

Configures the LDAP server map.

Command	ldap-server map {{[attribute <i>attribute_from_val</i> {to <i>attribute_to_val</i> }]} {[objectclass <i>objectclass_from_val</i> {to <i>objectclass_to_val</i> }]} {[default-attribute-value <i>default_from_val</i> {to <i>default_to_val</i> }]} {[override-attribute-value <i>override_from_val</i> {to <i>override_to_val</i> }]}}
Options	<ul style="list-style-type: none">• <i>attribute_from_val</i>—(Optional) Attribute map key• <i>attribute_to_val</i>—(Optional) Attribute map value• <i>objectclass_from_val</i>—(Optional) Objectclass map key• <i>objectclass_to_val</i>—(Optional) Objectclass map value• <i>default_from_val</i>—(Optional) Default attribute map key• <i>default_to_val</i>—(Optional) Default attribute map value• <i>override_from_val</i>—(Optional) Override attribute value map key• <i>override_to_val</i>—(Optional) Override attribute value map value
Modes	CONFIGURATION
Usage	Use this command to map an LDAP attribute to a value.
Examples	<pre>sonic(config)# ldap-server map objectclass objkey to objectVal</pre> <pre>sonic(config)# no ldap-server map objectclass objkey to objectVal</pre>
Releases	3.1 or later

ldap-server nss

Configures NSS for the LDAP server.

Command	<code>ldap-server nss {{timelimit <i>timelimit_val</i>} {bind-timelimit <i>bind_timelimit_val</i>} {idle-timelimit <i>idle_timelimit_val</i>} {retry <i>retry_val</i>} {port <i>port_val</i>} {scope <i>scope_val</i>} {version <i>ldap_version_val</i>} {base <i>ldap_base_val</i>} {ssl <i>ssl_val</i>} {binddn <i>binddn_val</i>} {bindpw <i>bindpw_val</i>} {nss-base-passwd <i>nss_base_passwd_val</i>} {nss-base-group <i>nss_base_group_val</i>} {nss-base-shadow <i>nss_base_shadow_val</i>} {nss-base-netgroup <i>nss_base_netgroup_val</i>} {nss-base-sudoers <i>nss_sudoers_val</i>} {nss-initgroups-ignoreusers <i>nss-initgroups_val</i>}}</code>
Options	<ul style="list-style-type: none">• <i>timelimit_val</i> — Time limit value• <i>bind_timelimit_val</i> — Bind time limit value• <i>idle_timelimit_val</i> — Idle time limit value• <i>retry_val</i> — Retry value• <i>port_val</i> — Port value• <i>scope_val</i> — Scope; select sub, one, or base• <i>ldap_version_val</i> — LDAP version• <i>ldap_base_val</i> — Base distinguished name• <i>ssl_val</i> — SSL; select on, off, or start_tls• <i>binddn_val</i> — Distinguished name to bind• <i>bindpw_val</i> — Credentials to bind; valid characters include ASCII printable except space• <i>nss_base_passwd_val</i> — NSS search base for password map• <i>nss_base_group_val</i> — NSS search base group• <i>nss_base_shadow_val</i> — NSS search base for shadow map• <i>nss_base_netgroup_val</i> — NSS search base for netgroup map• <i>nss_sudoers_val</i> — NSS search base for sudoers map• <i>nss-initgroups_val</i> — NSS initialization groups ignore users value
Modes	CONFIGURATION
Usage	None

Examples

```
sonic(config) # ldap-server nss timelimit 13  
  
sonic(config) # ldap-server nss bind-timelimit 10  
  
sonic(config) # ldap-server nss idle-timelimit 12  
  
sonic(config) # ldap-server nss retry 8  
  
sonic(config) # ldap-server nss port 81  
  
sonic(config) # ldap-server nss scope sub  
  
sonic(config) # ldap-server nss version 2  
  
sonic(config) # ldap-server nss base basetest  
  
sonic(config) # ldap-server nss ssl on  
  
sonic(config) # ldap-server nss binddn dnname  
  
sonic(config) # ldap-server nss bindpw testpasswd  
  
sonic(config) # ldap-server nss nss-base-passwd dnsearchstr  
  
sonic(config) # ldap-server nss nss-base-group grpmap  
  
sonic(config) # ldap-server nss nss-base-shadow grpmap  
  
sonic(config) # ldap-server nss nss-base-netgroup netgrpstr  
  
sonic(config) # ldap-server nss nss-base-sudoers sudomap  
  
sonic(config) # ldap-server nss nss-initgroups-ignoreusers grpstr  
  
sonic(config) # no ldap-server nss nss-initgroups-ignoreusers grpstr
```

Releases

3.1 or later

ldap-server pam

Configures PAM for the LDAP server.

Command

```
ldap-server pam {{timelimit timelimit_val} | {bind-timelimit  
bind_timelimit_val} | {retry retry_val} | {port port_val} | {scope  
scope_val} | {version ldap_version_val} | {base ldap_base_val} | {ssl  
ssl_val} | {binddn binddn_val} | {bindpw bindpw_val} | {pam-filter  
pam_filter_val} | {pam-login-attribute pam_login_val} | {pam-group-dn  
pam_group_val} | {pam-member-attribute pam_member_val} | {nss-base-passwd  
nss_base_passwd_val}}
```

Options

- *timelimit_val* — Time limit value
- *bind_timelimit_val* — Bind time limit value

- *retry_val* — Retry value
- *port_val* — Port value
- *scope_val* — Scope; select sub, one, or base
- *ldap_version_val* — LDAP version
- *ldap_base_val* — Base distinguished name
- *ssl_val* — SSL; select on, off, or start_tls
- *binddn_val* — Distinguished name to bind
- *bindpw_val* — Credentials to bind; valid characters include ASCII printable except space
- *pam_filter_val* — PAM filter name
- *pam_login_val* — PAM login attribute (default uid)
- *pam_group_val* — PAM group distinguished name
- *pam_member_val* — PAM member attribute value
- *nss_base_passwd_val* — NSS search base for password map

Modes

CONFIGURATION

Usage

None

Examples

```
sonic(config)# ldap-server pam timelimit 13

sonic(config)# ldap-server pam bind-timelimit 10

sonic(config)# ldap-server pam retry 8

sonic(config)# ldap-server pam port 81

sonic(config)# ldap-server pam scope sub

sonic(config)# ldap-server pam version 2

sonic(config)# ldap-server pam base basetest

sonic(config)# ldap-server pam ssl on

sonic(config)# ldap-server pam binddn dnname

sonic(config)# ldap-server pam bindpw testpasswd

sonic(config)# ldap-server pam pam-filter testfilter

sonic(config)# ldap-server pam pam-login-attribute loginattrstring

sonic(config)# ldap-server pam pam-group-dn grpdn

sonic(config)# ldap-server pam pam-member-attribute attrstring

sonic(config)# ldap-server pam nss-base-passwd dnsearchstr

sonic(config)# no ldap-server pam nss-base-passwd dnsearchstr
```

Releases

3.1 or later

ldap-server security-profile

Enables a security profile for LDAP service.

Command	<code>ldap-server security-profile <i>profile-name</i></code>
Options	<ul style="list-style-type: none">• <i>profile-name</i> — Enter the name of an LDAP security profile.
Modes	CONFIGURATION
Usage	Before configuring an LDAP security profile, create a trust store for the installed CA certificates and associate the trust store with the security profile. To create a security profile for LDAP, use the crypto security-profile command. To associate a CA certificate with a trust store, use the crypto trust-store ca-cert command.

Example	<pre>sonic(config)# crypto trust-store ldapts ca-cert ca sonic(config)# crypto security-profile ldapsecprofile peer-name-check true revocation-check true sonic(config)# crypto security-profile trust-store ldapsecprofile ldapts sonic(config)# ldap-server security-profile ldapsecprofile</pre>
----------------	---

Releases	4.4.1 or later
-----------------	----------------

ldap-server source-interface

Configures the source interface for LDAP packets.

Command	<code>ldap-server source-interface {Ethernet Loopback Management PortChannel Vlan}</code>
Options	<ul style="list-style-type: none">• Ethernet—Selects Ethernet as the source interface• Loopback—Selects Loopback as the source interface• Management—Selects Management as the source interface• PortChannel—Selects PortChannel as the source interface• Vlan—Selects VLAN as the source interface
Modes	CONFIGURATION
Usage	Use this command to set the source IP of the LDAP packets from the specified interface.
Examples	<pre>sonic(config)# ldap-server source-interface Loopback 3</pre> <pre>sonic(config)# no ldap-server source-interface</pre>

Releases	3.1 or later
-----------------	--------------

ldap-server sudo

Configures the sudo feature for the LDAP server.

Command	<code>ldap-server sudo {{timelimit <i>timelimit_val</i>} {bind-timelimit <i>bind_timelimit_val</i>} {retry <i>retry_val</i>} {port <i>port_val</i>} {version <i>ldap_version_val</i>} {base <i>ldap_base_val</i>} {ssl <i>ssl_val</i>} {binddn <i>binddn_val</i>} {bindpw <i>bindpw_val</i>} {sudoers-base <i>sudoers_val</i>}}</code>
Options	<ul style="list-style-type: none">• <i>timelimit_val</i> — Time limit value• <i>bind_timelimit_val</i> — Bind time value• <i>retry_val</i> — Retry value• <i>port_val</i> — Port value

- *ldap_version_val* — LDAP version
- *ldap_base_val* — Base distinguished name
- *ssl_val* — SSL; select on, off, or start_tls
- *binddn_val* — Distinguished name to bind
- *bindpw_val* — Credentials to bind; valid characters include ASCII printable except space
- *sudoers_val* — Sudo base distinguished name

Modes

CONFIGURATION

Usage

None

Examples

```
sonic(config)# ldap-server sudo timelimit 13

sonic(config)# ldap-server sudo bind-timelimit 10

sonic(config)# ldap-server sudo retry 8

sonic(config)# ldap-server sudo port 81

sonic(config)# ldap-server sudo scope sub

sonic(config)# ldap-server sudo version 2

sonic(config)# ldap-server sudo base basetest

sonic(config)# ldap-server sudo ssl on

sonic(config)# ldap-server sudo binddn dnname

sonic(config)# ldap-server sudo bindpw testpasswd

sonic(config)# ldap-server sudo sudoers-base dnqrystr

sonic(config)# no ldap-server sudo sudoers-base dnqrystr
```

Releases

3.1 or later

ldap-server vrf

Configures the VRF used for the LDAP server.

Commandldap-server vrf *vrf-name***Options***vrf-name*—Name for the VRF prefixed by Vrf (up to 15 characters)**Modes**

CONFIGURATION

Usage

Use this command to set the VRF used to reach the LDAP server.

Examples

```
sonic(config)# ldap-server vrf Vrf1

sonic(config)# no ldap-server vrf
```

Releases

3.1 or later

line vty

Enter line VTY mode for setting access filters or out of band service policy.

Command	line vty
Options	None
Modes	CONFIGURATION
Usage	Use the line vty command to apply access filters for an out-of-band service-policy. In Enterprise SONiC, a VTY ACL is used as a control-plane ACL. A VTY ACL applies deny, drop, and permit actions on packets sent from a front-end port or the Management port to the CPU, including SNMP, NTP, SSH, TACACS+, and RADIUS traffic. CAUTION: To avoid losing connectivity to the switch, you must explicitly permit the IP address of external devices to reach the switch in a control-plane ACL.

Example

```
sonic(config)# ip access-list CONTROL_PLANE_ACL
sonic(config-ipv4-acl)# seq 5 permit udp host 172.16.1.1 any eq 161
remark SNMP
sonic(config-ipv4-acl)# seq 10 permit tcp host 172.16.55.1 any eq 22
remark SSH
sonic(config-ipv4-acl)# seq 15 permit udp host 172.16.56.1 eq 123 any
remark NTP
sonic(config-ipv4-acl)# seq 20 permit ip host 192.168.1.1 host
192.168.1.2 remark mclag-peerip
sonic(config-ipv4-acl)# seq 1000 deny ip any any
sonic(config-ipv4-acl)# exit

sonic(config)# line vty
sonic(config-line-vty)# ip access-group CONTROL_PLANE_ACL in
```

Releases

3.1 or later

link state track

Creates a link state tracking group.

Command	link state track <i>group-name</i> [upstream downstream]
Options	<ul style="list-style-type: none">• <i>group-name</i> — Group name (up to 63 characters)• upstream — (Optional) Tracks upstream interfaces• downstream — (Optional) Tracks downstream interfaces
Modes	<ul style="list-style-type: none">• CONFIGURATION• INTERFACE
Usage	Use this command to create a link state tracking group for Ethernet, PortChannel, or VLAN interfaces. The name must begin with A-Z, a-z or 0-9. Underscore and hyphens can be used except as the first character. upstream and downstream options are only available in INTERFACE mode. NOTE: In an EVPN Ethernet segment, the multihomed downlink interfaces on a VTEP are shut down if all uplink interfaces on the VTEP go down. You can specify an optional <i>timeout</i> value (in seconds) to wait before bringing up multihomed interfaces after one or more uplink interfaces come up. Create a link-state track group and associate all downstream EVPN multihoming interfaces to the track group by entering the downstream all-evpn-es command. Enter the link state track upstream command to track the uplink states to an upstream network.

Examples

```
sonic(config-if-Ethernet28)# link state track FooBar upstream  
  
sonic(config-if-Ethernet28)# link state track FooBar downstream  
  
sonic(config-if-Ethernet28)# no link state track FooBar downstream  
  
sonic(config)# link state track trackGrp  
sonic(config-link-track)# downstream all-evpn-es  
sonic(config-link-track)# timeout 300  
sonic(config-link-track)# exit  
sonic(config)# interface Ethernet0  
sonic(config-if-Ethernet0)# link state track trackGrp upstream
```

Releases

3.0 or later

link-error-disable

Configures link error disable.

Command

```
link-error-disable [ flap-threshold { flaps { sampling-interval { window  
{ recovery-interval interval } } } } ]
```

Options

- *flaps* — Flap-threshold number (1 to 50; default is 3)
- *window* — Sampling-interval number (1 to 65535; default is 30)
- *interval* — Recovery-interval number (0 to 65534; default is 300)

Modes

- INTERFACE
- INTERFACE RANGE

Usage

- Flap-threshold interval (flaps) — The number of times that the port's link state goes from up to down and down to up before the recovery-interval is activated.
- Sampling-interval (window) — Sampling interval is the amount of time during which the specified flap-threshold can be crossed. If the flap-threshold is crossed during this sampling-interval, port is error-disabled.
- Recovery-interval (interval) — Recovery interval is the amount of time the port remains disabled (down) before it becomes enabled. Entering 0 indicates that the ports stay down until an administrative override occurs.

Examples

```
sonic(config)#interface ethernet 0  
sonic(config-if-Ethernet0)# link-error-disable flap-threshold 10  
sampling-interval 3 recovery-interval 10
```

Releases

4.0 or later

listen limit

Configures the maximum number of BGP dynamic neighbors to create.

Command

```
listen limit lmt-val
```

Options

lmt-val—Limit value (1 to 5000; default is 100)

Modes

ROUTER-BGP

Usage

Use this command to set the maximum number of peers accepted for a BGP instance.

Example

```
sonic(config-router-bgp)# listen limit 123
```

Releases

3.1 or later

listen range

Creates a listen range for BGP for dynamic BGP neighbors.

Command	<code>listen range addr {peer-group pgname}</code>
Options	<ul style="list-style-type: none">• <code>addr</code> — BGP neighbor IPv4 or IPv6 address in A.B.C.D/mask or A::B/mask format• <code>pgname</code> — Peer-group name
Modes	ROUTER-BGP
Usage	Use this command to accept a peering connection from neighbors to create dynamic neighbors.
Example	<pre>sonic(config-router-bgp)# listen range 192.168.0.0/16 peer-group PG_Ext</pre>
Releases	3.1 or later

lldp

Configure the LLDP frame receive and transmit mode at the interface level.

Command	<code>lldp mode</code>
Options	<code>mode</code> —Mode type; select receive or transmit.
Modes	INTERFACE
Usage	Use this command to enable or disable LLDP receive and transmit modes.
Examples	<pre>sonic(config)# interface Ethernet 28 sonic(config-if-Ethernet28)# lldp receive</pre> <pre>sonic(config-if-Ethernet28)# lldp transmit</pre> <pre>sonic(config-if-Ethernet28)# no lldp</pre>
Releases	3.1 or later

lldp enable

Enables or disables LLDP globally.

Command	<code>lldp enable</code>
Options	None
Modes	<ul style="list-style-type: none">• CONFIGURATION• INTERFACE
Usage	Use this command to enable LLDP globally or on an interface level. Use <code>no</code> form of this command to disable LLDP. By default, LLDP is enabled.
Examples	<pre>sonic(config)# interface Ethernet 12 sonic(config-if-Ethernet12)# lldp enable</pre> <pre>sonic(config-if-Ethernet12)# no lldp enable</pre>
Releases	3.1 or later

lldp med-tlv-select

Enables or disables LLDP-MED TLV advertisement.

Command	<code>lldp med-tlv-select <i>tlv</i></code>
Options	<i>tlv</i> — MED TLV type. Enter <code>network-policy</code> or <code>power-management</code> for the MED TLV type.
Modes	INTERFACE
Usage	Use the <code>lldp med-tlv-select</code> command to select the LLDP-MED TLVs to advertise.
Examples	<pre>sonic-cli(config)# interface Ethernet 0 sonic-cli(config-if-Ethernet0)# lldp med-tlv-select network-policy</pre> <pre>sonic-cli(config)# interface Ethernet 0 sonic-cli(config-if-Ethernet0)# lldp med-tlv-select power-management</pre> <pre>sonic-cli(config)# interface Ethernet 0 sonic-cli(config-if-Ethernet0)# no lldp med-tlv-select network-policy</pre>
Releases	4.0 or later

lldp multiplier

Configures the LLDP multiplier value used to determine the timeout value.

Command	<code>lldp multiplier <i>multiplier</i></code>
Options	<i>multiplier</i> — Multiplier value (hello-time x multiplier value)
Modes	CONFIGURATION
Usage	This command is used to determine the timeout value after which the LLDP neighbor entry is deleted (default 4).
Examples	<pre>sonic(config)# lldp multiplier 6</pre> <pre>sonic(config)# no lldp multiplier</pre>
Releases	3.1 or later

lldp system-description

Configures the LLDP system description.

Command	<code>lldp system-description <i>system_description</i></code>
Options	<i>system_description</i> —LLDP system description entered with quotes on both sides
Modes	CONFIGURATION
Usage	Use this command to configure the LLDP system description that is carried in the LLDP PDU.
Examples	<pre>sonic(config)# lldp system-description "SONiC"</pre> <pre>sonic(config)# no lldp system-description</pre>
Releases	3.1 or later

lldp system-name

Configures the LLDP system name.

Command

```
lldp system-name system_name
```

Options

system_name—Enter the LLDP system name description

Modes

CONFIGURATION

Usage

Use this command to configure the LLDP system name that is carried in the LLDP PDU.

Examples

```
sonic(config)# lldp system-name "SONiC"
```

```
sonic(config)# no lldp system-name
```

Releases

3.1 or later

lldp timer

Configures the LLDP hello time.

Command

```
lldp timer hello-time
```

Options

hello-time — LLDP timer rate in seconds (5 to 524; default 30)

Modes

CONFIGURATION

Usage

Use this command to set the interval at which periodic hellos are exchanged.

Examples

```
sonic(config)# lldp timer 10
```

```
sonic(config)# no lldp timer
```

Releases

3.1 or later

lldp tlv-select

Enables sending of TLVs in LLDP frames.

Command

```
lldp tlv-select tlv
```

Options

tlv — TLV type; select from the options:

- **link-aggregation**—Send the 802.1 link aggregation TLV in the LLDPPDU. Configure from INTERFACE mode. Enabled by default.
- **management-address**—Send the management IP address in the TLV. Configure from CONFIGURATION mode.
- **max-frame-size**—Send the 802.3 Maximum frame size TLV in the LLDPPDU. Configure from INTERFACE mode. Enabled by default.
- **system-capabilities**—Send system capabilities in the TLV. Configure from CONFIGURATION mode.
- **power-management**—Send power management information in the TLV. Configure from INTERFACE mode.
- **port-vlan-id**—Send the VLAN ID of the port in the TLV. Configure from INTERFACE mode.
- **vlan-name**—Send the 802.1 VLAN name TLV in the LLDPPDU. Configure from INTERFACE mode. Enabled by default.

Modes

- CONFIGURATION
- INTERFACE

Usage

Use the `lldp tlv-select` command to configure the LLDP TLVs to be advertised.

- In INTERFACE mode, the supported TLV types are power-management, vlan-name, max-frame-size, link-aggregation, and port-vlan-id.
- In CONFIGURATION mode, the supported TLV types are management-address and system-capabilities

Examples

```
sonic(config)# lldp tlv-select management-address

sonic(config)# lldp tlv-select system-capabilities

sonic(config)# interface Ethernet 1
sonic(config-if-Ethernet1)# lldp tlv-select power-management

sonic(config)# no lldp tlv-select
```

This example enables the advertisement of VLAN ID of the port in the TLV:

```
sonic(config)# interface Eth 4
sonic(config-if-Eth4)# switchport access Vlan 10
sonic(config-if-Eth4)# lldp tlv-select port-vlan-id

sonic(config)# interface Eth 4
sonic(config-if-Eth4)# lldp tlv-select vlan-name

sonic(config)# interface Eth 4
sonic(config-if-Eth4)# lldp tlv-select link-aggregation

sonic(config)# interface Eth 4
sonic(config-if-Eth4)# lldp tlv-select max-frame-size
```

The `show lldp neighbor` command output displays the VLAN names, link aggregation status, and the maximum frame size that are received on the peer device using LLDPDUs:

```
sonic# show lldp neighbor
Interface: Eth1/13,via: LLDP
  Chassis:
    ChassisID:      3c:2c:30:6d:72:80
    SysName:        Peer-B
    SysDescr:       SONiC Software Version:
SONiC.rel_dell_sonic_4.x_share.1164-cfbef127c - HwSku: DellEMC-S5232f-C32 - Distribution: Debian 10.13 - Kernel: 5.10.0-21-amd64
    TTL:            120
    MgmtIP:         fe80::3e2c:30ff:fe6d:7280
    Capability:    ROUTER, ON
  Port
    PortID:        Eth1/13
    PortDescr:     MC_LAG_to_MC_LAG_PEER
    PortVlanID:    10
    AggregStatus:  Aggregated, Aggregated Port ID 20
    MaxFrameSize:  9216
    VLAN Names:
      VLAN      NAME
      ----- 
      10        Vlan10
      20        Vlan20
      30        Vlan30
      40        Vlan40
      50        Vlan50
      60        Vlan60
      70        Vlan70
      80        Vlan80
      100       Vlan100
      2000      Vlan2000
LLDP-MED
```

```
Device Type: Network Connectivity Device
Capability: Capabilities, yes
```

When the link aggregation TLV is enabled and the port is not a member of a port channel, the show lldp neighbor command displays AggregStatus: Not aggregated:

```
sonic# show lldp neighbor
Interface: Eth1/13,via: LLDP
Chassis:
    ChassisID: 3c:2c:30:6d:72:80
    SysName: Peer-B
    SysDescr: SONiC Software Version:
SONiC_rel_dell_sonic_4.x_share.1164-cfbef127c - HwSku: DellEMC-S5232f-
C32 - Distribution: Debian 10.13 - Kernel: 5.10.0-21-amd64
    TTL: 120
    MgmtIP: fe80::3e2c:30ff:fe6d:7280
    Capability: ROUTER, ON
Port
    PortID: Eth1/13
    PortDescr: MC_LAG_to_MC_LAG_PEER
    PortVlanID: 10
    AggregStatus: Not aggregated
    MaxFrameSize: 9216
    VLAN Names:
        VLAN      NAME
        -----
        10        Vlan10
        20        Vlan20
        30        Vlan30
        40        Vlan40
        50        Vlan50
        60        Vlan60
        70        Vlan70
        80        Vlan80
        100       Vlan100
        2000      Vlan2000
LLDP-MED
    Device Type: Network Connectivity Device
    Capability: Capabilities, yes
```

Releases

3.1 or later

lldp tlv-set

Configures an IPv4 or IPv6 management address that advertises LLDP on an interface.

Command

```
lldp tlv-set management-address {ipv4 address} | {ipv6 address}
```

Options

- *ipv4-address*—IPv4 address in A.B.C.D format
- *ipv6-address*—IPv6 address in A::B/mask format

Modes

INTERFACE

Usage

Use this command to set the IPv4 and IPv6 management address in LLDP management address TLV. IPv4 and IPv6 addresses assigned on the management interface are used by default. Use this command to change that to a different address.

Examples

```
sonic-clis(config)# interface Ethernet 0
sonic-clis(config-if-Ethernet0)# lldp tlv-set management-address ipv4
10.1.1.1
```

```
sonic-clis(config)# interface Ethernet 0
sonic-clis(config-if-Ethernet0)# no lldp tlv-set management-address ipv4
10.1.1.1
```

Releases

4.0 or later

lldp vlan-name-tlv allowed vlan

Configures the list of VLANs whose names are to be carried in the LLDPPDU.

Command	lldp vlan-name-tlv allowed vlan <i>vlan-names</i>
Options	<i>vlan-names</i> —Enter the name of a single VLAN or a range of VLANs (1 to 4094)
Mode	INTERFACE
Usage	<p>By default, the name of all VLANs that are configured on a port using the <code>switchport trunk allowed vlan</code> and <code>switchport access vlan</code> commands are carried in the LLDPPDU. The <code>lldp vlan-name-tlv allowed vlan</code> command overrides the default list of VLAN names. The <code>lldp vlan-name-tlv allowed vlan</code> command also adds a VLAN to the list of VLAN names to be sent even if the VLAN is not added to the port. However, the name of the VLAN is sent only after adding the VLAN to the port.</p> <ul style="list-style-type: none">• Use a comma to separate a range of VLANs.• The command overwrites any existing list of VLAN names.• Use the <code>no lldp vlan-name-tlv allowed vlan</code> command to remove one or more VLANs from the list.

Examples	This example adds VLANs 10, 11, and 12 in the LLDPPDU:
	<pre>sonic(config)# interface Eth 1/1 sonic(config-if-Eth1/1)# lldp vlan-name-tlv allowed vlan 10,11,12</pre>

The following example adds VLAN 20, VLANs 70 to 100, and VLAN 142:

```
sonic(config)# interface Eth 1/1
sonic(config-if-Eth1/1)# lldp vlan-name-tlv allowed vlan 20,70-100,142
```

This example shows how only the last configuration takes effect:

```
sonic(conf-if-eth1/1/1)# lldp vlan-name-tlv allowed vlan 10,11,12
sonic(conf-if-eth1/1/1)# lldp vlan-name-tlv allowed vlan 10, 13, 15
```

The following example shows that the `no` form of this command removes a part from the list:

```
sonic(conf-if-eth1/1/1:1)# lldp vlan-name-tlv allowed vlan 10,13,15
sonic(conf-if-eth1/1/1:1)# no lldp vlan-name-tlv allowed vlan 10
```

Releases	4.4.0 or later
-----------------	----------------

lldp vlan-name-tlv max-tlv-count

Configures the maximum number of VLAN-name TLVs that are transmitted in the LLDPPDU. This command number restricts the number of VLAN names in the TLV.

Command	lldp vlan-name-tlv max-tlv-count <i>tlv-count</i>
Options	<i>tlv-count</i> —Enter the maximum number of VLAN-name TLVs. The range is from 1 to 128. The default is 10.
Mode	INTERFACE
Usage	Use the <code>no lldp vlan-name-tlv max-tlv-count</code> to set the default value of 10.
Examples	<pre>sonic(config)# interface Eth 1/1 sonic(config-if-Eth1/1)# lldp vlan-name-tlv max-tlv-count 50</pre>
Releases	4.4.0 or later

load-current-max-val

Configures the maximum current load threshold value for the quantization process.

Command	<code>load-current-max-val <i>load-current-maximum-value</i></code>
Options	<code><i>load-current-maximum-value</i></code> —The maximum current load threshold value in bytes. The range is from 0 to 133169151. On the Z9864F-ON platform, the range is from 0 to 66584575. The default value is 6291456.
Modes	ARS-PROFILE
Usage	<ul style="list-style-type: none">• Ensure that the corresponding minimum value is lesser than or equal to the maximum value.• If the maximum physical buffer usage is 16 MB for 100G ports, and you want to divide 16 MB into eight bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 10. For example, if you want to enter 6291456 as the value on a 100G port, divide 6291456 by 10 and enter that number. The system converts the value to 6291456 internally.• If the maximum physical buffer usage is 16 MB for 400G ports, and you want to divide 16 MB into eight bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 40. For example, if you want to enter 6291456 as the value on a 400G port, divide 6291456 by 40 and enter that number. The system converts the value to 6291456 internally.• If the maximum physical buffer usage is 16 MB for 800G ports, and you want to divide 16 MB into eight bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 80. For example, if you want to enter 6291456 as the value on an 800G port, divide 6291456 by 80 and enter that number. The system converts the value to 6291456 internally.• If all 800G, 400G, and 100G ports have the same maximum physical buffer usage which is set to 16 MB, set the value according to the port with the highest speed which is 16M / 80 (scaling factor for 800G).
Examples	<pre>sonic(config-ars-profile)# load-current-max-val 600000</pre>
Releases	4.4.0 or later

load-current-min-val

Configures the minimum current load threshold value for the quantization process.

Command	<code>load-current-min-val <i>load-current-minimum-value</i></code>
Options	<code><i>load-current-minimum-value</i></code> —Enter the minimum current load threshold value in bytes (0 to 133169151; default is 1048576)
Modes	ARS-PROFILE
Usage	<ul style="list-style-type: none">• Ensure that the corresponding maximum value is greater than or equal to the minimum value.• If the maximum physical buffer usage is 16 MB for 100G ports, and you want to divide 16 MB into eight bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 10. For example, if you want to enter 1048576 as the value on a 100G port, divide 1048576 by 10 and enter that number. The system converts the value to 1048576 internally.• If the maximum physical buffer usage is 16 MB for 400G ports, and you want to divide 16 MB into eight bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 40. For example, if you want to enter 1048576 as the value on a 400G port, divide 1048576 by 40 and enter that number. The system converts the value to 1048576 internally.• If the maximum physical buffer usage is 16 MB for 800G ports, and you want to divide 16 MB into eight bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 80. For example, if you want to enter 1048576 as the value on an 800G port, divide 1048576 by 80 and enter that number. The system converts the value to 1048576 internally.

- 800G port, divide 1048576 by 80 and enter that number. The system converts the value to 1048576 internally.
- If all 800G, 400G, and 100G ports have the same maximum physical buffer usage which is set to 16 MB, set the value according to the port with the highest speed which is 16M / 80 (scaling factor for 800G).

Examples

```
sonic(config) # ars profile default
sonic(config-ars-profile) # load-current-min-val 100000
```

Releases

4.4.0 or later

load-future-max-val

Configures the maximum future load threshold value for the quantization process.

Command

`load-future-max-val load-future-maximum-value`

Options

load-future-maximum-value—The maximum future load threshold value in bytes. The range is from 0 to 266338303. On the Z9864F-ON platform, the range is from 0 to 133169151. The default value is 12582912.

Modes

ARS-PROFILE

Usage

- Make sure the corresponding minimum value is lesser than or equal to the maximum value.
- If the maximum physical buffer usage is 16MB for 100G ports, and you want to divide 16MB into 8 bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 10. For example, if you want to enter 12582912 as the value on a 100G port, divide 12582912 by 10 and enter that number. The system converts the value to 12582912 internally.
- If the maximum physical buffer usage is 16MB for 400G ports, and you want to divide 16MB into 8 bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 40. For example, if you want to enter 12582912 as the value on a 400G port, divide 12582912 by 40 and enter that number. The system converts the value to 12582912 internally.
- If the maximum physical buffer usage is 16MB for 800G ports, and you want to divide 16MB into 8 bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 80. For example, if you want to enter 12582912 as the value on an 800G port, divide 12582912 by 80 and enter that number. The system converts the value to 12582912 internally.
- If all 800G, 400G, and 100G ports have the same maximum physical buffer usage which is set to 16MB, set the value according to the port with the highest speed which is 16M / 80 (scaling factor for 800G).

Examples

```
sonic(config-ars-profile) # load-future-max-val 1200000
```

Releases

4.4.0 or later

load-future-min-val

Configures the minimum future load threshold value for the quantization process.

Command

`load-future-min-val load-future-minimum-value`

Options

load-future-minimum-value—The minimum future load threshold value in bytes. The range is from 0 to 266338303. The default value is 2097152.

Modes

ARS-PROFILE

Usage

- Ensure that the corresponding maximum value is greater than or equal to the minimum value.
- If the maximum physical buffer usage is 16MB for 100G ports, and you want to divide 16MB into 8 bands, the minimum and maximum thresholds of current load and future load that you want to

configure should be divided by 10. For example, if you want to enter 2097152 as the value on a 100G port, divide 2097152 by 10 and enter that number. The system converts the value to 2097152 internally.

- If the maximum physical buffer usage is 16MB for 400G ports, and you want to divide 16MB into 8 bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 40. For example, if you want to enter 2097152 as the value on a 400G port, divide 2097152 by 40 and enter that number. The system converts the value to 2097152 internally.
- If the maximum physical buffer usage is 16MB for 800G ports, and you want to divide 16MB into 8 bands, the minimum and maximum thresholds of current load and future load that you want to configure should be divided by 80. For example, if you want to enter 2097152 as the value on an 800G port, divide 2097152 by 80 and enter that number. The system converts the value to 2097152 internally.
- If all 800G, 400G, and 100G ports have the same maximum physical buffer usage which is set to 16MB, set the value according to the port with the highest speed which is 16M / 80 (scaling factor for 800G).

Examples

```
sonic(config) # ars profile default  
sonic(config-ars-profile) # load-future-min-val 200000
```

Releases

4.4.0 or later

load-future-weight

Configures a weight value in percentage to the future port load quality measure in the switch pipeline.

Command `load-future-weight load-future-weight`

Options *load-future-weight*—The future port load quality measure in percentage. The range is from 0 to 100. The default value is 10.

Modes ARS-PROFILE

Usage The aggregate of past and future load weights should be less than or equal to 100.

Examples

```
sonic(config) # ars profile default  
sonic(config-ars-profile) # load-future-weight 35
```

Releases

4.4.0 or later

load-past-max-val

Configures the maximum past load threshold value for the quantization process.

Command `load-past-max-val load-past-maximum-value`

Options *load-past-maximum-value*—The maximum past load threshold value in Mbps. The range is from 0 to 10000. The default value is 6000.

Modes ARS-PROFILE

Usage Ensure that the corresponding minimum value is lesser than or equal to the maximum value.

Examples

```
sonic(config) # ars profile default  
sonic(config-ars-profile) # load-past-max-val 7000
```

Releases

4.4.0 or later

load-past-min-val

Configures the minimum past load threshold value for the quantization process.

Command	<code>load-past-min-val <i>load-past-minimum-value</i></code>
Options	<code><i>load-past-minimum-value</i></code> —The minimum past load threshold value in Mbps. The range is from 0 to 10000. The default value is 3000.
Modes	ARS-PROFILE
Usage	Ensure that the corresponding maximum value is greater than or equal to the minimum value.
Examples	<pre>sonic(config)# ars profile default sonic(config-ars-profile)# load-past-min-val 4000</pre>
Releases	4.4.0 or later

load-past-weight

Configures a weight value in percentage to the past port load quality measure in the switch pipeline.

Command	<code>load-past-weight <i>load-past-weight</i></code>
Options	<code><i>load-past-weight</i></code> —The past port load quality value in percentage. The range is from 0 to 100. The default value is 80.
Modes	ARS-PORT-PROFILE
Usage	The aggregate of past and future load weights should be less than or equal to 100.
Examples	<pre>sonic(config)# ars port-profile default sonic(config-ars-port-profile)# load-past-weight 65</pre>
Releases	4.4.0 or later

load-scaling-factor

Configures the port load-scaling factor.

Command	<code>load-scaling-factor <i>port-load-scaling-factor</i></code>
Options	<code><i>port-load-scaling-factor</i></code> —Enter the port load-scaling factor. The values are 0, 1, 2.5, 4, 5, 10, 20, 40, and 80. The default value is 0.
Modes	ARS-PORT-PROFILE
Usage	If you configure 0, the port load-scaling factor is automatically derived based on the speed of the port. When the port-profile is already bound to any of the ports, modifying the <code>load-scaling-factor</code> command has the following restrictions:
	<ul style="list-style-type: none">• Configuring value 0 is allowed.• If the modified value of the load-scaling-factor is different that of the speed of ports under bind (current port-profile), the configuration is not allowed and the system shows an error message.• If you try to change the port speed and the configured load scale factor is a nonzero value, the configuration is not allowed and the system shows an error message.

Table 2. Port speed and scaling factor

Port Speed in Gbps	Scaling factor
10	1
25	2.5

Table 2. Port speed and scaling factor (continued)

Port Speed in Gbps	Scaling factor
40	4
50	5
100	10
200	20
400	40
800	80
Any	0 (auto derived)

Example

```
sonic(config) # ars port-profile default
sonic(config-ars-port-profile) # load-scaling-factor 5
```

Releases

4.4.0 or later

local-as

Configures a local AS number for a BGP neighbor or neighbors in a peer-group.

Command

```
local-as asnum {[no-prepend] [replace-as]}
```

Options

- *asnum* — Local AS number (1 to 4294967295)
- *no-prepend* — (Optional) Local AS values are not prepended to the AS_PATH attribute
- *replace-as* — (Optional) Globally-configured AS values are not prepended to the AS_PATH attribute

Modes

- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage

Use this command to configure a local AS number for a BGP neighbor or neighbors in a peer-group, and control how the local AS number is prepended to the AS_PATH of incoming and outgoing routes. Without modifiers, the specified local-as is prepended to the received AS_PATH when receiving routing updates from the peer, and prepended to the outgoing AS_PATH (after the process local AS) when transmitting local routes to the peer. If the *no-prepend* option is specified, the supplied local-as is not prepended to the received AS_PATH. If the *replace-as* option is specified, only the supplied local-as is prepended to the AS_PATH when transmitting local-route updates to this peer.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 30.30.30.3
sonic(config-router-bgp-neighbor) # local-as 65200 no-prepend
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # local-as 65200 non-prepend
```

```
sonic(config-router-bgp-neighbor) # no local-as 65200 no-prepend
sonic(config-router-bgp-pg) # no local-as 65200 non-prepend
```

Releases

3.0 or later

locator-led chassis

Enables or disables the locator chassis LED.

Command	locator-led chassis {on [timer value] off}
Options	value—(Optional) Time value in minutes (1 through 120)
Modes	EXEC
Usage	Use this command to turn on or turn off the locator chassis LED. If the command is run successfully on supported platforms, the system displays the message as Success else displays the message as Failed. If this command is run on unsupported platforms, the system displays the message Not supported.
Examples	Examples on supported platforms : sonic# locator-led chassis on Success sonic# locator-led chassis on timer 5 Success Locator LED will be off after 5 minutes
	Examples on unsupported platforms: sonic# locator-led chassis on Not supported sonic# locator-led chassis off
Releases	3.2 or later

log-adjacency-changes

Configures the router to send a syslog message when an OSPF neighbor does up or down.

Command	log-adjacency-changes [detail]
Options	detail — (Optional) Logs detailed adjacency changes
Modes	ROUTER-OSPF
Usage	This command is enabled by default but only up or down events are reported. Use the detail option to view complete information.
Examples	sonic(config-router-ospf)# log-adjacency-changes sonic(config-router-ospf)# log-adjacency-changes detail sonic(config-router-ospf)# no log-adjacency-changes
Releases	3.1 or later

log-neighbor-changes

Enables logging of neighbor state transition events.

Command	log-neighbor-changes
Options	None
Modes	ROUTER-BGP
Usage	Use this command to enable logging of neighbor up/down events along with reason code for down event.
Examples	<pre>sonic(config-router-bgp) # log-neighbor-changes</pre> <pre>sonic(config-router-bgp) # no log-neighbor-changes</pre>
Releases	3.0 or later

logger

Enters messages into the system log.

Command	logger message
Options	message—Message to enter into the system log
Command mode	EXEC
Usage	Use this command to enter custom messages into the system log.
Example	<pre>sonic# logger</pre>

Releases 3.1 or later

logging security-profile

Enables the security profile for Syslog TLS communication with a Syslog server.

Command	logging security-profile <i>profile-name</i>
Options	• <i>profile-name</i> — Enter the name of a TLS security profile used in Syslog server connections.
Modes	CONFIGURATION
Usage	Before you enable a TLS security profile, you must configure TLS to be used to send Syslog messages to a remote Syslog server (logging server command). Then you must create a trust store for TLS CA certificates, associate an installed CA certificate with the trust store, create a TLS security profile that is used to authenticate Syslog servers, and associate the TLS security profile with the trust store. The logging server uses the TLS security-profile certificate to establish Syslog server connections. To create a TLS security profile, use the crypto security-profile command. To associate a CA certificate with a trust store, use the crypto trust-store ca-cert command.
Example	<pre>sonic(config) # logging server 100.104.120.166 message-type log protocol tls vrf Vrf001 sonic(config) # crypto trust-store syslogts ca-cert ca sonic(config) # crypto security-profile logserver peer-name-check true revocation-check true sonic(config) # crypto security-profile logserver trust-store syslogts sonic(config) # logging security-profile logserver</pre>
Releases	4.4.1 or later

logging server

Configures a remote server to receive Syslog and audit log messages.

Command	<code>logging server {hostname ip-address ipv6-address} [source-interface interface-type] [protocol protocol] [remote-port port-number] [vrf vrf-name] [message-type type] [severity level]</code>
Options	<ul style="list-style-type: none">• <i>hostname</i> — Enter the hostname of a remote server.• <i>ip-address</i> — Enter the IP address of the remote server.• <i>ipv6-address</i> — Enter the IPv6 address of the remote server.• <i>source-interface interface-type</i> — (Optional) Enter an Ethernet, loopback, management, port channel, or VLAN interface IP address to be used as the source interface when sending packets.• <i>protocol protocol</i> - (Optional) Enter the communication protocol to use when sending logging server messages: <code>tcp</code>, <code>tls</code>, or <code>udp</code>. <code>UDP</code> is the default.• <i>remote-port port-number</i> — (Optional) Enter the remote port number. The range is from 1 to 65535.• <i>vrf vrf-name</i> — (Optional) Enter the name of the VRF used to send Syslog messages.• <i>message-type type</i> — (Optional) Enter a message type (The default is to send all Syslog and audit log messages):<ul style="list-style-type: none">◦ <code>log</code>: Send all Syslog messages.◦ <code>event</code>: Send only Syslog messages that are tagged with the keywords <code>EVENT</code> and <code>ALARM</code> for system operation and alarms.◦ <code>audit</code>: Send only audit log messages.◦ <code>auditd-system</code>: Send Auditd messages.• <i>severity level</i> — (Optional) Enter the severity level of the logged messages to be sent to a remote server. Messages only with the specified and higher severity levels are sent. Messages with lower severity levels are not forwarded to remote servers.<ul style="list-style-type: none">◦ To forward all Syslog or audit log messages to a remote server, set the severity level to the lowest level <code>0 emerg</code>. The severity levels of Syslog and audit log messages are <code>debug(7)</code>, <code>info(6)</code>, <code>notice(5)</code>, <code>warning(4)</code>, <code>error(3)</code>, <code>crit(2)</code>, <code>alert(1)</code>, and <code>emerg(0)</code>. The default severity level is <code>notice</code>.◦ For Event messages (<i>message-type event</i>), the severity level setting is ignored. Event messages of all severity levels are forwarded to a remote server.
Modes	CONFIGURATION
Usage	Use this command to configure a remote server to which Syslog or audit log messages are sent.
Examples	<pre>sonic(config)# logging server message-type log 20.1.1.1 source-interface Ethernet 2 vrf Vrf1</pre> <pre>sonic(config)# no logging server 20.1.1.1 message-type log source-interface Ethernet 2 vrf Vrf1</pre> <pre>sonic(config)# logging server message-type event 10.59.143.28 source-interface Loopback 1 vrf Vrf1</pre> <pre>sonic(config)# logging server 100.104.120.166 message-type log protocol tls vrf Vrf001</pre> <pre>sonic(config)# logging server 100.94.218.203 message-type audit severity info</pre>
Releases	3.2 or later

login exec-timeout

Configures the timeout used to terminate a user session when a user session is idle longer than the configured time.

Command	<code>login exec-timeout <i>timeout-seconds</i></code>
Options	<code><i>timeout-seconds</i></code> — Enter the login session timeout in seconds (0 to 3600; default is 600).
Modes	CONFIGURATION
Usage	The login session timeout applies to MF-CLI, console, and SSH sessions. To apply the <code>login exec-timeout</code> configuration to MF-CLI, SSH, and console sessions, you must restart the session. The login session timeout can only be configured by <code>admin</code> and <code>secadmin</code> roles. To unconfigure the current <code>login exec-timeout</code> value and return to the default setting, enter the <code>no login exec-timeout</code> command.
Examples	<pre>sonic(config)# login exec-timeout 1200</pre>
Releases	4.4.0 or later

login lockdown

Configures the maximum number of failed login attempts and lockout period.

Command	<code>login lockdown {max-retries <i>number</i> period <i>minutes</i> console-exempt}</code>
Options	<ul style="list-style-type: none"><code>max-retries <i>number</i></code> — Maximum number of consecutive failed login attempts that are allowed before a user is locked out (0 to 16; default 3).<code>period <i>minutes</i></code> — Number of minutes that a user ID is prevented from logging in to the switch after the maximum number of failed login attempts is exceeded (0 to 43200; default 0).<code>console-exempt</code> — (Optional) Disable lockout for console logins and enable a user to log in through the console when the user ID is locked out.
Modes	CONFIGURATION
Usage	By default, the login lockdown feature is disabled. A maximum of three consecutive failed password attempts are supported on a switch. No lockout period (0 minutes) is configured. To enable the login lockdown feature, configure a lockout period. Login failures include failures on the console as well. To disable the login lockdown feature, configure the lockout period as 0. Use the <code>login lockdown console-exempt</code> command to disable lockout for logins from the console and allow locked out users to log in to the switch from the console.
Examples	<pre>sonic(config)# login lockdown max-retries 5</pre> <pre>sonic(config)# login lockdown period 10</pre> <pre>sonic(config)# login lockdown console-exempt</pre>
Releases	4.2.0 or later

login password-attributes

Creates stronger password rules to increase password strength.

Command	<code>login password-attributes {[min-length <i>number</i>] [character-restriction {[upper] [lower] [numeric] [special-char]}}]}</code>
Options	<ul style="list-style-type: none"><code>min-length <i>number</i></code> — (Optional) Enter the minimum number of required alphanumeric characters (6 to 32; default 8).

- `character-restriction upper` — (Optional) Enter the minimum number of uppercase characters required in a password (0 to 31; default 0).
- `character-restriction lower` — (Optional) Enter the minimum number of lowercase characters required in a password (0 to 31; default 0).
- `character-restriction numeric` — (Optional) Enter the minimum number of numeric characters required in a password (0 to 31; default 0).
- `character-restriction special-char` — (Optional) Enter the minimum number of special characters required in a password (0 to 31; default 0).

Modes

CONFIGURATION

Usage

When you log in to Enterprise SONiC the first time and are prompted to change your password, and when you configure new users and roles, the password requirement is eight alphanumeric characters minimum. Use the `login password-attributes` command to increase password strength. The password rules you create apply to password configuration with the `username password role` command

i **NOTE:** The password requirements you create are applied only to new user passwords configured with the `username password role` command. New password requirements are not applied to existing user passwords that were created without the stronger requirements.

Examples

```
sonic(config)# login password-attributes min-length 7
sonic(config)# login password-attributes character-restriction lower 4
sonic(config)# login password-attributes character-restriction upper 1
```

Releases

4.4.0 or later

mab

Enables MAC Authentication Bypass (MAB) on an interface.

Command

`mab [auth-type {pap | eap-md5 | chap}]`

Options

- `auth-type`—(Optional) Specify the authentication type to be used for MAB
- `chap`—Enable CHAP as an authentication type
- `eap-md5`—Enable EAP-MD5 as an authentication type
- `pap`—Enable PAP as an authentication type

Modes

INTERFACE

Usage

By default, MAB is disabled on the interface. This command provides options to specify the type of authentication to be used, which can be either EAP-MD5, PAP, CHAP. If MAB is enabled without the authentication type, EAP-MD5 is used by default.

Examples

Enable MAB without authentication type:

```
sonic# configure terminal
sonic(config)# interface Ethernet 1
sonic(config-if-Ethernet1)# mab
sonic(config-if-Ethernet1)#

```

Enable MAB with authentication type:

```
sonic# configure terminal
sonic(config)# interface Ethernet 1
sonic(config-if-Ethernet1)# mab auth-type chap
```

Releases

4.0 or later

mab request format

Sets configuration parameters that are used to format attribute1 for MAB requests to the RADIUS server.

Command map request format attribute 1 groupsize *size* {separator {separator-type {[lowercase | uppercase]}}}

- Options**
- *size*—Enter group size with in the supported values listed . The valid values are 1, 2, 4, and 12 (default 2).
 - *separator-type*—Configure separator as '-' or ':' or '.' (default ':').
 - *lowercase*—(Optional) Use lowercase for formatting the RADIUS attribute 1 in MAB request.
 - *uppercase*—(Optional) Use uppercase for formatting the RADIUS attribute 1 in MAB request (default).

Modes CONFIGURATION

Usage RADIUS attribute 1 is the username, which is often the client MAC address. The default case for the MAC address is uppercase.

Examples

```
sonic# configure terminal
sonic(config)# mab request format attribute 1 groupsize 2 separator :
lowercase
```

Releases 4.0 or later

mab timeout

Configures MAB timers on an interface.

Command mab timeout server-timeout *server-timeout*

Options *server-timeout* *server-timeout*—Enter the value in seconds (1 to 65535; default is 30).

Modes INTERFACE

Usage Use this command to set the timer value that dot1x uses to timeout the authentication server.

Examples

```
sonic# configure terminal
sonic(config)# interface Ethernet 10
sonic(config-if-Ethernet10)# mab timeout server-timeout 400
```

Releases 4.1.0 or later

mac access-group

Configures a MAC access group.

Command mac access-group *access-list-name* {in | out}

- Options**
- *access-list-name* — MAC access list name (up to 63 characters)
 - *in* — Apply the filter to incoming traffic
 - *out* — Apply the filter to outgoing traffic

Modes INTERFACE

Usage ACL must be created first and be of type MAC to be applied. Only one ACL of a given type can be applied per interface and per direction.

Examples

```
sonic(config-if-Vlan10) # mac access-group macacl-example in  
sonic(config-if-Vlan10) # no mac access-group
```

Releases

3.1 or later

mac access-list

Creates a MAC access-list.

Command

```
mac access-list access-list-name
```

Options

access-list-name — MAC access-list name (up to 63 characters)

Modes

INTERFACE

Usage

ACL name can be of maximum 63 characters. The name must begin with A-Z, a-z or 0-9. Underscore and hyphens can be used except as the first character. ACL name must be unique across all ACL types.

Examples

```
sonic(config) # mac access-list macacl-example  
sonic(config) # no mac access-list macacl-example
```

Releases

3.1 or later

mac address-table

Adds a static MAC address table.

Command

```
mac address-table mac-address {vlan {phy-if-name | PortChannel}}
```

Options

- *mac-address*—Static MAC address to add in nn:nn format
- *phy-if-name*—(Optional) Physical interface ID (0 to 255)

Modes

CONFIGURATION

Usage

Use this command to add a static MAC address manually to the MAC address table. Specify the Ethernet port, PortChannel, and VLAN through which the device with the static MAC address can be reached and to which the switch can forward packets.

Examples

```
sonic# configure terminal  
sonic(config) # mac address-table 00:22:33:44:55:66  
sonic(config) # no mac address-table 00:22:33:44:55:66
```

Releases

3.2 or later

mac address-table aging-time

Adds MAC address table aging time.

Command

```
mac address-table aging-time mac-time
```

Options

mac-time—Enter the MAC time in seconds (0 to 1,000,000; default is 600).

Modes

CONFIGURATION

Usage Use this command to configure the aging time for all dynamically learned MAC addresses. Static MAC address entries are not affected by the `mac address-table aging-time` command. When the aging time is reached, a dynamic MAC address entry is deleted from the table. Enter 0 to disable MAC aging. Use the no version of the command to restore the default aging time.

Examples

```
sonic# configure terminal
sonic(config)# mac-address-table aging-time 300

sonic(config)# no mac-address-table aging-time
```

Releases 3.1 or later

mac address-table dampening-interval

Sets the MAC move dampening threshold interval.

Command `mac address-table dampening-interval seconds`
Options *interval-value*—Enter the dampening interval value (5 to 120; default 5)
Command mode CONFIGURATION
Usage Use this command to configure the minimum time interval that a dynamic MAC address can be moved to different interfaces.

Examples

```
sonic(config)# mac address-table dampening-interval 10

sonic(config)# no mac address-table dampening-interval
```

Releases 3.1 or later

mac address-table dampening-threshold

Sets the MAC move dampening threshold.

Command `mac address-table dampening-threshold number`
Options *threshold-value*—Enter the dampening threshold value (5 to 100; default 5)
Command mode EXEC
Usage Use this command to limit the maximum number times that a dynamic MAC address can be moved to different interfaces.

Example

```
sonic# mac address-table dampening-threshold 10
```

Releases 3.1 or later

mac-holdtime

Configures the hold time used to wait before aging out the MAC addresses of downstream devices that are learned from multihomed peer VTEPs and that have not been used.

Command `mac-holdtime seconds`
Options *seconds* — Hold time in seconds (0-86400; default 300)
Modes EVPN-ESI-MULTIHOMING

Usage

When a MAC address is deleted from the multihomed VTEP on which it is learned, the timer is restarted on the remote multihomed VTEPs in the EVPN Ethernet segment, which continue to advertise the downstream MAC address. To configure the hold time used to wait before aging out ARP/ND entries that are learned from multihomed peer VTEPs and that have not been used, use the [neigh-holddtime](#) command.

Examples

```
sonic(config) # evpn esi-multihoming
sonic(config-evpn-esi-mh) # mac-holddtime 2000
```

Releases

4.2.0 or later

map

Configures VNI-VLAN and VNI-VRF mappings.

Command

```
map vni {vnid {{Vlan {vid {[count] [numvid]}}} | {vrf vrf-name}}}
```

Options

- *vnid*—VNI value (1 to 16777215)
- *vid*—VLAN ID (1 to 4094)
- *numvid*—(Optional) Number of mappings
- *vrf-name*—VRF instance name (up to 63 characters)

Modes

INTERFACE VXLAN

Usage

Use this command to map L2 VNIs to VLAN or L3 VNIs to VRF.

Examples

```
sonic(config) # interface Vxlan vtep1
sonic(config-if-Vxlan-vtep1) # map vni 100 vlan 100 count 2
sonic(config-if-Vxlan-vtep1) # map vni 100 vrf vrf1

sonic(config-if-Vxlan-vtep1) # no map vni 100 vrf vrf1
```

Releases

3.0 or later

match access-group

Match parameters using an access-group.

Command

```
match access-group {mac | ip | ipv6} access-list-name
```

Options

- *mac access-list-name*—MAC access-list name (up to 63 characters)
- *ip access-list-name*—IPv4 access-list name (up to 63 characters)
- *ipv6 access-list-name*—IPv6 access-list name (up to 63 characters)

Modes

CLASS-MAP

Usage

Use this command to match the incoming traffic based on MAC ACL, IP ACL, or IPv6 ACL.

Examples

```
sonic(config) # class-map class_ip_acl match-type acl
sonic(config-class-map) # match access-group ip ip_acl1

sonic(config-class-map) # no match access-group
```

Releases

3.1 or later

match as-path

Configures a routing policy to match criteria to an AS path.

Command	<code>match as-path <i>as-path-name</i></code>
Options	<code><i>as-path-name</i></code> — Name of the established AS-PATH ACL (up to 140 characters)
Modes	ROUTE-MAP
Usage	Use this command to configure a filter to match routes that have a specific AS path in their BGP path.
Examples	<pre>sonic(config)# route-map match_as_path permit 1 sonic(config-route-map)# match as-path acl10 sonic(config-route-map)# no match as-path</pre>
Releases	3.0 or later

match community

Configures a routing policy to match criteria to a BGP community.

Command	<code>match community <i>community-name</i></code>
Options	<code><i>community-name</i></code> — Name of the configured community list
Modes	ROUTE-MAP
Usage	Use this command to configure a filter to match routes that have a specific COMMUNITY attribute in their BGP path.
Examples	<pre>sonic(config-route-map)# match community commlist1 sonic(config-route-map)# no match community</pre>
Releases	3.0 or later

match dei

Matches packets using the drop eligible indicator (DEI) value.

Command	<code>match dei <i>dei-val</i></code>
Options	<code><i>dei-val</i></code> —DEI value (0 to 1)
Modes	CLASS-MAP
Usage	Use this command to match the incoming traffic based on drop DEI value.
Examples	<pre>sonic(config)# class-map class1_fields match-type fields match-all sonic(config-class-map)# match dei 0 sonic(config-class-map)# no match dei</pre>
Releases	3.1 or later

match destination-address

Match packets using the destination address.

Command	<code>match destination-address {{mac {{destination-mac-addr destination-mac-mask} {destination-mac-host destination-mac-addr}}} {ip {destination-ip-prefix {destination-ip-host destination-ip}}} {ipv6 {destination-ip-prefix {destination-ip-host destination-ip}}}}}</code>
Options	<ul style="list-style-type: none">• <code>destination-mac-addr</code>—Destination MAC host address• <code>destination-mac-mask</code>—Destination MAC address in nn::nn format• <code>destination-ip-prefix</code>—Destination IP prefix in A.B.C.D/mask format• <code>destination-ip</code>—Destination host IP address in A.B.C.D/mask or A::B/mask format
Modes	CLASS-MAP
Usage	Use this command to match the incoming traffic based on destination MAC address, IP address, or IPv6 address.
Examples	<pre>sonic(config)# class-map class1_fields match-type fields match-all sonic(config-class-map)# match destination-address ip 2.1.1.1/32 sonic(config-class-map)# no match destination-address ip</pre>
Releases	3.1 or later

match dscp

Configures class-map to match DSCP.

Command	<code>match dscp {default cs1 cs2 cs3 cs4 cs5 cs6 cs7 af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 ef voice-admit dscp-val}</code>
Options	<code>dscp-val</code> —DSCP value
Modes	CLASS-MAP
Usage	Use this command to match the incoming traffic based on DSCP values.
Examples	<pre>sonic(config)# class-map class1_fields match-type fields match-all sonic(config-class-map)# match dscp cs1 sonic(config-class-map)# no match dscp</pre>
Releases	3.1 or later

match ethertype

Matches packets based on the ethertype value.

Command	<code>match ethertype {arp ip ipv6 ethertype}</code>
Options	<ul style="list-style-type: none">• <code>ethertype</code>—Description (0x600 to 0xffff)• <code>arp</code>—ARP ethertype (0x806)• <code>ip</code>—IPv4 ethertype (0x800)• <code>ipv6</code>—IPv6 ethertype (0x86dd)
Modes	CLASS-MAP

Usage	Use this command to match the incoming traffic based on Ethertype.
Examples	<pre>sonic(config) # class-map class1_fields match-type fields match-all sonic(config-class-map) # match ethertype ip sonic(config-class-map) # match ethertype 0x8100 sonic(config-class-map) # no match ethertype</pre>
Releases	3.1 or later

match evpn

Sets a routing policy to match criteria to BGP EVPN.

Command	<code>match evpn {default-route {route-type {macip multicast prefix}} {vni vni-number}}</code>
Options	<code>vni-number</code> —VNI number
Command mode	ROUTE-MAP
Usage	Use this command to match EVPN routes based on route-type and VNI.
Examples	<pre>sonic(config-router-evpn) # match evpn route-type prefix sonic(config-router-evpn) # no match evpn route-type prefix</pre>
Releases	3.1 or later

match ext-community

Configures a routing policy to match criteria to a BGP extended community.

Command	<code>match ext-community <i>community-name</i></code>
Options	<code><i>community-name</i></code> — Name of the configured ext-community list
Modes	ROUTE-MAP
Usage	Use this command to configure a filter to match routes that have a specific EXTCOMMUNITY attribute in their BGP path.
Examples	<pre>sonic(config-route-map) # match ext-community extcommalist1 sonic(config-route-map) # no match ext-community</pre>
Releases	3.0 or later

match interface

Configures a routing policy to match criteria to an interface.

Command	<code>match interface {<i>phy-if-name</i> PortChannel {Vlan <i>vlan-id</i>}}</code>
Options	<ul style="list-style-type: none"> <code><i>phy-if-name</i></code> — Physical interface name as the next-hop interface <code><i>vlan-id</i></code> — VLAN number as the next-hop interface (1 to 4094)
Modes	ROUTE-MAP

Usage	Use this command to configure a filter to match routes whose next-hop is the configured interface.
Examples	<pre>sonic(config-route-map) # match interface Ethernet 28</pre> <pre>sonic(config-route-map) # no match interface</pre>
Releases	3.2 or later

match ip protocol

Updates class-map match IP attributes.

Command	<code>match ip protocol {ip-protocol-val icmp icmpv6 tcp udp}</code>
Options	<code>ip-protocol-val</code> —Enter the IP protocol number (0 to 255)
Modes	CLASS-MAP
Usage	Use this command to match the incoming traffic based on IP protocol values.
Examples	<pre>sonic(config) # class-map class1_fields match-type fields match-all</pre> <pre>sonic(config-class-map) # match ip protocol tcp</pre> <pre>sonic(config-class-map) # no match ip protocol</pre>
Releases	3.1 or later

match ip address prefix-list

Configures routing policy match criteria to an IPv4 prefix-list.

Command	<code>match ip address prefix-list <i>prefix-list-name</i></code>
Options	<code>prefix-list-name</code> — Name of the configured IPv4 prefix-list to match against
Modes	ROUTE-MAP
Usage	Use this command to configure a filter to match routes based on a specified IPv4 prefix-list name.
Examples	<pre>sonic(config-route-map) # match ip address prefix-list test100</pre> <pre>sonic(config-route-map) # no match ip address prefix-list</pre>
Releases	3.0 or later

match ip next-hop prefix-list

Configures a routing policy to match criteria to a next-hop prefix-list.

Command	<code>match ip next-hop prefix-list <i>match-hop</i></code>
Options	<code>match-hop</code> — Name of the configured IPv4 prefix-list to match against
Modes	ROUTE-MAP
Usage	Use this command to configure a filter to match based on the next-hop IPv4 addresses specified in IP prefix lists.

Examples

```
sonic(config-route-map)# match ip next-hop prefix-list test100
```

```
sonic(config-route-map)# no match ip next-hop prefix-list
```

Releases

3.0 or later

match ipv6 address prefix-list

Configures a routing policy to match criteria to an IPv6 prefix-list.

Command

```
match ipv6 address prefix-list prefix-list-name
```

Options

prefix-list-name — Prefix-list name to match against

Modes

ROUTE-MAP

Usage

Use this command to configure a filter to match routes based on a specified IPv6 prefix-list name.

Examples

```
sonic(config-route-map)# match ipv6 address prefix-list test100
```

```
sonic(config-route-map)# no match ipv6 address prefix-list
```

Releases

3.0 or later

match l4-port

Matches packets based on the TCP/UDP port.

Command

```
match l4-port {source | destination} {{eq eq-port-val} | {range begin-port-val end-port-val}}
```

Options

- *source* — Match packets based on the source
- *destination* — Match packets based on the destination
- *eq-port-val* — Match packets based on the equal port value
- *begin-port-val* — Match packets based on the beginning port value
- *end-port-val* — Match packets based on the ending port value

Modes

CLASS-MAP

Usage

Match on source port is allowed only when IP protocol is set to TCP or UDP.

Examples

```
sonic(config)# class-map class1 fields match-type fields match-all  
sonic(config-class-map)# match l4-port source eq 10
```

```
sonic(config-class-map)# no match l4-port source
```

Releases

3.1 or later

match local-preference

Configures a routing policy to match criteria to local-preference.

Command

```
match local-preference match-loc
```

Options

match-loc — Local-preference to match against

Modes

ROUTE-MAP

Usage Use this command to configure a routing policy to match criteria to a local-preference value.

Examples

```
sonic(config-route-map) # match local-preference 10000  
sonic(config-route-map) # no match local-preference
```

Releases 3.0 or later

match metric

Configures a filter to match on a specific value.

Command match metric *match-met*
Options metric *match-met* — Value to match the route metric against (0 to 4294967295)
Modes ROUTE-MAP

Usage Use this command to configure a routing policy to match criteria to a metric.

Examples

```
sonic(config-route-map) # match metric 429132  
sonic(config-route-map) # no match metric
```

Releases 3.0 or later

match origin

Configures a filter to match routes based on the origin attribute of BGP.

Command match origin {egp | igrp | incomplete}
Options

- egp—Match only remote EGP routes
- igrp—Match only local IGP routes
- incomplete—Match on unknown routes learned through some other means

Modes ROUTE-MAP

Usage Use this command to match the routes based on the origin attribute of BGP.

Examples

```
sonic(config) # route-map bgp  
sonic(config-route-map) # match origin egp  
sonic(config-route-map) # no match origin
```

Releases 3.0 or later

match pcp

Matches packets based on PCP.

Command match pcp {be | bk | ee | ca | vi | vo | ic | nc | {pcp-val}}
Options

- be—Best effort
- bk—Background
- ee—Excellent effort
- ca—Critical applications

- vi—Video, < 100 ms latency and jitter
- v0—Voice, < 10 ms latency and jitter
- ic—Internetwork control
- nc—Network control
- *pcp-val*—Enter the PCP value (0 to 7)

Modes

CLASS-MAP

Usage

Use this command to match the incoming traffic based on the PCP value in the VLAN header.

Examples

```
sonic(config)# class-map class1_fields match-type fields match-all
sonic(config-class-map)# match pcp vi

sonic(config-class-map)# no match pcp
```

Releases

3.1 or later

match peer

Configures a routing policy to match criteria to a peer IP.

Commandmatch peer {*match-peer* | *phy-if-name* | PortChannel | { Vlan *vlan-id*} }**Options**

- *match-peer* — Peer IPv4 or IPv6 address in A.B.C.D or A::B format
- *phy-if-name* — Physical interface name
- Vlan *vlan-id* — VLAN ID (1 to 4094)

Modes

ROUTE-MAP

Usage

Use this command to configure a routing policy to match criteria to an IPv4 or IPv6 peer.

Examples

```
sonic(config-route-map)# match peer 10.1.1.100 Vlan4

sonic(config-route-map)# no match peer
```

Releases

3.2 or later

match protocol

Matches protocol trap to classifier.

Commandmatch protocol *trap-id***Options***trap-id*—Trap ID to match (up to 63 characters)**Modes**

- CLASS-MAP
- CLASSIFIER

Usage

Only the match conditions that are configured for a user-created CoPP classifier can be added and removed. You cannot modify the system CoPP classifier match conditions. You can add a protocol trap ID only to a single user CoPP classifier. Adding a protocol trap ID to multiple user CoPP classifiers results in a configuration error and can result in undefined behavior.

Examples

```
sonic(config)# classifier copp-system-arp match-type copp
sonic(config-classifier)# match protocol arp_req
sonic(config-classifier)# match protocol arp_resp
sonic(config-classifier)# match protocol neigh_discovery

sonic(config-class-map)# no match protocol
```

Releases	3.1 or later
-----------------	--------------

match source-address

Matches packets based on the source address.

Command	match source-address {{mac {{source-mac-addr source-mac-mask} {source-mac-host source-mac-addr}}}} {ip {source-ip-prefix {source-ip-host source-ip}}}} {ipv6 {source-ip-prefix {source-ip-host source-ip}}}}
----------------	--

Options	<ul style="list-style-type: none">• <i>source-mac-addr</i>—Enter the source MAC address• <i>source-mac-mask</i>—Source MAC mask• <i>source-ip-prefix</i>—Source IP or IPv6 prefix• <i>source-ip</i>—Source IP host address
----------------	---

Modes	CLASS-MAP
--------------	-----------

Usage	Use this command to match the incoming traffic based on the source MAC address, IP address, or IPv6 address.
--------------	--

Examples	<pre>sonic(config)# class-map class1_fields match-type fields match-all sonic(config-class-map)# match source-address ip 1.1.1.1/32 sonic(config-class-map)# no match source-address ip</pre>
-----------------	--

Releases	3.1 or later
-----------------	--------------

match source-protocol

Configures the source protocol to match.

Command	match source-protocol {bgp ospf ospfv3 static connected}
----------------	--

Options	None
----------------	------

Modes	ROUTE-MAP
--------------	-----------

Usage	Use this command to match BGP, OSPF, OSPFv3, static, or connected source protocols.
--------------	---

Examples	<pre>sonic(config-route-map)# match source-protocol bgp sonic(config-route-map)# no match source-protocol</pre>
-----------------	--

Releases	3.0 or later
-----------------	--------------

match source-vrf

Matches packets based on the source VRF.

Command	match source-vrf <i>src-vrf</i>
----------------	---------------------------------

Options	<i>src-vrf</i> —Source VRF (up to 15 characters)
----------------	--

Modes	ROUTE-MAP
--------------	-----------

Usage	Use this command to match the routes based on source VRF.
--------------	---

Examples

```
sonic(config) # route-map map1 permit 10
sonic(config-route-map) # match source-vrf Vrf1

sonic(config-route-map) # no match source-vrf
```

Releases

3.1 or later

match tag

Creates a filter to redistribute only routes that match a specific tag value.

Command match tag *match-tag***Options** *match-tag*—Tag value to match with the tag number (1 to 4294967295)**Modes** ROUTE-BGP**Usage** Use this command to create a filter to distribute only routes that match a specific tag value.**Examples**

```
sonic(config-route-bgp) # match tag 656442

sonic(config-route-bgp) # no match tag
```

Releases

3.0 or later

match tcp-flags

Match packets based on TCP flags.

Command match tcp-flags {[fin] | [not-fin]} {[syn] | [not-syn]} {[rst] | [not-rst]} {[psh] | [not-psh]} {[ack] | [not-ack]} {[urg] | [not-urg]}**Options**

- fin — (Optional) Match packets to the finish flag
- not-fin — (Optional) Match packets to the not finish flag
- syn — (Optional) Match packets to the synchronize flag
- not-syn — (Optional) Match packets to the not synchronize flag
- rst — (Optional) Match packets to the reset flag
- not-rst — (Optional) Match packets to the not reset flag
- psh — (Optional) Match packets to the push flag
- not-psh — (Optional) Match packets to the not push flag
- ack — (Optional) Match packets to the acknowledge flag
- not-ack — (Optional) Match packets to the not acknowledge flag
- urg — (Optional) Match packets to the urgent flag
- not-urg — (Optional) Match packets to the not urgent flag

Modes CLASS-MAP**Usage** Match on TCP flags is allowed only when the IP protocol is set to TCP. *not-xxx* can be used to match the corresponding flag set to 0.**Examples**

```
sonic(config) # class-map class1 fields match-type fields match-all
sonic(config-class-map) # match tcp-flags urg

sonic(config-class-map) # no match tcp-flags
```

Releases

3.1 or later

match vlan

Match packets based on the VLAN ID.

Command	<code>match Vlan <i>vlan-id</i></code>
Options	<code>vlan-id</code> —Enter the VLAN ID (1 to 4094)
Modes	CLASS-MAP
Usage	Use this command to match the incoming traffic based on the VLAN ID.
Examples	<pre>sonic(config)# class-map class1_fields match-type fields match-all sonic(config-class-map)# match vlan 200 sonic(config-class-map)# no match vlan</pre>
Releases	3.1 or later

max-flows

Configures the maximum number of flows that can be maintained per ARS object.

Command	<code>max-flows <i>maximum-flows</i></code>
Options	<code>maximum-flows</code> —Enter the maximum flows. Valid values are 256, 512, 1024, 2048, 4096, 8192, 16384, and 32768. The default value is 256.
Modes	ARS-OBJECT
Usage	Configure the maximum flow value to the power of 2.
Example	<pre>sonic(config)# ars object default sonic(config-ars-object)# max-flows 256</pre>
Releases	4.4.0 or later

max-med

Configures BGP to advertise routes with maximum MED value under a given condition.

Command	<code>max-med {{on-startup {<i>stime</i> [<i>maxmedval</i>]}} {administrative [<i>maxmedval</i>]}}</code>
Options	<ul style="list-style-type: none">• <code><i>stime</i></code> — Startup time• <code><i>maxmedval</i></code> — (Optional) Maximum MED value
Modes	ROUTER-BGP
Usage	Use this command to instruct BGP to advertise routes with the maximum MED value. Set the condition under which routes with max MED value will be sent. Options include during the startup for a prespecified number of seconds, and the other is permanently (administrative). You can also specify the value for max MED.
Examples	<pre>sonic(config)# router bgp 65300 sonic(config-router-bgp)# max-med on-startup 300 2000 sonic(config-router-bgp)# no max-med on-startup</pre>
Releases	3.2 or later

max-metric

Configures a router than is running OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in the shortest path first calculations.

Command	<code>max-metric router-lsa {[administrative] {[on-startup <i>interdistance</i>]}} {[all [<i>maxmetricvalue</i>]]} {[include-stub [<i>maxmetricvalue</i>]]}}</code>
Options	<ul style="list-style-type: none">• <i>interdistance</i> — (Optional) Interdistance value• <i>maxmetricvalue</i> — (Optional) Maximum metric value
Modes	ROUTER-OSPF
Usage	Use this command to originate LSAs with a maximum metric (infinity) through all nonstub links, which allows BGP routing tables to converge without attracting traffic (if there are not alternate lower cost paths around the router). The router will advertise accurate (normal) metrics after the configured or default timer expire, or after BGP send a notification that routing tables have converged. This command can be enabled administratively or during OSPFv2 startup time. When enabled administratively, command advertising is effective until it unconfigures explicitly. When enabled for restart time, this command is advertised for the time that is specified in the configuration.
Examples	<pre>sonic(config-router-ospf)# max-metric router-lsa administrative</pre> <pre>sonic(config-router-ospf)# max-metric router-lsa on-startup 90</pre> <pre>sonic(config-router-ospf)# no max-metric router-lsa administrative</pre>
Releases	3.2 or later

maximum-paths

Configures the maximum number of equal-cost paths for load sharing.

Command	<code>maximum-paths <i>paths</i></code>
Options	<i>paths</i> — Number of parallel paths (1 to 64)
Command mode	ADDRESS-FAMILY
Usage	Use this command to configure BGP to control the maximum number of equal cost multipath routes to eBGP destinations, per address-family.
Examples	<pre>sonic(config-router-bgp-af)# maximum-paths 32</pre> <pre>sonic(config-router-bgp-af)# no maximum-paths</pre>
Releases	3.1 or later

maximum-paths ibgp

Configures the maximum number of equal-cost paths for load sharing.

Command	<code>maximum-paths ibgp <i>ipaths</i> [equal-cluster-length]</code>
Options	<i>ipaths</i> — Number of internal parallel paths (1 to 64)
Command mode	ADDRESS-FAMILY
Usage	Use this command to configure BGP to control the maximum number of equal cost multipath routes to iBGP destinations, per address-family.

Examples

```
sonic(config-router-bgp-af) # maximum-paths ibgp 32
```

```
sonic(config-router-bgp-af) # no maximum-paths ibgp
```

Releases

3.1 or later

maximum-prefix

Configures the maximum number of prefixes that are allowed from a BGP neighbor or neighbors in a peer-group.

Command

```
maximum-prefix max-prefix-val {[threshold-val] {[warning-only] | {[restart interval]}]}
```

Options

- *max-prefix-val* — Maximum prefix number (1 to 4294967295)
- *threshold-val* — (Optional) Threshold percentage (1 to 100)
- *interval* — (Optional) Interval

Command mode

ADDRESS-FAMILY

Usage

Use this command to set the upper limit on the number of BGP prefixes to accept from this neighbor, or neighbors in a peer-group. Set the optional threshold parameter to receive warnings when a threshold is reached, and when BGP restarts neighborship once the maximum prefix limit is exceeded.

Examples

```
sonic(config-router-bgp-neighbor-af) # maximum-prefix 2000 80 warning-only
```

```
sonic(config-router-bgp-neighbor-af) # no maximum-prefix 2000 80 warning-only
```

Releases

3.1 or later

mclag

Configures an MLAG interface.

Command

```
mclag domain_id
```

Options

domain_id—Domain ID (1 to 4095)

Modes

INTERFACE

Usage

Use this command to configure the port channel as MLAG port-channel interface. This command is applicable only on the port-channel interface.

Examples

```
sonic(config) # interface PortChannel 200  
sonic(config-if-po200) # mclag 12
```

```
sonic(config-if-po10) # no mclag
```

Releases

3.0 or later

mclag domain

Configures the MLAG domain ID.

Command

```
mclag domain mlag-domain-id
```

Options

domain mlag-domain-id—MLAG domain ID number (1 to 4095)

Modes

CONFIGURATION

Usage	Use this command to configure the MCLAG domain.
Examples	<pre>sonic# configure terminal sonic(config)# mclag domain 100 sonic(config-mclag-domain-100)# sonic(config)# no mclag domain</pre>
Releases	3.0 or later

mclag gateway-mac

Deletes the gateway MAC for MCLAG.

Command	<code>mclag gateway-mac <i>gw_mac</i></code>
Options	<i>gw_mac</i> —Gateway MAC address
Modes	CONFIGURATION
Usage	By default, an MCLAG switch and its peers use the system MAC address of the active peer as the gateway MAC address in L3 interfaces. Use this command to use a common configurable gateway MAC address for the L3 VLAN interfaces in which the peer link is a VLAN member.
Examples	<pre>sonic(config)# mclag gateway-mac 00:aa:bb:bb:cc:cc sonic(config)# no mclag gateway-mac</pre>
Releases	3.1 or later

mclag-peer-gateway

Configures MCLAG peer gateway.

Command	<code>mclag-peer-gateway</code>
Options	None
Modes	INTERFACE
Usage	Use this command to enable MCLAG peer gateway on VLAN interface. This enables the switch to route traffic on behalf of other MCLAG peer when packet hashes to the peer with the destination MAC of other MCLAG peer. This command should be used along with <code>mclag-separate-ip</code> command. Configure <code>mclag-separate-ip</code> command first, and followed-by <code>mclag-peer-gateway</code> command. This command is applicable only on a VLAN interface.
Examples	<pre>sonic# configure terminal sonic(config)# interface Vlan 10 sonic(config-if-vlan-10)# mclag-peer-gateway</pre>
Releases	4.0 or later

mclag-separate-ip

Configures separate IPs on a VLAN interface for L3 protocol support over MCLAG.

Command	<code>mclag-separate-ip</code>
Options	None

Modes	INTERFACE
Usage	Use this command to configure separate IPs (unique IPs) on the VLAN interface in both MCLAG peers for L3 protocol support. Also, when using EVPN/VXLAN with pip (primary-ip), this command must be configured on L3 VNI VLAN on the MCLAG peers. This command is applicable only on a VLAN interface.
Examples	<pre>sonic(config)# interface Vlan 10 sonic(config-if-Vlan10)# mclag-separate-ip</pre> <pre>sonic(config-if-Vlan10)# no mclag-separate-ip</pre>
Releases	3.2 or later

mclag-system-mac

Sets the MCLAG system MAC address.

Command	<code>mclag-system-mac mac-addr</code>
Options	<code>mac-addr</code> —MCLAG domain ID in nn:nn:nn:nn:nn:nn format
Modes	MCLAG
Usage	Use this command to set the MCLAG system MAC address to be used for the MCLAG interface.
Examples	<pre>sonic(config-mclag-domain-100)# mclag-system-mac 00:bb:bb:bb:cc:cc</pre> <pre>sonic(config-mclag-domain-100)# no mclag-system-mac</pre>
Releases	3.1 or later

meter-type

This command configures the meter-type for a scheduler policy queue.

Command	<code>meter-type {packets bytes}</code>
Options	<ul style="list-style-type: none"> • <code>packets</code>—Set meter-type to packets per second • <code>bytes</code>— Set meter-type to kilobytes per second
Modes	QOS SCHEDULER-POLICY
Usage	Use this command to set the meter type of the interface queue the scheduler policy is applied on. Meter-type must be set to bytes (kbps) for a policy that is applied on the physical interface and packets (pps) for a policy that is applied on CPU interface.
Examples	<pre>sonic(config)# qos scheduler-policy sched_pol sonic(config-sched-policy-sched_pol)# queue 0 sonic(config-scheduler-sched_pol-queue-0)# meter-type bytes</pre>
Releases	3.1.0 or later

minimum-ttl

Configures the minimum time to live (TTL) value expected in the incoming BFD control packet for a multihop peer.

Command	<code>minimum-ttl minimum-ttl-value</code>
----------------	--

Options	<i>minimum-ttl-value</i> — Minimum expected TTL value for incoming multihop BFD packets (1 to 254; default is 254)
Modes	<ul style="list-style-type: none"> • PEER • BFD PROFILE
Usage	This configuration is valid for multihop peers only.
Examples	<p>Example for PEER mode:</p> <pre>device# configure terminal device(config)# bfd device(config-bfd)# peer 192.168.0.5 interface Ethernet0 device(config-bfd-peer)# minimum-ttl 250</pre> <p>Example for PROFILE mode:</p> <pre>device# configure terminal device(config)# bfd device(config-bfd)# profile fast device(config-bfd-profile)# minimum-ttl 250</pre> <pre>device# configure terminal device(config)# bfd device(config-bfd)# profile fast device(config-bfd-profile)# no minimum-ttl 250</pre>
Releases	4.0 or later

mirror

Add mirror to drop counter.

Command	<code>mirror <i>string</i></code>
Options	<i>string</i> —Name of the mirror session
Modes	DROPCOUNTERS
Usage	Use this command to add a counter to an existing mirror session.
Examples	<pre>sonic# configure terminal sonic(config)# dropcounters drop sonic(config-dropcounters-drop)# mirror any</pre>

Releases	4.0 or later
-----------------	--------------

mirror-session

Configures a mirror-session.

Command	<code>mirror-session <i>session-name</i></code>
Options	<i>session-name</i> —Name of the mirror session (up to 24 characters)
Modes	CONFIGURATION
Usage	Use this command to configure a mirror session for mirroring packets.

Examples

```
sonic(config) # mirror-session sess10  
sonic(config) # no mirror-session
```

Releases

3.0 or later

mode

Configure the ARS path reassignment mode.

Command

```
mode {fixed | flowlet-quality | flowlet-random | packet-quality | packet-random}
```

Options

- *fixed*—Fixed path assignment.
- *flowlet-quality*—Per flowlet quality-based path reassignment. This is the default setting.
- *flowlet-random*—Per flowlet random path reassignment. This option is not supported on the Z9664F-ON platform.
- *packet quality*—Per packet quality-based path reassignment.
- *packet random*—Per packet random path reassignment. This option is not allowed when the object is bound to a route-map. This option is not allowed when a nondefault value is present on the *max-flows* or *idle-time* commands.

Modes

ARS-OBJECT

Usage

Some ARS modes are not supported on specific platforms.

Example

```
sonic(config-ars-object) # mode flowlet-quality
```

Releases

4.4.0 or later

monitoring-fbs

Configures key-profile for monitoring flow-based-services.

Command

```
monitoring-fbs {egress | ingress} key-profile {ip | ipv4 | ipv6 | l2 | l2-ipv4}
```

Options

- *egress*—egress direction
- *ingress*—ingress direction
- *ip*—IPv4 and IPv6 key-profile
- *ipv4*—IPv4 key-profile
- *ipv6*—IPv6 key-profile
- *l2*—L2 key-profile
- *l2-ipv4*—L2 and IPv4 key-profile

Modes

TCAM

Usage

Use this command to set the hardware TCAM key-profiles for monitoring flow-based service policies.

Examples

```
sonic# configure terminal  
sonic(config)# hardware  
sonic(config-hardware)# tcam  
sonic(config-hardware-tcam)# monitoring-fbs ingress key-profile ip
```

Releases

4.0 or later

mtu

Configures maximum transmission unit (MTU) frame size for IP traffic on an interface.

Command `mtu mtu`

Options `mtu` — Maximum frame size in bytes (1312 to 9216; default 9100)

Modes INTERFACE

Usage Use this command to configure IP MTU on a physical, VLAN, PortChannel, or Management interface.

Examples

```
sonic(config-if-Ethernet28)# mtu 2000
```

```
sonic(config-if-Ethernet28)# no mtu
```

Releases 3.0 or later

N, O, and P commands

Topics:

- name
- nat
- nat-zone
- neigh-holdtime
- neigh-suppress
- neighbor
- network
- network import-check
- network prefix
- network-policy
- network-policy
- next-hop-self
- no crm all
- ntp authenticate
- ntp authentication-key
- ntp server
- ntp source-interface
- ntp trusted-key
- ntp vrf
- ospf abr-type
- ospf router-id
- override-capability
- passive
- passive-interface
- passive-interface (for OSPFv2)
- passive-mode
- password
- pbf next-hop-group
- pbf replication-group
- pbs
- peer
- peer-group
- peer-ip
- peer-link
- pfc-priority
- pfc-priority pg
- ping
- ping vrf
- ping vrf mgmt
- ping6
- ping6 vrf
- ping6 vrf mgmt
- pir
- poe detection
- poe disable
- poe power management
- poe priority

- poe reset
- police
- police
- policy-map
- pool
- port
- port
- port-group
- portchannel graceful-shutdown
- port-load-current
- port-load-exponent
- port-load-future
- port-load-future-weight
- port-load-past
- port-load-past-weight
- port-security enable
- port-security maximum
- port-security violation
- preempt
- prefix-list
- primary-ip
- priority
- priority-flow-control
- priority-flow-control watchdog action
- priority-flow-control watchdog counter-poll
- priority-flow-control watchdog off
- priority-flow-control watchdog on
- priority-flow-control watchdog polling-interval
- priority-flow-control watchdog restore-time
- profile

name

Configures region name for the MST.

Command	<code>name <i>mst-name</i></code>
Options	<code><i>mst-name</i></code> — Enter a name for up to 32 characters. You can enter a null string by entering inverted commas.
Modes	SPANNING-TREE MST
Usage	The default name set is the system MAC address. Entering inverted commas ("") enters a null string as the name.
Examples	<pre>sonic(config)# spanning-tree mst configuration sonic(config-mst)# name mst1</pre> <pre>sonic(config)# spanning-tree mst configuration sonic(config-mst)# name ""</pre> <pre>sonic(config)# no name</pre>
Releases	4.0 or later

nat

Enters network address translation (NAT) configuration mode.

Command

nat

Options

None

Modes

CONFIGURATION

Usage

Use this command to enter NAT configuration mode to configure static or dynamic NAT.

Example

```
sonic(config)# nat  
sonic(config-nat)#
```

Releases

3.0 or later

nat-zone

Configures a NAT zone on a physical, Loopback, PortChannel, or VLAN interface.

Command

nat-zone *zone*

Options

zone — Zone number (0 to 3)

Modes

INTERFACE

Usage

Use this command to configure a NAT zone on Layer 3 (L3) interfaces so that NAT address translation is performed on packets when a packet transverses a zone on a configured interface.

Examples

```
sonic(config-if-Ethernet4)# ip address 20.20.20.20/24  
sonic(config-if-Ethernet4)# nat-zone 1  
  
sonic(config-if-lo1)# ip address 10.10.10.10/32  
sonic(config-if-lo1)# nat-zone 2  
  
sonic(config-if-po2)# ip address 25.25.25.25/24  
sonic(config-if-po2)# nat-zone 1  
  
sonic(config-if-Vlan5)# ip address 23.23.23.23/24  
sonic(config-if-Vlan5)# nat-zone 1  
  
sonic(config-if-Vlan5)# no nat-zone
```

Releases

3.0 or later

neigh-holdtime

Configures the hold time used to wait before aging out ARP/ND entries that are learned from multihomed peer VTEPs and that have not been used.

Command

neigh-holdtime *seconds*

Options

seconds — Hold time in seconds (0-86400; default 1080).

Modes

EVPN-ESI-MULTIHOMING

Usage

When an ARP entry is deleted from the multihomed VTEP on which it is learned, the timer is restarted on the remote multihomed VTEPs in the EVPN Ethernet segment, which continue to advertise the IP-MAC address association. To configure the hold-time used to wait before aging out the MAC addresses of

downstream devices that are learned from multihomed peer VTEPs and that have not been used, use the [mac-holdtime](#) command.

Examples

```
sonic(config) # evpn esi-multipathing  
sonic(config-evpn-esi-mh) # neigh-holdtime 2000
```

Releases

4.2.0 or later

neigh-suppress

Enables ARP and ND suppression on a VLAN interface.

Command

neigh-suppress

Options

None

Modes

INTERFACE

Usage

Use this command to enable neighbor suppression for ARP and IPv6 neighbor discovery packets. Enabling this command stops flooding of ARP and IPv6 neighbor discovery packets for known hosts and the switch would respond to those packets. ARP and IPv6 neighbor discovery packets to unknown hosts would be flooded. This command works only on VLAN interfaces configured with IP or IPv6 address, and the VLAN should be mapped to VNI.

Examples

```
sonic# configure terminal  
sonic(config) # interface Vlan 10  
sonic(config-if-vlan10) # neigh-suppress
```

```
sonic(config-if-Vlan10) # no neigh-suppress
```

Releases

3.0 or later

neighbor

Creates a remote IP or unnumbered peer, and enters into neighbor configuration mode.

Command

neighbor {ip | {interface {Ethernet | PortChannel | Vlan}}}

Options

- *ip* — IPv4 or IPv6 address of the neighbor in A.B.C.D or A::B format
- *interface* — Ethernet, PortChannel, or VLAN interface that connects to an unnumbered neighbor

Modes

BGP-NEIGHBOR

Usage

Use this command to create an IPv4 or IPv6 BGP neighbor. Enter the neighbor's IPv4 or IPv6 address directly, or you can optional enter an interface name for an unnumbered BGP neighbor.

Examples

```
sonic(config-router-bgp) # neighbor 30.30.30.3  
sonic(config-router-bgp-neighbor) #
```

```
sonic(config-router-bgp) # no neighbor 30.30.30.3
```

Releases

3.0 or later

network

Configures networks in an area.

Command

network ipaddrmask {area areaid}

Options	<ul style="list-style-type: none"> • <i>ipaddrmask</i> — IPv4 or IPv6 address in A.B.C.D/mask or A::B/mask format • <i>areaid</i> — Area ID in A.B.C.D or 0..4294967295 format
Modes	ROUTER-OSPF
Usage	<p>Use this command to configure or associate network addresses into specific areas. Interfaces belonging to these network addresses are considered as part of the area specified. This command is mutually exclusive with area within a VRF. When this command is used in a VRF, area cannot be used.</p>
Examples	<pre>sonic(config-router-ospf) # network 10.1.1.0/24 area 0</pre> <pre>sonic(config-router-ospf) # network 19.1.1.0/16 area 19</pre> <pre>sonic(config-router-ospf) # no network 19.1.1.0/16 area 19</pre>
Releases	3.0 or later

network import-check

Configure BGP to check if a BGP network route exists in the local route table before advertising the network.

Command	network import-check
Options	None
Modes	ROUTER-BGP
Usage	<p>By default, BGP networks are advertised to neighbors irrespective of if the same route exists in local route table or not. This behavior may lead to a data traffic void. Use this command to place a restriction on BGP networks to get advertised only if a corresponding route from an internal gateway protocol (iGP) exists in local route table.</p>
Examples	<pre>sonic(config-router-bgp) # network import-check</pre> <pre>sonic(config-router-bgp) # no network import-check</pre>
Releases	3.0 or later

network prefix

Configures a network as local to this AS and adds it to the BGP routing table.

Command	network prefix {[backdoor] {[route-map <i>route-map-name</i>]}}
Options	<ul style="list-style-type: none"> • <i>prefix</i>—IPv4 or IPv6 address and prefix number to the network in A.B.C.D/mask or A::B/mask format • <i>backdoor</i>—(Optional) Backdoor route-map • <i>route-map <i>route-map-name</i></i>—(Optional) Name of the established route-map
Modes	BGP-ADDRESS-FAMILY
Usage	<p>Use this command to enable routing of an IPv4 or IPv6 network to announce using BGP. This command can be used to statically inject routes into BGP. Use route-map to modify or set the various attributes of the route.</p>
Examples	<pre>sonic(config-router-bgp-af) # network 10.10.0.0/16</pre> <pre>sonic(config-router-bgp-af) # no network 10.10.0.0/16</pre>

Releases	3.0 or later
-----------------	--------------

network-policy

Configures a network policy profile.

Command	network-policy profile <i>np_num</i>
Options	<i>np_num</i> —Enter the network policy number (1 to 128)
Modes	CONFIGURATION
Usage	Use this command to configure a network policy profile for setting LLDP-MED parameters.
Examples	<pre>sonic(config) # network-policy profile 1</pre> <pre>sonic(config) # no network-policy profile 1</pre>

Releases	4.0 or later
-----------------	--------------

network-policy

Configures a network policy profile.

Command	network-policy profile <i>np_num</i>
Options	<i>np_num</i> —Enter the network policy number (1 to 128)
Modes	INTERFACE
Usage	Use this command to configure a network policy profile for setting LLDP-MED parameters.
Examples	<pre>sonic(config) # interface Eth1</pre> <pre>sonic(config-if-Eth1) # network-policy 1</pre> <pre>sonic(config) # no network-policy 1</pre>

Releases	4.0 or later
-----------------	--------------

next-hop-self

Disables the next-hop calculation for a BGP neighbor, or neighbors in a peer-group.

Command	next-hop-self [force]
Options	force — (Optional) Forces the next-hop attribute
Modes	<ul style="list-style-type: none">NEIGHBOR-ADDRESS-FAMILYPEER-GROUP-ADDRESS-FAMILY
Usage	Use this command to disable BGP next-hop attribute computation and override the next-hop by the sender's address. This command influences next-hop processing of eBGP routes to iBGP peers.
Examples	<pre>sonic(config) # router bgp 100</pre> <pre>sonic(config-router-bgp) # neighbor 20.20.20.2</pre> <pre>sonic(config-router-bgp-neighbor) # remote-as 300</pre>

```

sonic(config-router-bgp-neighbor) # address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af) # next-hop-self

sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # next-hop-self

sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family 12vpn evpn
sonic(config-router-bgp-neighbor-af) # next-hop-self

sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # address-family 12vpn evpn
sonic(config-router-bgp-pg-af) # next-hop-self

sonic(config-router-bgp-neighbor-af) # no next-hop-self
sonic(config-router-bgp-pg-af) # no next-hop-self

```

Releases 3.0 or later

no crm all

Removes all CRM monitoring configurations on the switch and restores the default values.

Command	no crm all
Options	None
Modes	CONFIGURATION
Usage	The default settings for CRM monitoring are: <ul style="list-style-type: none"> • Polling interval: 5 minutes • High threshold: 85% • Low threshold: 70%
Examples	<pre>sonic(config) # no crm all</pre>

Releases 4.2.1 or later

ntp authenticate

Enables NTP authentication.

Command	ntp authenticate
Options	None
Modes	CONFIGURATION
Usage	By default, NTP authentication is disabled.
Examples	<pre>sonic(config) # ntp authenticate</pre> <pre>sonic(config) # no ntp authenticate</pre>

Releases 3.1 or later

ntp authentication-key

Configures an NTP authentication key.

Command ntp authentication-key *key-number* { auth-type { key [encrypted] } }

Options

- *key-number*—Enter the key number
- *auth-type*—Enter the authentication type; select md5, sha1, or sha2-256
- *key*—Enter the authentication key word
- *encrypted*—(Optional) Encrypts the authentication key

Modes

CONFIGURATION

Usage

Use this command to configure an NTP authentication key.

Examples

```
sonic(config)# ntp authentication-key 128 md5 Dell2020
```

```
sonic(config)# ntp authentication-key 128 md5 dryjsgjd123 encrypted
```

```
sonic(config)# no ntp authentication-key 128
```

Releases

3.1 or later

ntp server

Configures an NTP server from which the switch synchronizes its time.

Command ntp server {*ipv4-address* | *ipv6-address* | *ntp-server-name*} [*prefer {true | false}*] [*key key-number*] [*minpoll min-poll*] [*maxpoll max-pol1*]

Options

- *ipv4-address* — IPv4 address in A.B.C.D format
- *ipv6-address* — IPv6 address in A::B format
- *ntp-server-name* — NTP server name (up to 64 characters)
- *prefer {true | false}* — Enable or disable server as the preferred NTP server.
- *key-number* — (Optional) Authentication key ID to authenticate the NTP server that serves as the time source (1 to 65535)
- *min-poll* — Minimum amount of time to poll the server in seconds
- *max-poll* — Maximum amount of time to poll the server in seconds

Modes

CONFIGURATION

Usage

Use this command to configure an NTP server for time synchronization. Use the `ntp vrf` command to specify the VRF in which NTP is enabled.

Examples

```
sonic(config)# ntp server 10.11.0.1 key 128
sonic(config)# ntp server pool.ntp.org
```

```
sonic(config)# no ntp server 10.11.0.1
```

Add NTP server as preferred server:

```
sonic(config)# ntp server 99.1.1.1 prefer true
```

Remove preferred NTP server configuration:

```
sonic(config)# ntp server 99.1.1.1 prefer false
```

Releases

3.2 or later

ntp source-interface

Configures the switch interface whose IPv4 or IPv6 address is used as the source address in packets sent to the NTP server.

Command ntp source-interface {Ethernet | Loopback | Management | PortChannel | Vlan}

- Options**
- Ethernet — Ethernet interface
 - Loopback — Loopback interface
 - Management — Management interface
 - PortChannel — PortChannel interface
 - Vlan — VLAN interface

Modes CONFIGURATION

Usage You can configure multiple global NTP source interfaces. By default, a single NTP source interface is selected using an internal NTP source interface selection algorithm.

Examples

```
sonic(config)# ntp source-interface Ethernet 8  
  
sonic(config)# ntp source-interface Management 0  
  
sonic(config)# ntp source-interface Loopback 88  
  
sonic(config)# ntp source-interface PortChannel 18  
  
sonic(config)# ntp source-interface Vlan 888  
  
sonic(config)# no ntp source-interface
```

Releases 3.1 or later

ntp trusted-key

Configures an NTP authentication key number for a trusted time source.

Command ntp trusted-key *key-number*

Options *key-number*—Enter the key number (1 to 65535)

Modes CONFIGURATION

Usage Use this command to configure the trusted authentication key numbers that the switch must receive in NTP packets in order to accept the NTP server time. Trusted keys identify trusted sources—the NTP servers from which the switch accepts time synchronization.

Examples

```
sonic(config)# ntp trusted-key 128  
  
sonic(config)# no ntp trusted-key 128
```

Releases 3.1 or later

ntp vrf

Configures an NTP server to operate in the Management, default, or a user-defined VRF.

Command ntp vrf {mgmt | default | *vrf-name*}

Options	<ul style="list-style-type: none"> ● <code>mgmt</code> — Enable NTP in the Management VRF. ● <code>default</code> — Enable NTP in the default VRF. ● <code>vrf-name</code> — Enable NTP in a user-defined VRF.
Modes	CONFIGURATION
Usage	<p>By default, the NTP is enabled in a VRF:</p> <ul style="list-style-type: none"> ● If no NTP VRF is configured: <ul style="list-style-type: none"> ○ If the Management VRF is not configured, NTP is enabled in the default VRF. ○ If the Management VRF is configured, NTP is enabled in the Management VRF. ● If the Management VRF is configured and the Management VRF is configured as the NTP VRF: <ul style="list-style-type: none"> ○ NTP is enabled in the Management VRF. ● If the default VRF is configured as the NTP VRF: <ul style="list-style-type: none"> ○ NTP is enabled in the default VRF, regardless of whether the Management VRF is configured or not. ● If a user-defined VRF is configured as the NTP VRF: <ul style="list-style-type: none"> ○ NTP is enabled in the user-defined VRF.
Examples	<pre>sonic(config) # ntp vrf mgmt</pre> <pre>sonic(config) # ntp vrf default</pre> <pre>sonic(config) # no ntp vrf</pre>
Releases	3.1 or later

ospf abr-type

Configures the OSPFv2 router ABR type.

Command	<code>ospf abr-type {cisco ibm shortcut standard}</code>
Options	None
Command mode	ROUTER-OSPF
Usage	Use this command to configure the ABR type such as <code>cisco</code> , <code>ibm</code> , <code>shortcut</code> , or <code>standard</code> .
Examples	<pre>sonic(config) # router ospf</pre> <pre>sonic(config-router-ospf) # ospf abr-type shortcut</pre> <pre>sonic(config-router-ospf) # ospf abr-type cisco</pre> <pre>sonic(config-router-ospf) # no ospf abr-type</pre>
Releases	3.1 or later

ospf router-id

Configures the OSPFv2 router ID.

Command	<code>ospf router-id <i>routerid</i></code>
Options	<code>routerid</code> — Router ID in A.B.C.D format
Command mode	ROUTER-OSPF
Usage	Use the command to configure the default router ID. If the router ID is not present at startup or new configuration, the highest IPv4 address is considered the router ID. When configuring a specific router ID,

the newly configured router ID is used. The same router ID is used until a new router ID is configured, a router ID is unconfigured, or a system restart.

Examples

```
sonic(config-router-ospf) # ospf router-id 19.1.1.1
```

```
sonic(config-router-ospf) # no ospf router-id
```

Releases

3.1 or later

override-capability

Configures BGP to override the result of capability negotiation with local configuration, and ignore the remote peer's capability value.

Command `override-capability`**Options** None**Modes**

- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage

Use this command to ignore the negotiated capability parameters with a BGP neighbor or neighbors in a peer-group, and instead use the locally configured parameters.

Examples

```
sonic(config-router-bgp) # neighbor 30.30.30.3
sonic(config-router-bgp-neighbor) # override-capability
```

```
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # override-capability
```

```
sonic(config-router-bgp-neighbor) # no override-capability
sonic(config-router-bgp-pg) # no override-capability
```

Releases

3.0 or later

passive

Configures a BGP neighbor as passive.

Command `passive`**Options** None**Modes**

- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage

Use this command to configure a BGP neighbor or neighbor in a peer-group as passive. BGP neighbors will not initiate a session, and will listen to any incoming BGP session.

Examples

```
sonic(config-router-bgp) # neighbor 30.30.30.3
sonic(config-router-bgp-neighbor) # passive
```

```
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # passive
```

```
sonic(config-router-bgp-neighbor) # no passive
sonic(config-router-bgp-pg) # no passive
```

Releases

3.0 or later

passive-interface

Suppresses routing updates on an interface.

Command	passive-interface {default Ethslot/port [ipaddr]}
Options	<ul style="list-style-type: none">• default — Set all interfaces as passive interfaces by default.• Ethslot/port — Enter an Ethernet interface name.• ipaddr — (Optional) Enter an IP address in A.B.C.D format.
Modes	ROUTER-OSPF
Usage	Use this command to configure OSPFv2 passive interfaces. Specify default to configure all interfaces as passive interfaces. Use the no passive-interface command to reactivate all interfaces or a specified interface.
Examples	<pre>sonic(config-router-ospf)# passive-interface default</pre> <pre>sonic(config-router-ospf)# no passive-interface Eth1/16</pre>
Releases	3.1 or later

passive-interface (for OSPFv2)

Configures OSPFv2 passive interfaces.

Command	passive-interface {default Ethslot/port Loopback loopback-id PortChannel port-channel-id Vlan vlan-id} [ip-address]
Options	<ul style="list-style-type: none">• Ethslot/port — Ethernet interface• loopback-id — Loopback ID• port-channel-id — Port channel name• vlan-id — VLAN ID• ip-address — IP address in A.B.C.D format
Modes	ROUTER OSPF
Usage	By default, all OSPFv2 interfaces are active. To configure all OSPFv2 interfaces as passive interfaces, enter the passive-interface default command. To reactivate specified OSPFv2 interfaces, use the no passive-interface command.
Examples	<pre>sonic-cli(config-router-ospf)# passive-interface default</pre> <pre>sonic-cli(config-router-ospf)# no passive-interface Ethernet0</pre>
Releases	4.0 or later

passive-mode

Configures a BFD peer as passive, where the session creation is not initiated by this peer.

Command	passive-mode
Options	None
Modes	<ul style="list-style-type: none">• PEER• BFD PROFILE
Usage	Peer enabled with passive mode does not initiate session creation but responds to session creation requests. By default, Passive mode is disabled for a BFD peer.

Examples

Example for PEER mode:

```
device()#configure terminal  
device(config)#bfd  
device(config-bfd)# peer 192.168.0.5 interface Ethernet0  
device(config-bfd-peer)# passive-mode
```

```
device()#configure terminal  
device(config)#bfd  
device(config-bfd)# peer 192.168.0.5 interface Ethernet0  
device(config-bfd-peer)# no passive-mode
```

Example for PROFILE mode:

```
device()#configure terminal  
device(config)#bfd  
device(config-bfd)# profile fast  
device(config-bfd-profile)# passive-mode
```

```
device()#configure terminal  
device(config)#bfd  
device(config-bfd)# profile fast  
device(config-bfd-profile)# no passive-mode
```

Releases

4.0 or later

password

Configures a password for message digest 5 (MD5) authentication on the TCP connection between two neighbors.

Command

```
password string [encrypted]
```

Options

- *string* — MD5 password (16-byte)
- *encrypted* — (Optional) Indicates if the password should be encrypted

Modes

- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage

Use this command to configure an MD5 password to be used with the TCP socket connection to the remote peer. This command is for security purposes. When a password is configured for a BGP neighbor or peer-group, the sender will include a 16-byte MD5 digest in the TCP header of BGP message. The receiver validates the digest before accepting the BGP message.

Examples

```
sonic(config-router-bgp)# neighbor 30.30.30.3  
sonic(config-router-bgp-neighbor)# password jackandjillwentupthehill
```

```
sonic(config-router-bgp)# peer-group PG_Ext  
sonic(config-router-bgp-pg)# password ilovebeansbecausetheyaremean
```

```
sonic(config-router-bgp-neighbor)# no password  
sonic(config-router-bgp-pg)# no password
```

Releases

3.0 or later

pbf next-hop-group

Creates a policy-based forwarding next-hop group.

Command

```
pbf next-hop-group fbs-nhgrp-name [type {ip | ipv6}]
```

Options	<i>fbs-nhgrp-name</i> —Next-hop group name (up to 63 characters)
Modes	CONFIGURATION
Usage	The group name must begin with A-Z, a-z, or 0-9. Underscore and hyphens can be used except as the first character. A next-hop-group can be ip or ipv6. The group type cannot be updated after it is created. The group type is mandatory at the time of creating the group.
Examples	<pre>sonic(config) # pbf next-hop-group ipv4-group-1 type ip sonic(config-pbf-ip-nh-group) #</pre>
Releases	3.2 or later

pbf replication-group

Configures policy-based forwarding (PBF) replication group.

Command	<code>pbf replication-group <i>fbs-replgrp-name</i> [type {ip ipv6}]</code>
Options	<i>fbs-replgrp-name</i> — Name of the replication group (up to 63 characters)
Modes	CONFIGURATION
Usage	The group name must begin with A-Z, a-z, or 0 to 9. Underscore and hyphens can be used except as the first character. A next-hop-group can be IP or IPv6. The group type cannot be updated after it is created. The group type is mandatory at the time of creating the group.
Examples	<pre>sonic# configure terminal sonic(config)# pbf replication-group group1 type ip sonic(config-pbf-ip-repl-group) #</pre>
Releases	4.0 or later

pbs

Sets the peak burst size (PBS) in bytes.

Command	<code>pbs <i>pbs-value</i></code>
Options	<i>pbs-value</i> —250-125000000 bytes for physical interface queues, and 0-100000 packets for CPU interface queues
Modes	SCHEDULER-POLICY-QUEUE
Usage	Use this command to set the peak burst size for a queue in a scheduler policy.
Examples	<pre>sonic(config) # qos scheduler-policy policy1 sonic(config-sched-policy) # queue 1 sonic(config-sched-policy-queue-q1) # pbs 250</pre>
Releases	3.1 or later

peer

Configures an IPv4 or IPv6 single-hop or multi-hop bidirectional forwarding detection (BFD) peer.

Command	<code>peer {<i>peer_ipv4</i> <i>peer_ipv6</i>} [<i>vrf</i>] <i>vrfname</i> [<i>multihop</i>] [<i>local-address</i>] {<i>local_ipv4</i> <i>local_ipv6</i>} [<i>interface</i>] <i>interfacename</i></code>
Options	<ul style="list-style-type: none"> • <i>peer_ipv4</i> — Peer IPv4 address in A.B.C.D format • <i>peer_ipv6</i> — Peer IPv6 address in A::B format

- *vrfname* — VRF instance name
- *local_ipv4* — Local IPv4 address in A.B.C.D format
- *local_ipv6* — Local IPv6 address in A::B format
- *interfacename* — Interface name

Modes

CONFIGURATION-BFD

Usage

Use this command to configure an IPv4 or IPv6 single-hop and multi-hop bidirectional forwarding detection (BFD) peer. A single-hop BFD peer interface must be configured, and for a multi-hop BFD peer a local address must be configured.

Examples

```
sonic(config)# bfd
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0

sonic(config)# bfd
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0 vrf Vrf1

sonic(config)# bfd
sonic(config-bfd)# peer 192.168.0.2 multihop local-address 192.168.0.3

sonic(config)# bfd
sonic(config-bfd)# peer 192.168.0.2 multihop local-address 192.168.0.3 vrf Vrf1

sonic(config-bfd)# no peer 192.168.0.5 interface Ethernet0
sonic(config-bfd)# no peer 192.168.0.5 interface Ethernet0 vrf Vrf1
sonic(config-bfd)# no peer 192.168.0.2 multihop local-address 192.168.0.3
sonic(config-bfd)# no peer 192.168.0.2 multihop local-address 192.168.0.3 vrf Vrf1
```

Releases

3.0 or later

peer-group

Creates a BGP peer-group, and assigns a BGP neighbor to a peer-group.

Command

`peer-group template-str`

Options

template-str—Peer group name

Modes

- ROUTER-BGP
- BGP-NEIGHBOR

Usage

Use this command to configure a peer-group and assign a peer-group to a BGP neighbor. Peer-groups help to increase scaling by supplying the same update information to all peers. In addition, the peer-group template makes it easier to configure settings for many BGP neighbors.

Examples

```
sonic(config)# router bgp 65300
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-# pg)

sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# peer-group PG_Ext

sonic(config-router-bgp)# no peer-group PG_Ext
sonic(config-router-bgp-neighbor)# no peer-group PG_Ext
```

Releases

3.0 or later

peer-ip

Configures an MCLAG peer IPv4 address.

Command	<code>peer-ip <i>address</i></code>
Options	<i>address</i> —Enter the peer IPv4 address in A.B.C.D format
Modes	MCLAG-DOMAIN
Usage	Use this command to configure the IP address on the peer-switch to which the MCLAG keepalive link has to be formed.
Examples	<pre>sonic# configure terminal sonic(config)# mclag domain 10 sonic(config-mclag-domain-10)# peer-ip 10.10.1.100 sonic(config-mclag)# no peer-ip</pre>
Releases	3.0 or later

peer-link

Configures an MCLAG peer on an Ethernet or PortChannel interface.

Command	<code>peer-link {<i>eth-if</i> <i>po-if</i>}</code>
Options	<ul style="list-style-type: none">• <i>eth-if</i>—Enter the Ethernet peer interface link• <i>po-if</i>—Enter the PortChannel peer interface link
Modes	MCLAG-DOMAIN
Usage	Use this command to configure or change an MCLAG session peer link. The peer-link can be configured only on Ethernet and PortChannel interfaces.
Examples	<pre>sonic# configure terminal sonic(config)# mclag domain 100 sonic(config-mclag-domain-100)# peer-link PortChannel 100 sonic(config-mclag-domain-100)# no peer-link</pre>
Releases	3.0 or later

pfc-priority

Adds PFC priority to a queue entry in the map.

Command	<code>pfc-priority dot1p {queue <i>qid</i>}</code>
Options	<ul style="list-style-type: none">• <i>dot1p</i>—Enter the dot1p priority.• <i>queue qid</i>—Enter the queue ID.
Modes	QOS-MAP
Usage	Use this command to associate a set of priority flow control (PFC) priorities to queues.
Examples	<pre>sonic# configure terminal sonic(config)# qos map pfc-priority-queue pfc-priority-queue-name</pre>

```
sonic(config-pfc-priority-queue-map-pfc-priority-queue-name)# pfc-
priority 1 queue 4

sonic(config)# no dot1p 1
```

Releases	3.1 or later
-----------------	--------------

pfc-priority pg

Configures a PFC priority-to-priority group entry in a QoS pfc-priority-to-pg map.

Command	<code>pfc-priority dot1p-value pg pg-value</code>
Options	<ul style="list-style-type: none"><code>dot1p-value</code> — Enter a dot1p priority value (0-7).<code>pg-value</code> — Enter a priority group value (0-7).
Modes	PFC-priority-pg-map
Usage	To configure a PFC priority-to-priority group mapping on switch interfaces, use the qos-map pfc-priority-pg command.

Examples	<pre>sonic(config)# qos-map pfc-priority-pg pfc-pg-remap sonic(config-pfc-priority-pg-map-pfc-pg-remap)# pfc-priority 0 pg 0 sonic(config-pfc-priority-pg-map-pfc-pg-remap)# no pfc-priority 0</pre>
-----------------	---

Releases	4.2.1 or later
-----------------	----------------

ping

Tests network connectivity to an IPv4 device.

Command	<code>ping [vrf {mgmt vrf-name}] [-LRUbdfnqrVAB] [-c count] [-i interval] [-I interface] [-M pmtdisc_option] [-l preload] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline] [-W timeout] [hop1 hop2 ...] destination-address</code>
Options	<ul style="list-style-type: none"><code>vrf {mgmt vrf-name}</code> — (Optional) Pings an IPv4/IPv6 address in the management or a specified VRF instance.<code>-a</code> — (Optional) Audible ping.<code>-A</code> — (Optional) Adaptive ping. An inter-packet interval adapts to the round-trip time so that one (or more, if you set the <i>preload</i> option) unanswered probe is present in the network. The minimum interval is 200 milliseconds for a non-super user, which corresponds to Flood mode on a network with a low round-trip time.<code>-b</code> — (Optional) Pings a broadcast address.<code>-B</code> — (Optional) Does not allow ping to change the source address of probes. The source address is bound to the address used when the ping starts.<code>-c count</code> — (Optional) Stops the ping after sending the specified number of ECHO_REQUEST packets until the timeout expires.<code>-d</code> — (Optional) Sets the SO_DEBUG option on the socket being used.<code>-D</code> — (Optional) Prints the timestamp before each line.<code>-f</code> — (Optional) Flood ping. For every ECHO_REQUEST sent, a period "." is printed. For every ECHO_REPLY received, a backspace is printed to provide a rapid display of how many packets are dropped.<code>-F flow-label</code> — (Optional - for ping6 only) Allocates and sets a 20-bit flow label on echo request packets. If the <i>flow-label</i> value is zero, the kernel allocates a random flow label.

- **-i interval** — (Optional) Enter the interval in seconds to wait between sending each packet, from 0 to 60; the default is 1 second.
- **-I interface** — (Optional) Enter the source interface *interface-type interface-number* without spaces or the interface IPv4/IPv6 address.
 - For a physical Ethernet interface, enter `Ethernetport-number`; for example, `Ethernet1`.
 - For a port-channel interface, enter `PortChannelportchannel-number`; for example, `PortChannel1`.
 - For a VLAN interface, enter `Vlanvlan-id`; for example, `Vlan10`.
 - For a Loopback interface, enter `Loopbacknumber`; for example, `Loopback0`.
 - For the Management interface, enter `Management0`.
- **-l preload** — (Optional) Enter the number of packets that ping sends before waiting for a reply. Only a super user can pre-load more than three.
- **-L** — (Optional) Suppress the loopback of multicast packets for a multicast target address.
- **-m mark** — (Optional) Tags the packets sent to ping a remote device. Use this option with policy routing.
- **-M pmtudisc_option** — (Optional) Enter the path MTU (PMTU) discovery strategy:
 - do prevents fragmentation, including local.
 - want performs PMTU discovery and fragments large packets locally.
 - dont does not set the Don't Fragment (DF) flag.
- **-p pattern** — (Optional) Enter a maximum of 16 pad bytes to fill out the packet you send to diagnose data-related problems in the network; for example, `-p ff` fills the sent packet with all 1's.
- **-Q tos** — (Optional) Enter a maximum of 1500 bytes in decimal or hexadecimal datagrams to set QoS-related bits.
- **-s packetsize** — (Optional) Enter the number of data bytes to send, from 1 to 65468, default 56.
- **-S sndbuf** — (Optional) Sets the sndbuf socket. By default, the sndbuf socket buffers one packet maximum.
- **-t ttl** — (Optional) Enter the IPv4/IPv6 time-to-live (TTL) value in seconds.
- **-T timestamp option** — (Optional) Set special IP timestamp options. Valid values for the *timestamp option* are `tsonly` (only timestamps), `tsandaddr` (timestamps and addresses), or `tsprespec host1 [host2 [host3 [host4]]]` (timestamp pre-specified IPv4/IPv6 hops).
- **-v** — (Optional) Verbose output.
- **-V** — (Optional) Display the version and exit.
- **-w deadline** — (Optional) Enter the time-out value in seconds before the ping exits regardless of how many packets send or receive.
- **-W timeout** — (Optional) Enter the time to wait for a response in seconds. This setting affects the time-out only if there is no response, otherwise ping waits for two round-trip times (RTTs).
- **destination-address** — Enter the IPv4/IPv6 address of the remote device that you are trying to access.

Modes

Usage

The ping command uses an ICMP ECHO_REQUEST to receive an ICMP ECHO_RESPONSE from a network host or gateway. Each ping packet has an IPv4 and ICMP header, and a time value and a number of "pad" bytes used to fill out the packet. A ping operation sends a packet to a specified IP address and measures the time that it takes to get a response from the address or device. If the destination IP address is active, replies are sent back from the server including the IP address, number of bytes sent, lapse time in milliseconds, and TTL, which is the number of hops back from the source to the destination.

Example

```
sonic# ping 10.14.1.95 -c 5
PING 10.14.1.95 (10.14.1.95) 56(84) bytes of data.
64 bytes from 10.14.1.95: icmp_seq=1 ttl=61 time=4.43 ms
64 bytes from 10.14.1.95: icmp_seq=2 ttl=61 time=4.44 ms
64 bytes from 10.14.1.95: icmp_seq=3 ttl=61 time=4.37 ms
64 bytes from 10.14.1.95: icmp_seq=4 ttl=61 time=4.47 ms
64 bytes from 10.14.1.95: icmp_seq=5 ttl=61 time=4.31 ms

--- 10.14.1.95 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 4.310/4.408/4.475/0.093 ms
```

Releases	3.1 or later
-----------------	--------------

ping vrf

Tests network connectivity to a specific VRF.

Command ping vrf *vrf-name ip-address*

- Options**
- *vrf-name*—Enter the VRF name prefixed by Vrf (up to 15 characters)
 - *ip-address*—Enter the IP address to ping

Modes EXEC

Usage Use this command to test the network connectivity on the user-defined VRF.

Example

```
sonic# ping vrf Vrf-100 102.43.1.254
ping: Warning: source address might be selected on device other than Vrf-100.
PING 102.43.1.254 (102.43.1.254) from 102.43.1.254 Vrf-100: 56(84) bytes of data.
64 bytes from 102.43.1.254: icmp_seq=1 ttl=64 time=0.160 ms
64 bytes from 102.43.1.254: icmp_seq=2 ttl=64 time=0.103 ms
64 bytes from 102.43.1.254: icmp_seq=3 ttl=64 time=0.075 ms
64 bytes from 102.43.1.254: icmp_seq=4 ttl=64 time=0.096 ms
64 bytes from 102.43.1.254: icmp_seq=5 ttl=64 time=0.102 ms
64 bytes from 102.43.1.254: icmp_seq=6 ttl=64 time=0.072 ms
64 bytes from 102.43.1.254: icmp_seq=7 ttl=64 time=0.090 ms
64 bytes from 102.43.1.254: icmp_seq=8 ttl=64 time=0.103 ms
^C
--- 102.43.1.254 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7166ms
rtt min/avg/max/mdev = 0.072/0.100/0.160/0.025 ms
```

Releases	3.1 or later
-----------------	--------------

ping vrf mgmt

Tests network connectivity to the Management VRF.

Command ping vrf mgmt *ip-address*

- Options** *ip-address*—Enter the IP address to ping

Modes EXEC

Usage Use this command to test the network connectivity on the Management VRF.

Example

```
sonic# ping vrf mgmt 100.95.11.184
PING 100.95.11.184 (100.95.11.184) 56(84) bytes of data.
64 bytes from 100.95.11.184: icmp_seq=1 ttl=61 time=0.476 ms
64 bytes from 100.95.11.184: icmp_seq=2 ttl=61 time=0.260 ms
64 bytes from 100.95.11.184: icmp_seq=3 ttl=61 time=0.265 ms
64 bytes from 100.95.11.184: icmp_seq=4 ttl=61 time=0.262 ms
64 bytes from 100.95.11.184: icmp_seq=5 ttl=61 time=0.240 ms
^C
--- 100.95.11.184 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4091ms
rtt min/avg/max/mdev = 0.240/0.300/0.476/0.090 ms
```

Releases	3.1 or later
-----------------	--------------

ping6

Tests network connectivity to an IPv6 device.

Command

```
ping6 [vrf {mgmt | vrf-name}] [-LRUbdfnqrvVaAB] [-c count] [-i interval]
[-I interface] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
[-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
[-W timeout] [hop1 hop2 ...] destination-address
```

Options

- **vrf {mgmt | vrf-name}** — (Optional) Pings an IPv4/IPv6 address in the management or a specified VRF instance.
- **-a** — (Optional) Audible ping.
- **-A** — (Optional) Adaptive ping. An inter-packet interval adapts to the round-trip time so that one (or more, if you set the *preload* option) unanswered probe is present in the network. The minimum interval is 200 milliseconds for a non-super user, which corresponds to Flood mode on a network with a low round-trip time.
- **-b** — (Optional) Pings a broadcast address.
- **-B** — (Optional) Does not allow ping to change the source address of probes. The source address is bound to the address used when the ping starts.
- **-c count** — (Optional) Stops the ping after sending the specified number of ECHO_REQUEST packets until the timeout expires.
- **-d** — (Optional) Sets the SO_DEBUG option on the socket being used.
- **-D** — (Optional) Prints the timestamp before each line.
- **-f** — (Optional) Flood ping. For every ECHO_REQUEST sent, a period ":" is printed. For every ECHO_REPLY received, a backspace is printed to provide a rapid display of how many packets are dropped.
- **-F flow-label** — (Optional - for ping6 only) Allocates and sets a 20-bit flow label on echo request packets. If the *flow-label* value is zero, the kernel allocates a random flow label.
- **-i interval** — (Optional) Enter the interval in seconds to wait between sending each packet, from 0 to 60; the default is 1 second.
- **-I interface** — (Optional) Enter the source interface *interface-type interface-number* without spaces or the interface IPv4/IPv6 address.
 - For a physical Ethernet interface, enter *Ethernetport-number*; for example, *Ethernet1*.
 - For a port-channel interface, enter *PortChannelportchannel-number*; for example, *PortChannel1*.
 - For a VLAN interface, enter *Vlanvlan-id*; for example, *Vlan10*.
 - For a Loopback interface, enter *Loopbacknumber*; for example, *Loopback0*.
 - For the Management interface, enter *Management0*.
- **-l preload** — (Optional) Enter the number of packets that ping sends before waiting for a reply. Only a super user can pre-load more than three.
- **-L** — (Optional) Suppress the loopback of multicast packets for a multicast target address.
- **-m mark** — (Optional) Tags the packets sent to ping a remote device. Use this option with policy routing.
- **-M pmtudisc_option** — (Optional) Enter the path MTU (PMTU) discovery strategy:
 - do prevents fragmentation, including local.
 - want performs PMTU discovery and fragments large packets locally.
 - dont does not set the Don't Fragment (DF) flag.
- **-p pattern** — (Optional) Enter a maximum of 16 pad bytes to fill out the packet you send to diagnose data-related problems in the network; for example, **-p ff** fills the sent packet with all 1's.
- **-Q tos** — (Optional) Enter a maximum of 1500 bytes in decimal or hexadecimal datagrams to set QoS-related bits.
- **-s packetsize** — (Optional) Enter the number of data bytes to send, from 1 to 65468, default 56.
- **-S sndbuf** — (Optional) Sets the sndbuf socket. By default, the sndbuf socket buffers one packet maximum.
- **-t ttl** — (Optional) Enter the IPv4/IPv6 time-to-live (TTL) value in seconds.

- **-T timestamp option** — (Optional) Set special IP timestamp options. Valid values for the *timestamp option* are *tsonly* (only timestamps), *tsandaddr* (timestamps and addresses), or *tsprespec host1 [host2 [host3 [host4]]]* (timestamp pre-specified IPv4/IPv6 hops).
- **-v** — (Optional) Verbose output.
- **-V** — (Optional) Display the version and exit.
- **-w deadline** — (Optional) Enter the time-out value in seconds before the ping exits regardless of how many packets send or receive.
- **-W timeout** — (Optional) Enter the time to wait for a response in seconds. This setting affects the time-out only if there is no response, otherwise ping waits for two round-trip times (RTTs).
- **destination-address** — Enter the IPv4/IPv6 address of the remote device that you are trying to access.

Modes

EXEC

Usage

The `ping6` command uses an ICMP ECHO_REQUEST to receive an ICMP ECHO_RESPONSE from a network host or gateway. Each ping packet has an IPv6 and ICMP header, then a time value and a number of "pad" bytes used to fill out the packet. This operation sends a packet to a specified IPv6 address and then measures the time it takes to get a response from the address or device.

Example

```
sonic# ping6 20::1
PING 20::1(20::1) 56 data bytes
64 bytes from 20::1: icmp_seq=1 ttl=64 time=2.07 ms
64 bytes from 20::1: icmp_seq=2 ttl=64 time=2.21 ms
64 bytes from 20::1: icmp_seq=3 ttl=64 time=2.37 ms
64 bytes from 20::1: icmp_seq=4 ttl=64 time=2.10 ms
^C
--- 20::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.078/2.194/2.379/0.127 ms
```

Releases

3.1 or later

ping6 vrf

Tests network connectivity to a specific VRF.

Command

`ping6 vrf vrf-name ip-address`

Options

- *vrf-name*—Enter the VRF name prefixed by *Vrf* (up to 15 characters)
- *ip-address*—Enter the IPv6 address

Modes

EXEC

Usage

Use this command to test the network connectivity on the user-defined VRF.

Example

```
sonic(config)# ping6 vrf Vrf-100 101:12a:1:1::254
ping6: Warning: source address might be selected on device other than Vrf-100.
PING 101:12a:1:1::254(101:12a:1:1::254) from 101:12a:1:1::254 Vrf-100: 56 data bytes
64 bytes from 101:12a:1:1::254: icmp_seq=1 ttl=64 time=0.103 ms
64 bytes from 101:12a:1:1::254: icmp_seq=2 ttl=64 time=0.084 ms
64 bytes from 101:12a:1:1::254: icmp_seq=3 ttl=64 time=0.074 ms
^C
--- 101:12a:1:1::254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2041ms
rtt min/avg/max/mdev = 0.074/0.087/0.103/0.012 ms
```

Releases

3.1 or later

ping6 vrf mgmt

Tests network connectivity to a specific Management VRF.

Command

`ping6 vrf mgmt`

Options	None
Modes	EXEC
Usage	Use this command to test the network connectivity on the Management VRF.
Example	<pre>sonic# ping6 vrf mgmt</pre>
Releases	3.1 or later

pir

Configures the peak information rate in kbps.

Command	<code>pir <i>pir</i></code>
Options	<i>pir</i> —Enter the PIR rate in kbps.
Modes	CONFIGURATION
Usage	Use this command to set the peak information rate in kbps for physical interface queues and in pps for CPU interface queues.
Examples	<pre>sonic# configure terminal sonic(config)# qos scheduler-policy pol1 sonic(config-sched-policy-pol1)# queue 0 sonic(config-sched-policy-pol1-queue-0)# pir 10000</pre> <pre>sonic(config)# qos scheduler-policy pol2 sonic(config-sched-policy-pol2)# port sonic(config-sched-policy-pol2-port)# pir 10000</pre>
Releases	3.1 or later

poe detection

Configures PoE Detection mode for a port.

Command	<code>poe detection { dot3bt 2pt-dot3af 2pt-dot3af+legacy 4pt-dot3af 4pt-dot3af+legacy legacy dot3bt+legacy }</code>
Options	<ul style="list-style-type: none"> • <code>dot3bt</code>—Dot3bt detection • <code>2pt-dot3af</code>—2 Point Dot3af detection • <code>2pt-dot3af+legacy</code>—2 Point Dot3af detection followed by Legacy detection • <code>4pt-dot3af</code>—4 Point Dot3af detection • <code>4pt-dot3af+legacy</code>—4 Point Dot3af detection followed by Legacy detection • <code>legacy</code>— Legacy detection • <code>dot3bt+legacy</code>—Dot3bt detection followed by Legacy detection
Modes	<ul style="list-style-type: none"> • INTERFACE • INTERFACE RANGE
Usage	Use detection mode to set the type of devices that PoE can detect and power up. By default, PoE powers up both IEEE standard devices and pre-IEEE legacy devices which were pre-standard. If you restrict the PoE controller to detect only IEEE standard devices (<code>poe detection dot3bt</code>), you can return to the default detection setting by entering <code>no poe detection</code> .

Examples

```
sonic(config)# interface Ethernet 1/1
sonic(config-if-Eth1/1)# poe detection dot3bt
```

```
sonic(config)# interface Ethernet 1/1
sonic(config-if-Eth1/1)# no poe detection
```

Releases

4.0 or later

poe disable

Disables PoE at the port level.

Command `poe disable`**Options** None

- Modes**
- INTERFACE
 - INTERFACE RANGE

Usage Use this command to disable PoE on a port or port range.**Examples**

```
sonic-cli(config)# interface Ethernet 0
sonic-cli(config-if-Ethernet0)# poe disable
```

```
sonic-cli(config)# interface Ethernet 0
sonic-cli(config-if-Ethernet0)# no poe disable
```

Releases

4.0 or later

poe power management

Configures the PoE power management model.

Command `poe power management { class | dynamic }`

- Options**
- class — Class based power management
 - dynamic — Dynamic power management

Modes CONFIGURATION**Usage** Use this command to set PoE Power management model.**Examples**

```
sonic-cli(config)# poe power management dynamic
```

```
sonic-cli(config)# no poe power management dynamic
```

Releases

4.0 or later

poe priority

Configures the PoE port priority.

Command `poe priority { low | high | critical }`

- Options**
- low—Low priority
 - high—High priority
 - critical—Critical priority

Modes	<ul style="list-style-type: none"> • INTERFACE • INTERFACE RANGE
Usage	Sometimes the switch may not be able to supply power to all connected devices. If adequate power capacity is not available for all PoE-enabled ports, the port priority is used to determine which ports supply power. If ports are configured with the same priority level, a lower-numbered port has a higher priority. By default, a PoE-enabled port has low priority.
Examples	<pre>sonic(config)# interface Ethernet 1/1 sonic-cli(config-if-Eth1/1)# poe priority high</pre> <pre>sonic(config)# interface Ethernet 1/1 sonic-cli(config-if-Eth1/1)# no poe priority</pre>
Releases	4.0 or later

poe reset

Resets the PoE port.

Command	poe reset [<port>]
Options	<i>port</i> —(Optional) Ethernet port number
Modes	EXEC
Usage	Use this command to reset power-supply (PSE) operation on all PoE ports or on a specified PoE port. The port stops delivering power and performs the PoE detection and power delivery cycle again.
Examples	<pre>sonic-cli# poe reset sonic-cli# poe reset Ethernet0</pre>
Releases	4.0 or later

police

Sets rate limiting parameters.

Command	police {{cir cir-value {[cbs cbs-value]} {[pir pir-value]} {[pbs pbs-value]}} {cbs cbs-value {[pir pir-value]} {[pbs pbs-value]}} {pir pir-value {[pbs pbs-value]}} {pbs pbs-value}}
Options	<ul style="list-style-type: none"> • <i>cir cir-value</i> — CIR value • <i>cbs cbs-value</i> — (Optional) CBS value • <i>pir pir-value</i> — (Optional) PIR value • <i>pbs pbs-value</i> — (Optional) PBS value
Modes	POLICY-MAP
Usage	If only CIR is configured, then its a single rate, two color policer. Any traffic exceeding CIR value is marked as red and is dropped. If both CIR and PIR are configured, then it is a two rate three color policer. Any traffic that exceeds CIR but less than PIR is marked as yellow. Any traffic that is more than PIR is marked as red and is dropped. <ul style="list-style-type: none"> • <i>cir</i> — Committed information rate in bits per second. CIR is mandatory. The value can be optionally suffixed with kbps (1000), mbps(1000000), gbps (1000000000) or tbps (100000000000)cir 300000000 cbs 300000000 pir 300000000 pbs 300000000 • <i>cbs</i> — Committed burst size in bytes. The value can be suffixed with KB (1000), MB (1000000), GB (1000000000) or TB(1000000000000). The default value is 20% of the CIR in bytes. If configured, it must be greater than or equal to CIR in bytes.

- **pir** — Peak information rate in bits per second. The value can be optionally suffixed with kbps (1000), mbps (1000000), gbps (1000000000) or tbps (1000000000000). If configured, it must be greater than CIR
- **pbs** — Peak burst size. The value can be suffixed with KB (1000), MB (1000000), GB (10000000000) or TB (10000000000000). The default value is 20% of the PIR value in bytes. If configured, it must be greater than PIR value in bytes and also CBS value

Examples

```
sonic(config-policy-map-flow)# cir 300000000 cbs 300000000 pir 300000000 pbs 300000000
sonic(config-policy-map-flow)# no cir
```

Releases

3.1 or later

police

Sets rate limiting parameters.

Command

`police {{cir cir-value { [cbs cbs-value] }}}`

Options

- **cir cir-value**—CIR value
- **cbs cbs-value**—CBS value

Modes

COPP-ACTION

Usage

Use this command to change the rate limit values for each CoPP action group.

Examples

```
sonic(config)# copp-action copp-user-arp
sonic(config-action)# police cir 6000 cbs 6000
sonic(config-action)# no police cir
```

Releases

3.1 or later

policy-map

Configures flow-based services policies.

Command

`policy-map fbs-policy-name type {acl-copp | copp | forwarding | monitoring | qos}`

Options

- **fbs-policy-name** — Flow-based services policy name (up to 63 characters)
- **acl-copp** — ACL COPP policy
- **copp** — COPP policy
- **forwarding** — Forwarding policy
- **monitoring** — Monitoring policy
- **qos** — QoS policy

Modes

CONFIGURATION

Usage

Policy-map name must begin with A-Z, a-z or 0-9. Underscore and hyphens can be used except as the first character.

Examples

```
sonic(config)# policy-map policy_vrf type forwarding
sonic(config)# no policy-map policy_vrf
```

Releases

3.2 or later

pool

Creates a network address translation (NAT) pool.

Command `pool pool-name global-ip-range [global-port-range]`

Options • *pool-name*—NAT pool name

• *global-ip-range*—Global IP range

• *global-port-range*—(Optional) Global port range (1 to 65535)

Modes CONFIGURATION

Usage Use this command to create a pool for NAT.

Examples

```
sonic(config-nat)# pool pool1
```

```
sonic(config-nat)# no pool pool1
```

Releases 3.0 or later

port

Configures a TCP port for a BGP neighbor.

Command `port tcpport`

Options *tcpport*—TCP port number

Modes BGP-NEIGHBOR

Usage Use this command to configure a TCP port of a BGP neighbor.

Examples

```
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# port 61356
```

```
sonic(config-router-bgp-neighbor)# no port
sonic(config-router-bgp-pg)# no port
```

Releases 3.0 or later

port

Specify the UDP port on which a device listens for requests from configured DACs.

Command `port port-number`

Options *port-number*—Enter a port number (1025 through 65535; default is 3799).

Modes RADIUS-DA

Usage Use this command to specify the UDP port on which a device listens for requests from configured DACs.

Examples

```
sonic(config)# aaa server radius dynamic-author
sonic(config-radius-da)# port 5252
```

Releases 4.1.0 or later

port-group

Configures the port speed for all member ports of a port-group.

Command	<code>port-group pg {speed port_speed}</code>
Options	<ul style="list-style-type: none">• <i>pg</i>—Port-group ID• <i>port_speed</i>—Port speed<ul style="list-style-type: none">◦ 10000—10G◦ 25000—25G◦ auto—Enables interface speed autonegotiation.

Modes	CONFIGURATION
--------------	---------------

Usage	Only the S5224F-ON, S5248F-ON, and S5296F-ON switches support port groups.
--------------	--

Examples	<pre>sonic(config)# port-group 1 speed 10000</pre>
-----------------	--

```
sonic(config)# no port-group 1 speed
```

Releases	3.1 or later
-----------------	--------------

portchannel graceful-shutdown

Enables graceful shutdown on all port channels on the switch.

Command	<code>portchannel graceful-shutdown</code>
Options	None
Modes	CONFIGURATION
Usage	If you enable graceful shutdown globally, all port channels are operationally brought DOWN, except for port channels that have graceful shutdown specifically disabled — see graceful-shutdown . If you disable graceful shutdown globally, all port channels exit graceful shutdown mode and no longer shut down with no frame loss, except for port channels that have graceful shutdown specifically enabled. To globally disable port-channel graceful shutdown, enter the <code>no portchannel graceful-shutdown</code> command.
Examples	<pre>sonic(config)# portchannel graceful-shutdown</pre>
Releases	4.0.3 or later

port-load-current

Sets the port load value to the current-sampled value, when the sampled value is less than the average.

Command	<code>port-load-current</code>
Options	None.
Modes	ARS-PROFILE
Usage	By default, this option is disabled.
Example	<pre>sonic(config-ars-profile)# port-load-current</pre>
Releases	4.4.0 or later

port-load-exponent

Sets the EWMA exponent that is used in port loading computation.

Command	<code>port-load-exponent <i>port-load-exponent-value</i></code>
Options	<i>port-load-exponent-value</i> —The port load exponential value. The range is from 1 to 16. The default value is 2.
Modes	ARS-PROFILE
Usage	The larger the exponent, the larger is the weight to the previously computed port loading value.
Example	<pre>sonic(config-ars-profile)# port-load-exponent 4</pre>
Releases	4.4.0 or later

port-load-future

Enables the future port load as the quality parameter.

Command	<code>port-load-future</code>
Options	None.
Modes	ARS-PROFILE
Usage	This is the average queued bytes measured on a port. By default, this option is enabled.
Example	<pre>sonic(config-ars-profile)#port-load-future</pre>
Releases	4.4.0 or later

port-load-future-weight

Configures the future port load weight attribute for EWMA calculations.

Command	<code>port-load-future-weight <i>future-weight-value</i></code>
Options	<i>future-weight-value</i> —The future port load weight. The range is from 1 to 16. The default value is 2.
Modes	ARS-PROFILE
Usage	A large weight lowers the significance of instantaneous measure on the overall average.
Example	<pre>sonic(config-ars-profile)# port-load-future-weight 4</pre>
Releases	4.4.0 or later

port-load-past

Enables the past port load as the quality parameter.

Command	<code>port-load-past</code>
Options	None.
Modes	ARS-PROFILE
Usage	This is the average egress bytes that are measured on a port. By default this option is enabled.

Example

```
sonic(config-ars-profile) # port-load-past
```

Releases

4.4.0 or later

port-load-past-weight

Configures the past port load weight attribute for EWMA calculations.

Command

```
port-load-past-weight past-weight-value
```

Options

past-weight-value—The past port load weight attribute. The range is from 1 to 16. The default value is 2.

Modes

ARS-PROFILE

Usage

A large weight lowers the significance of instantaneous measure on the overall average.

Example

```
sonic(config-ars-profile) # port-load-past-weight 4
```

Releases

4.4.0 or later

port-security enable

Enables or disables port security feature at the interface level.

Command

```
port-security enable
```

Options

None

Modes

- INTERFACE
- INTERFACE PORTCHANNEL

Usage

Use this command to enable port security on a specific interface. When you enable the port security feature on a port, MAC learning limit mode is set on the port. The port should be a switchport to enable port-security.

Examples

```
sonic(config) # interface Ethernet 0
sonic(config-if-Ethernet0) # port-security enable
```

```
sonic-(config)# interface Ethernet 0
sonic(config-if-Ethernet0) # no port-security enable
```

Releases

4.0 or later

port-security maximum

Configures the maximum number of secure MAC addresses that are allowed on an interface.

Command

```
port-security maximum maximum
```

Options

maximum—Maximum number of secure MAC addresses allowed on the interface (1 to 4097)

Modes

- INTERFACE
- INTERFACE PORTCHANNEL

Usage

Use this command to configure the maximum number of secure MAC addresses allowed on an interface after you enable port security on an interface.

Examples

```
sonic(config)# interface Ethernet 0
sonic(config-if-Ethernet0)# port-security maximum 3

sonic(config-if-Ethernet0)# no port-security maximum
```

Releases

4.0 or later

port-security violation

Configures the action to take when there is a security violation.

Command `port-security violation violation`**Options** *violation*—Enter `protect` to configure the action to take when there is a violation.**Modes**

- INTERFACE
- INTERFACE PORTCHANNEL

Usage Use the `port-security violation` command to configure the action to take when there is a security violation. When a MAC learn-limit violation is detected, a configured protect action protects the port by dropping all packets with unknown source MAC addresses.**Examples**

```
sonic(config)# interface Ethernet 1
sonic(config-if-Ethernet1)# port-security violation protect

sonic(config-if-Ethernet1)# no port-security violation
```

Releases

4.0 or later

preempt

Configures preempt for IPv4 VRRP instances.

Command `preempt`**Options** None**Modes** VRRP**Usage** By default, it is enabled. Use `no preempt` command to disable preempt.**Examples**

```
sonic# configure terminal
sonic(config)# interface Ethernet 4
sonic(config-if-Ethernet4)# vrrp 1 address-family ipv4
sonic(config-if-Ethernet4-vrrp-ipv4-1)# preempt

sonic(config-if-Ethernet6)# vrrp 1 address-family ipv6
sonic(config-if-Ethernet4-vrrp-ipv6-1)# preempt

sonic(config-if-Ethernet4-vrrp-ipv4-1)# no preempt
```

Releases

3.1 or later

prefix-list

Configures a prefix-list for a BGP neighbor or peer-group.

Command	<code>prefix-list <i>pname</i> {in out}</code>
Options	<code><i>pname</i></code> — Prefix-list name to filter inbound and/or outbound
Modes	<ul style="list-style-type: none">• NEIGHBOR-ADDRESS-FAMILY• PEER-GROUP-ADDRESS-FAMILY
Usage	Use this command to define a policy (route filtering) for a BGP neighbor or BGP peer-group in an outbound or/and inbound direction.
Examples	<pre>sonic(config-router-bgp)# neighbor 20.20.20.2 sonic(config-router-bgp-neighbor)# remote-as 300 sonic(config-router-bgp-neighbor)# address-family ipv4 unicast sonic(config-router-bgp-neighbor-af)# prefix-list pl_allow_remote in sonic(config-router-bgp)# peer-group PG_Ext sonic(config-router-bgp-pg)# address-family ipv4 unicast sonic(config-router-bgp-pg-af)# prefix-list pl_allow_remote in sonic(config-router-bgp-pg-af)# no prefix-list pl_allow_remote in</pre>
Releases	3.0 or later

primary-ip

Configures the primary IPv4 address on MLAG peers in a logical VTEP.

Command	<code>primary-ip {<i>ipv4-address</i> Loopback <i>number</i>}</code>
Options	<ul style="list-style-type: none">• <i>ipv4-address</i> — Enter an IPv4 address in A.B.C.D format. An IPv6 address is not supported as a primary IP address on an MLAG VTEP.• <i>Loopback number</i> — Enter a loopback ID number (0 - 16383). The loopback interface must be configured with an IPv4 address.
Modes	INTERFACE-VXLAN-VTEP
Usage	If you use MLAG to configure two VTEPs to form a logical VTEP, it is recommended that you configure a primary IP address in addition to the source IP address on each node. If you specify a loopback number for the primary IP address, the loopback interface must be configured with an IPv4 address. You cannot reconfigure or delete a loopback IP address if it is being used as the primary IP address on an MLAG VTEP. You can reconfigure or delete a primary IP address "on the fly" on an MLAG VTEP if VLAN- or VRF-to-VNI mapping is configured.
Examples	<pre>sonic(config)# interface vxlan vtep1 sonic(config-if-vxlan-vtep1)# primary-ip 1.1.1.2 sonic(config-if-vxlan-vtep1)# no primary-ip sonic(config)# interface vxlan vtep2 sonic(config-if-vxlan-vtep2)# external-ip Loopback 10</pre>
Releases	3.2 or later

priority

Configures the priority for master election.

Command	<code>priority priority-value</code>
Options	<code>priority-value</code> —Enter the priority value (1 to 254; default is 100)
Modes	VRRP
Usage	Use this command to configure the priority for master election. The router that has the highest priority becomes the master.
Examples	<pre>sonic(config-if-Ethernet4)# vrrp 1 address-family ipv4 sonic(config-if-Ethernet4-vrrp-ipv4-1)# priority 120 sonic(config-if-Ethernet4-vrrp-ipv4-1)# no priority</pre>
Releases	3.0 or later

priority-flow-control

Configures priority flow control (PFC) on an interface.

Command	<code>priority-flow-control {priority dot1p asymmetric watchdog}</code>
Options	<ul style="list-style-type: none">• <code>priority dot1p</code>—Enable lossless PFC for a specified dot1p priority; the defaults are 3 and 4. On Trident4 (TD4, such as Z9432F-ON), Tomahawk4 (TH4, such as Z9664F-ON), and Tomahawk5 (TH5, such as Z9864F-ON) switches, you can reconfigure the PFC priorities on any switch port to a non-default value between 0 and 7. To enter two priorities with the command, separate the PFC priority values with a comma; for example, <code>priority-flow-control priority 0,1</code>.<ul style="list-style-type: none">◦ Only two lossless priorities are configurable per port.◦ By default, lossless priorities 3 and 4 are fixed. You can reconfigure either value 3 or value 4 or both values on a Trident4 (TD4), Tomahawk4 (TH4), or Tomahawk5 (TH5) switch.◦ On a TD4, TH4, or TH5 switch, the configured priority values must be the same as the priority mapping in the pfc-priority-to-pg QoS map.• <code>asymmetric</code>—Enable asymmetric PFC.• <code>watchdog</code>—Enable PFC watchdog.
Modes	INTERFACE
Usage	To enable lossless PFC priorities on an interface, use the <code>priority-flow-control</code> command. Based on the PFC priority, the interface sends PFC pause frames to stop a peer from sending lossless priority traffic when traffic congestion occurs. When asymmetric PFC is enabled and PFC pause frames are received from a peer, the interface honors pause frames on all PFC priorities (not only lossless priority traffic) and stops sending packets. The interface continues to send pause frames if there is lossless traffic congestion. If PFC watchdog is enabled and a continuous pause is received on an interface, PFC watchdog detects and mitigates the PFC storm. NOTE: In Release 4.4.0, you can reconfigure the default PFC priority values only on a Trident4 (TD4, such as Z9432F-ON), Tomahawk4 (TH4, such as Z9664F-ON), or Tomahawk5 (TH5, such as Z9864F-ON) switch by using the <code>roce enable pfc-priority</code> command. For example: <pre>sonic(config)# roce enable pfc-priority 1,7</pre> NOTE: If you reconfigure the PFC priority values on a TD4, TH4, or TH5 switch, the configured <code>priority-flow-control</code> priority and the <code>qos-map pfc-priority-pg</code> map associated with PG 3 and 4 must have the same priority configuration.

Examples

```
sonic(config-if-Ethernet4) # priority-flow-control asymmetric
```

```
sonic(config-if-Ethernet4) # no priority-flow-control
```

Releases

3.1 or later

priority-flow-control watchdog action

Configures PFC watchdog storm action.

Command

```
priority-flow-control watchdog action {alert | drop | forward}
```

Options

- **alert**—Sends an alert message when a PFC storm is detected.
- **drop**—Drops incoming packets that are destined for lossless queues.
- **forward**—Forwards all packets that are destined to the queue and all packets in the queue.

Modes

INTERFACE

Usage

Use this command to configure the PFC watchdog action after a PFC storm is detected on a lossless queue.

Examples

```
sonic# configure terminal  
sonic(config)# interface Ethernet 4  
sonic(config-if-Ethernet4) # priority-flow-control watchdog action
```

```
sonic(config-if-Ethernet4) # no priority-flow-control watchdog action
```

Releases

3.1 or later

priority-flow-control watchdog counter-poll

Enables PFC watchdog FLEX counters.

Command

```
priority-flow-control watchdog counter-poll
```

Options

None

Modes

CONFIGURATION

Usage

Use this command to enable PFC watchdog to poll FLEX counters.

Examples

```
sonic# configure terminal  
sonic(config) # priority-flow-control watchdog counter-poll
```

```
sonic(config) # no priority-flow-control watchdog counter-poll
```

Releases

3.1 or later

priority-flow-control watchdog off

Disables PFC watchdog.

Command

```
priority-flow-control watchdog off
```

Options

None

Modes

INTERFACE

Usage

Use this command to disable PFC watchdog on an interface.

Examples

```
sonic# configure terminal
sonic(config)# interface Ethernet 4
sonic(config-if-Ethernet4)# priority-flow-control watchdog off
```

Releases

3.1 or later

priority-flow-control watchdog on

Enables PFC watchdog.

Command

`priority-flow-control watchdog on detect-time detection-time`

Options

detection-time—Enter the detection time in milliseconds (100-5000)

Modes

INTERFACE

Usage

Use this command to configure the detection time for detecting a PFC storm from a peer switch on lossless queues and enable PFC watchdog on the interface.

Examples

```
sonic# configure terminal
sonic(config)# interface Ethernet 4
sonic(config-if-Ethernet4)# priority-flow-control watchdog on
```

Releases

3.1 or later

priority-flow-control watchdog polling-interval

Configures the PFC watchdog polling interval.

Command

`priority-flow-control watchdog polling-interval interval`

Options

interval—Specify an interval by entering a number in milliseconds (100 to 3000; default is 100)

Modes

CONFIGURATION

Usage

Use this command to configure the PFC watchdog polling interval for checking incoming packets.

Examples

```
sonic# configure terminal
sonic(config)# priority-flow-control watchdog polling-interval 100

sonic(config)# no priority-flow-control watchdog polling-interval
```

Releases

3.1 or later

priority-flow-control watchdog restore-time

Configures the PFC watchdog restoration time.

Command

`priority-flow-control watchdog restore-time restore-time`

Options

restore-time—Restore time in milliseconds (100-60000)

Modes

INTERFACE

Usage

Use this command to configure the PFC watchdog restoration time. When no PFC frames are received for the configured restore time, PFC is re-enabled on the queue.

Examples

```
sonic# configure terminal
sonic(config)# interface Ethernet 4
```

```
sonic(config-if-Ethernet4) # priority-flow-control watchdog restore-time  
3000
```

```
sonic(config-if-Ethernet4) # no priority-flow-control watchdog restore-  
time
```

Releases	3.1 or later
-----------------	--------------

profile

Changes the default configurations of a BFD peer without configuring static BFD peers.

Command `profile profile-name`

Options `profile-name` — Profile name (up to 63 characters)

Modes

- BFD
- PEER
 - peer <*peer_ipv4*>
 - peer <*peer_ipv6*>
 - peer [interface] <*interfacename*>
 - peer [local-address] <*local_ipv4*>
 - peer [local-address] <*local_ipv6*>
 - peer [multihop]
 - peer [vrf] <*vrfname*>

Usage

A BFD profile acts as a template configuration, which can be attached to multiple BFD peers. A BFD profile can be associated to a BFD static peer, BGP neighbor or peer-group, OSPF, and PIM neighbors. If a BFD profile is associated with a BFD peer, BGP neighbor or peer-group, and if OSPF and PIM are not configured, the profile takes effect after it is configured.

- When you configure BFD parameters in a static peer and a BFD profile is also associated with the static BFD peer, the BFD parameters configured in the peer takes precedence over BFD profile.
- If BGP, OSPF and PIM share a BFD session, and if the BFD profile associated with BGP, OSPF, and PIM is different, the latest configured profile in either BGP, OSPF, or PIM takes effect.
- The BFD profile configuration can be changed dynamically. All the configuration parameters take effect immediately and BFD timers are renegotiated using the polling method.
- If a BFD profile associated with a BGP, OSPF, PIM, or BFD static peer is deleted, the associated BFD session resets to the default values. The profile configuration must be deleted from BGP, OSPF, PIM, or BFD static peer as well.

Examples

BFD mode:

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# profile active1
```

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# no profile active1
```

BFD PEER mode:

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0  
sonic(config-bfd-peer)# profile active1
```

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0  
sonic(config-bfd-peer)# no profile active1
```

Associate a BFD profile with a BFD static peer:

```
sonic# configure terminal  
sonic(config)# bfd  
sonic(config-bfd)# peer 1.1.1.1 interface Ethernet32  
sonic(config-bfd-peer)# profile active1
```

Associate a BFD profile with a BGP neighbor:

```
sonic# configure terminal  
sonic(config)# router bgp 1  
sonic(config-router-bgp)# neighbor 1.1.1.1  
sonic(config-router-bgp-neighbor)# bfd profile active1
```

Associate a BFD profile with a BGP peer group:

```
sonic# configure terminal  
sonic(config)# router bgp 1  
sonic(config-router-bgp)# peer-group group1  
sonic(config-router-bgp-pg)# bfd profile active1
```

Associate a BFD profile with an OSPF interface:

```
sonic# configure terminal  
sonic(config)# interface Ethernet32  
sonic(config-if-Ethernet32)# ip ospf bfd profile active1
```

Associate a BFD profile with a PIM interface:

```
sonic# configure terminal  
sonic(config)# interface Ethernet32  
sonic(config-if-Ethernet32)# ip pim bfd profile active1
```

Releases

4.0 or later

Q and R commands

Topics:

- qos-fbs
- qos map dot1p-tc
- qos map dscp-tc
- qos-map pfc-priority-pg
- qos map pfc-priority-queue
- qos map tc-dot1p
- qos map tc-dscp
- qos map tc-pg
- qos map tc-queue
- qos scheduler-policy
- qos wred-policy
- qos-map dot1p-tc
- qos-map dscp-tc
- qos-map pfc-priority-queue
- qos-map tc-dot1p
- qos-map tc-dscp
- qos-map tc-pg
- qos-map tc-queue
- qos-mode
- queue
- radius-server auth-type
- radius-server host
- radius-server key
- radius-server nas-ip
- radius-server retransmit
- radius-server statistics
- radius-server timeout
- radv enable
- random-seed
- rd
- read-quanta
- reboot
- receive-interval
- redirect security-profile
- redistribute
- redistribute
- refresh
- remark
- remote-as
- remove-private-as
- renew dhcp-lease
- request-data-size
- revision
- roce enable
- route-map
- route-map
- route-map delay-timer

- route-reflector allow-outbound-policy
- route-reflector-client
- route-scale routes
- route-scale hosts
- route-server-client
- route-target
- router bgp
- router ospf
- router-id

qos-fbs

Configures key-profile for QoS flow-based-services.

Command `qos-fbs {egress | ingress} key-profile {ip | ipv4 | ipv6 | l2 | 12-ipv4}`

Options

- egress—egress direction
- ingress—ingress direction
- ip—IPv4 and IPv6 key-profile
- ipv4—IPv4 key-profile
- ipv6—IPv6 key-profile
- l2—L2 key-profile
- 12-ipv4—L2 and IPv4 key-profile

Modes TCAM

Usage Use this command to set the hardware TCAM key-profiles for QoS flow-based service policies.

Examples

```
sonic# configure terminal
sonic(config)# hardware
sonic(config-hardware)# tcam
sonic(config-hardware-tcam)# qos-fbs ingress key-profile ip
```

Releases 4.0 or later

qos map dot1p-tc

Creates a map to associate a set of dot1p to traffic classes.

Command `qos map dot1p-tc name`

Options `name` — Policy map name (up to 32 characters)

Modes CONFIGURATION

Usage This map used to assign a traffic class to data packets on the basis of the received packets dot1p field.

Examples

```
sonic(config)# qos map dot1p-tc dot1p-map

sonic(config)# no qos map dot1p-tc dot1p-map
```

Releases 3.1 or later

qos map dscp-tc

Creates a map to associate a set of differentiated services code point (DSCP) to traffic classes.

Command `qos map dscp-tc name`

Options	<i>name</i> — Policy map name (up to 32 characters)
Modes	CONFIGURATION
Usage	This map used to assign a traffic class to data packets on the basis of the received packets DSCP field.
Examples	<pre>sonic(config)# qos map dscp-tc dscp-map</pre> <pre>sonic(config)# no qos map dscp-tc dscp-map</pre>
Releases	3.1 or later

qos-map pfc-priority-pg

Applies a PFC priority-to-priority group mapping on a switch interface.

Command	<code>qos-map pfc-priority-pg <i>pg-name</i></code>
Options	• <i>pg-name</i> — Enter the name of a priority group (up to 32 characters).
Modes	INTERFACE
Usage	To map a PFC priority to a priority group map in a QoS pfc-priority-to-pg map, use the pfc-priority pg command.
Examples	<pre>sonic(config-if-Eth1/2)# qos-map pfc-priority-pg pfc-pg-remap</pre> <pre>sonic(config-if-Eth1/2)# no qos-map pfc-priority-pg</pre>
Releases	4.2.1 or later

qos map pfc-priority-queue

Creates a map to associate a set of priority flow control (PFC) priorities to queues.

Command	<code>qos map pfc-priority-queue <i>name</i></code>
Options	<i>name</i> — PFC priority queue name (up to 32 characters)
Modes	CONFIGURATION
Usage	This map is used to classify a queue for data packets on the basis of the received packets dot1p field.
Examples	<pre>sonic(config)# qos map pfc-priority-queue pfc-priority-queue-map</pre> <pre>sonic(config)# no qos map pfc-priority-queue pfc-priority-queue-map</pre>
Releases	3.1 or later

qos map tc-dot1p

Creates a map to associate a set of traffic class to dot1p (VLAN PCP value).

Command	<code>qos map tc-dot1p <i>name</i></code>
Options	<i>name</i> — dot1p policy-map name (up to 32 characters)
Modes	CONFIGURATION
Usage	This map is used to remark the dot1p field in egress packets on the basis of the internal traffic class.

Examples

```
sonic(config)# qos map tc-dot1p tc_dot1p  
sonic(config)# no qos map tc-dot1p tc_dot1p
```

Releases

3.1 or later

qos map tc-dscp

Creates a map to associate a set of traffic class to differentiated services code point (DSCP).

Command

`qos map tc-dscp name`

Options

name — DSCP policy map name (up to 32 characters)

Modes

CONFIGURATION

Usage

This map is used to remark the DSCP field in egress packets on the basis of the internal traffic class.

Examples

```
sonic(config)# qos map tc-dscp tc_dscp  
sonic(config)# no qos map tc-dscp tc_dscp
```

Releases

3.1 or later

qos map tc-pg

Creates a map to associate a set of traffic class to priority group.

Command

`qos map tc-pg name`

Options

name — Priority group name (up to 32 characters)

Modes

CONFIGURATION

Usage

This map is used to assign a priority group to data packets on the basis of the traffic class.

Examples

```
sonic(config)# qos map tc-pg tc-pg-map  
sonic(config)# no qos map tc-pg tc-pg-map
```

Releases

3.1 or later

qos map tc-queue

Creates a map to associate a set of traffic class to queue.

Command

`qos map tc-queue name`

Options

name — Queue map name (up to 32 characters)

Modes

CONFIGURATION

Usage

This map is used to assign an egress queue to data packets on the basis of the traffic class.

Examples

```
sonic(config)# qos map tc-queue tc-queue-map  
sonic(config)# no qos map tc-queue tc-queue-map
```

Releases	3.1 or later
-----------------	--------------

qos scheduler-policy

Configures the QoS scheduler policy.

Command	<code>qos scheduler-policy name</code>
Options	<code>name</code> — Scheduler policy name (up to 32 characters)
Modes	CONFIGURATION
Usage	None
Examples	<pre>sonic(config)# qos scheduler-policy sched-policy1</pre> <pre>sonic(config)# no qos scheduler-policy sched-policy1</pre>

Releases	3.1 or later
-----------------	--------------

qos wred-policy

Creates WRED policies.

Command	<code>qos wred-policy name</code>
Options	<code>name</code> —WRED policy name (up to 32 characters)
Modes	CONFIGURATION
Usage	Use this command to enter the WRED policy mode and set the WRED policy settings.
Examples	<pre>sonic(config)# qos wred-policy wred-green</pre> <pre>sonic(config)# no qos wred-policy wred-green</pre>

Releases	3.1 or later
-----------------	--------------

qos-map dot1p-tc

Applies a dot1p-to-traffic class mapping on an interface.

Command	<code>qos-map dot1p-tc dot1p_tc_map_name</code>
Options	<code>dot1p_tc_map_name</code> —Enter a dot1p-traffic-class map name (up to 32 characters).
Modes	INTERFACE
Usage	Use this command to configure dot1p-to-traffic class mapping on an interface.
Example	<pre>sonic(config-if-Eth1/2)# qos-map dot1p-tc dot1p-map</pre> <pre>sonic(config-if-Eth1/2)# no qos-map dot1p-tc dot1p-map</pre>

Releases	3.1 or later
-----------------	--------------

qos-map dscp-tc

Applies a DSCP-to-traffic class mapping on an interface.

Command	<code>qos-map dscp-tc <i>dscp_tc_map_name</i></code>
Options	<code><i>dscp_tc_map_name</i></code> —Enter a DSCP traffic-class map name (up to 32 characters).
Modes	INTERFACE
Usage	Use this command to apply the DSCP-to-traffic class mapping on an interface.
Examples	<pre>sonic# configure terminal sonic(config)# interface Ethernet 1/2 sonic(config-if-Eth1/2)# qos-map dscp-tc dscp-map</pre> <pre>sonic(config-if-Eth1/2)# no qos-map dscp-tc dscp-map</pre>
Releases	3.1 or later

qos-map pfc-priority-queue

Applies a PFC priority-to-queue mapping on an interface.

Command	<code>qos-map pfc-priority-queue <i>pfc_priority_queue_map_name</i></code>
Options	<code><i>pfc_priority_queue_map_name</i></code> —Enter a PFC priority-queue map name (up to 32 characters)
Modes	INTERFACE
Usage	Use this command to apply a PFC priority-to-queue mapping on an interface.
Examples	<pre>sonic# configure terminal sonic(config)# interface Ethernet 1/2 sonic(config-if-Eth1/2)# qos-map pfc-priority-queue pfc-priority-queue-map</pre> <pre>sonic(config-if-Eth1/2)# no qos-map pfc-priority-queue pfc-priority-queue-map</pre>
Releases	3.1 or later

qos-map tc-dot1p

Applies a traffic class-to-dot1p mapping on an interface.

Command	<code>qos-map tc-dot1p <i>tc_dot1p_map_name</i></code>
Options	<code><i>tc_dot1p_map_name</i></code> —Enter a traffic class-dot1p map name (up to 32 characters).
Modes	INTERFACE
Usage	Use this command to apply a traffic class-to-dot1p mapping on an interface.
Examples	<pre>sonic# configure terminal sonic(config)# interface Ethernet 1/2 sonic(config-if-Eth1/2)# qos-map tc-dot1p dot1p-map</pre> <pre>sonic(config-if-Eth1/2)# no qos-map tc-dot1p dot1p-map</pre>

Releases 3.1 or later

qos-map tc-dscp

Applies a traffic class-to-DSCP mapping on an interface.

Command `qos-map tc-dscp tc_dscp_map_name`

Options `tc_dscp_map_name`—Enter a traffic class-DSCP map name (up to 32 characters).

Modes INTERFACE

Usage Use this command to apply a traffic class-to-DSCP mapping on an interface.

Examples

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1/2  
sonic(config-if-Eth1/2)# qos-map tc-dscp dscp-map
```

```
sonic(config-if-Eth1/2)# no qos-map tc-dscp dscp-map
```

Releases 3.1 or later

qos-map tc-pg

Applies a traffic class-to-priority group mapping on an interface.

Command `qos-map tc-pg tc_pg_map_name`

Options `tc_pg_map_name`—Enter a traffic class-to-priority group map name (up to 32 characters).

Modes INTERFACE

Usage Use this command to apply a traffic class-to-priority group mapping on an interface.

Examples

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1/2  
sonic(config-if-Eth1/2)# qos-map tc-pg tc-pg-map
```

```
sonic(config-if-Eth1/2)# no qos-map tc-pg tc-pg-map
```

Releases 3.1 or later

qos-map tc-queue

Applies a traffic class-to-queue mapping on an interface.

Command `qos-map tc-queue tc_queue_map_name`

Options `tc_queue_map_name`—Enter a traffic class-to-queue map name (up to 32 characters).

Modes INTERFACE

Usage Use this command to apply a traffic class-to-queue mapping on an interface.

Examples

```
sonic# configure terminal  
sonic(config)# interface Ethernet 1/2  
sonic(config-if-Eth1/2)# qos-map tc-queue tc-queue-map
```

```
sonic(config-if-Eth1/2)# no qos-map tc-queue tc-queue-map
```

Releases 3.1 or later

qos-mode

Configures QoS mode.

Command	<code>qos-mode {uniform {pipe {dscp dscp-value}}}}</code>
Options	<ul style="list-style-type: none">• <code>uniform</code>—Copies the DSCP value to the outer IP header at encapsulation. Also, may copy the outer header DSCP value to the inner IP header at decapsulation.• <code>pipe</code>—Assigns a user-defined DSCP value to the outer IP header at encapsulation and the inner IP header DSCP value remains intact at decapsulation.• <code>dscp dscp-value</code>—DSCP value (0 to 63)
Modes	INTERFACE
Usage	The default QoS mode is <code>pipe</code> . The command can be used only on VXLAN mode.
Example	<pre>sonic(config)# interface vxlan vtep-leaf sonic(config-if-vxlan-vtep-leaf)# qos-mode uniform</pre> <pre>sonic(config-if-vxlan-vtep-leaf)# qos-mode pipe dscp 10</pre>
Releases	3.1 or later

queue

Sets queue configuration based on the WRED policy.

Command	<code>queue qid {wred-policy wred_prof_name}</code>
Options	<ul style="list-style-type: none">• <code>qid</code>—Enter the Queue ID (0 to 7)• <code>wred-policy wred_prof_name</code>—Enter the WRED policy name (up to 32 characters)
Modes	<ul style="list-style-type: none">• INTERFACE• SCHEDULER-POLICY
Usage	Use this command to set a WRED policy to a queue on an interface. When used in scheduler policy mode, this command enters queue context to set scheduling parameters.
Examples	<pre>sonic(config)# interface Ethernet 10 sonic(config-if-Ethernet-10)# queue 7 wred-policy wred-policy1</pre> <pre>sonic(config)# qos scheduler-policy new_policy sonic(config-sched-policy-new_policy)# queue 3 sonic(config-scheduler-new_policy-queue-3) #</pre> <pre>sonic(config-if-Ethernet-10)# no queue 7 wred-policy</pre>
Releases	3.1 or later

radius-server auth-type

Configures the global RADIUS server authentication type.

Command	<code>radius-server auth-type [chap pap mschapv2]</code>
Options	<ul style="list-style-type: none">• <code>chap</code> — Enables <code>chap</code> for the authentication type (default)• <code>pap</code> — Enables <code>pap</code> for the authentication type• <code>mschapv2</code> — Enables <code>mschap</code> for the authentication type

Modes	CONFIGURATION
Usage	Use this command to configure a default RADIUS server authentication type that is used for remote user access. The authentication type is used to encrypt or decrypt data that is sent and received between the switch and the RADIUS server. If you have not configured a server-specific authtype, this global value is used for that RADIUS server.
Examples	<pre>sonic(config)# radius-server auth-type pap</pre> <pre>sonic(config)# no radius-server auth-type</pre>
Releases	3.0 or later

radius-server host

Configures a RADIUS server and the key used to authenticate the switch on the server.

Command	<code>radius-server host <i>host_ip</i> [<i>auth-port vauth_port</i>] [<i>auth-type vauth_type</i>] [<i>key vkey</i>] [<i>priority vpriority</i>] [<i>retransmit vretransmit</i>] [<i>source-interface</i> {Ethernet Loopback Management PortChannel Vlan SubInterface}] [<i>timeout vtimeout</i>] [<i>vrf {mgmt vrf-name}</i>]</code>
Options	<ul style="list-style-type: none"> • <i>host_ip</i> — IPv4 or IPv6 host in A.B.C.D or A::B format • <i>vauth_port</i> — (Optional) Port number • <i>vauth_type</i> — (Optional) Authentication type; select pap, chap, or mschapv2 • <i>vkey</i> — (Optional) Secret key (up to 31 characters) • <i>vpriority</i> — (Optional) Priority number (1 to 64) • <i>vretransmit</i> — (Optional) Retransmit attempts • <i>vtimeout</i> — (Optional) Timeout in seconds • <i>vrf-name</i> — (Optional) VRF name prefixed by Vrf_ (up to 15 characters)
Modes	CONFIGURATION
Usage	Use this command to configure a RADIUS server host. The authentication key must match the key configured on the RADIUS server, and you cannot enter spaces in the key. You can configure global settings for the timeout and retransmit attempts allowed on RADIUS servers.
Examples	<pre>sonic(config)# radius-server host 10.59.100.2 key testing123</pre> <pre>sonic(config)# no radius-server host 10.59.100.2 key testing123</pre>
Releases	3.2 or later

radius-server key

Configures the global authentication key for the RADIUS server.

Command	<code>radius-server key <i>key</i></code>
Options	<i>key</i> — Authentication key (up to 31 characters)
Modes	CONFIGURATION
Usage	Use this command to modify the global value for the RADIUS server authentication key. If you have not configured a server-specific authentication key, this global value is used for that RADIUS server. The authentication key can include all printable ASCII characters with a few exceptions (#, SPACE, and COMMA), and up to 65 characters.

Examples

```
sonic(config) # radius-server key testing123  
sonic(config) # no radius-server key
```

Releases

3.0 or later

radius-server nas-ip

Configures the global RADIUS network access server (NAS) IP address.

Command`radius-server nas-ip nas_ip`**Options**`nas_ip`—NAS IP address in A.B.C.D or A::B format**Modes**

CONFIGURATION

Usage

Use this command to configure the NAS IP address for a RADIUS server group. The management interface IP address is used as the default NAS IP address.

Examples

```
sonic(config) # radius-server nas-ip 10.59.100.2  
sonic(config) # no radius-server nas-ip
```

Releases

3.1 or later

radius-server retransmit

Configures the number of authentication attempts allowed on the RADIUS server.

Command`radius-server retransmit retransmit`**Options**`retransmit` — Number of retry attempts (0 to 100; default 3)**Modes**

CONFIGURATION

Usage

Use this command to globally configure the number of retransmit attempts allowed for authentication requests on RADIUS servers. If you have not configured a server-specific retransmit, this global value is used for that server.

Examples

```
sonic(config) # radius-server retransmit 10  
sonic(config) # no radius-server retransmit
```

Releases

3.0 or later

radius-server statistics

Configures global RADIUS statistics.

Command`radius-server statistics {enable | disable}`**Options**

- `enable`—Enables RADIUS statistics
- `disable`—Disables RADIUS statistics

Modes

CONFIGURATION

Usage

Use this command to enable or disable RADIUS server statistics globally.

Examples

```
sonic(config) # radius-server statistics enable
```

```
sonic(config) # radius-server statistics disable
```

Releases

3.1 or later

radius-server timeout

Configures the timeout used to resend RADIUS authentication requests.

Command

```
radius-server timeout seconds
```

Options

seconds — Retransmission time (1 to 60 seconds; default 5)

Modes

CONFIGURATION

Usage

Use this command to globally configure the timeout value used on RADIUS servers. If you have not configured a server-specific timeout, this global value is used for that server.

Examples

```
sonic(config) # radius-server timeout 10
```

```
sonic(config) # no radius-server timeout
```

Releases

3.0 or later

radv enable

Enable the SONiC router advertisement daemon inside the radv docker (RADVD) to send router advertisement (RA) messages on an interface.

Command

```
radv enable
```

Options

None

Modes

CONFIGURATION

Usage

The `radv enable` command is provided only for backward compatibility with community SONiC (radv docker) and is disabled by default. This command is not required for the switch to send router advertisements. It is strongly recommended not to enable the `radv enable` command. If you use this command to configure the switch, you must save the switch configuration and reload the switch.

Examples

```
sonic(config) # radv enable
```

Releases

4.0.3 or later

random-seed

Specifies the random seed value for adaptive routing and switching.

Command

```
random-seed random-seed-value
```

Options

random-seed-value—The random seed value. The range is from 0 to 16777214. The default value is 10.

Modes

ARS-PROFILE

Usage

For the Z9664F-ON platform, specify a nonzero random seed value.

Example

```
sonic(config-ars-profile)#random-seed 167877
```

Releases

4.4.0 or later

rd

Specifies the route-distinguisher (RD) to attach to routes exported from the current VRF into EVPN.

Command `rd rdvalue`

Options `rdvalue`—Route-distinguisher in A.B.C.D:NN or ASN:NN format

Modes BGP-ADDRESS-FAMILY

Usage Use this command to specify the RD value to attach to routes exported from the current VRF into EVPN.

Examples

```
sonic(config)# router bgp 100 vrf Vrf1  
sonic(config-router-bgp)# address-family l2vpn evpn  
sonic(config-router-bgp-af)# rd 11:11
```

```
sonic(config)# router bgp 100  
sonic(config-router-bgp)# address-family l2vpn evpn  
sonic(config-router-bgp-af)# vni 100  
sonic(config-router-bgp-af-vni)# rd 11:11
```

```
sonic(config-router-bgp-af)# no rd 11:11  
sonic(config-router-bgp-af-vni)# no rd 11:11
```

Releases

3.0 or later

read-quanta

Configures the maximum number of BGP packets to read from peer socket in one cycle.

Command `read-quanta rdval`

Options `rdval` — Maximum number of packets to read

Modes ROUTER-BGP

Usage Use this command to configure the maximum number of BGP packets to read from the peer socket in one cycle of I/O. BGP packets are read off the wire, one loop at a time. This setting controls how many iterations the loop runs for.

Examples

```
sonic(config)# router bgp 65300  
sonic(config-router-bgp)# read-quanta 6
```

```
sonic(config-router-bgp)# no read-quanta
```

Releases

3.0 or later

reboot

Reboots the switch.

Command `reboot`

Options None

Modes	EXEC
Usage	Use this command to reboot the switch. Dell Technologies recommends saving the configuration using <code>write memory</code> command before rebooting the switch.
Example	<pre>sonic# reboot reboot in process Waiting for the reboot operation to complete</pre>
Releases	3.1 or later

receive-interval

Configures the minimum interval to receive BFD packets.

Command	<code>receive-interval receive_interval</code>
Options	<code>receive_interval</code> —Peer receive interval in milliseconds (10 to 60000; default is 300)
Modes	<ul style="list-style-type: none"> • PEER • BFD PROFILE
Usage	Use this command to configure the minimum interval during which the system can receive BFD control packets.
Example	<p>Example for PEER mode:</p> <pre>sonic# configure terminal sonic(config)# bfd sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0 sonic(config-bfd-peer)# receive-interval 100</pre> <p>Example for PROFILE mode:</p> <pre>sonic# configure terminal sonic(config)# bfd sonic(config-bfd)# profile fast sonic(config-bfd-profile)# receive-interval 100</pre>
Releases	3.0 or later

redirect security-profile

Configures a new security profile for the redirect feature.

Command	<code>redirect security-profile security-profile-name</code>
Modes	CONFIGURATION
Usage	The security-profile points to the CA certificate file to be used by redirect for HTTPS connections.
Examples	<pre>sonic(config)# redirect security-profile test123</pre>
Releases	4.1.0 or later

redistribute

Redistributes connected, static, and OSPF routes into BGP.

Command	<code>redistribute {connected static ospf} [route-map route-map-name] [metric metvalue]</code>
----------------	--

Options

- `connected` — Redistributes routes from physically connected interfaces
- `static` — Redistributes routes from manually configured routes
- `ospf` — Redistributes OSPF internal routes
- `route-map-name` — (Optional) Route-map name
- `metvalue` — (Optional) Default metric value for redistributed routes

Modes

BGP-ADDRESS-FAMILY

Usage

Use this command to configure the redistribution of routes into the Border Gateway Protocol (BGP). Also, a route-map can be applied to the routes being redistributed.

Examples

```
sonic(config-router-bgp) # address-family ipv4 unicast
sonic(config-router-bgp-af) # redistribute connected

sonic(config-router-bgp-af) # no redistribute connected
```

Releases

3.0 or later

redistribute

Redistributes connected, static, kernel, and BGP routes into OSPF.

Command

```
redistribute {{bgp {[metric bgpmetricval]} {[metric-type bgpmetrictype]} {[route-map bgproutemapname]}} | {connected {[metric connmetricval]} {[metric-type connmetrictype]} {[route-map connroutemapname]}} | {static {[metric staticmetricval]} {[metric-type staticmetrictype]} {[route-map staticroutemapname]}} | {kernel {[metric kernelmetricval]} {[metric-type kernelmetrictype]} {[route-map kernelroutemapname]}}}}
```

Options

- `bgpmetricval` — (Optional) BGP metric value
- `bgpmetrictype` — (Optional) BGP metric type
- `bgproutemapname` — (Optional) BGP route-map name
- `connmetricval` — (Optional) Connected metric value
- `connmetrictype` — (Optional) Connected metric type
- `connroutemapname` — (Optional) Connected route-map name
- `staticmetricval` — (Optional) Static metric value
- `staticmetrictype` — (Optional) Static metric type
- `staticroutemapname` — (Optional) Static route-map name
- `kernelmetricval` — (Optional) Kernel metric value
- `kernelmetrictype` — (Optional) Kernel metric type
- `kernelroutemapname` — (Optional) Kernel route-map name

Modes

ROUTER-OSPF

Usage

Use this command to configure route redistribution into an OSPFv2 router. You can modify the redistributed route metric and metric type using this command. Route-map can also be applied to redistributed route. Unconfiguring any of the redistribute attribute for a protocol unconfigures all attributes.

Examples

```
sonic(config-router-ospf) # redistribute bgp

sonic(config-router-ospf) # redistribute bgp route-map bgpospfrmap

sonic(config-router-ospf) # redistribute static metric 10 metrictype 1 routemap
redist_rmap

sonic(config-router-ospf) # redistribute connected metric 10 metrictype 1

sonic(config-router-ospf) # no redistribute connected
```

Releases	3.1 or later
-----------------	--------------

refresh

Configures the LSA refresh interval.

Command	<code>refresh timer <i>refreshtimer</i></code>
Options	<code>refreshtimer</code> —Enter the refresh timer value in seconds (10 to 1800; default is 1800)
Modes	ROUTER-OSPF
Usage	Use this command to configure the LSA refresh interval.
Examples	<pre>sonic(config) # router ospf sonic(config-router-ospf) # refresh timer 10 sonic(config-router-ospf) # no refresh timer</pre>

Releases	3.1 or later
-----------------	--------------

remark

Sets a remark value or description for an ACL.

Command	<code>remark <i>remark-val</i></code>
Options	<code>remark-val</code> — Remark value (up to 256 characters)
Modes	CONFIGURATION
Usage	Remark with spaces should be mentioned in double quotes.
Examples	<pre>sonic(config-mac-acl) # remark "Example ACL remark" sonic(config-mac-acl) # no remark</pre>

Releases	3.1 or later
-----------------	--------------

remote-as

Adds a remote AS to the specified BGP neighbor or peer-group.

Command	<code>remote-as {internal external <i>as-num-dot</i>}</code>
Options	<ul style="list-style-type: none"><code>internal</code> — Tag neighbor or peer-group as internal (iBGP)<code>external</code> — Tag neighbor or peer-group as external (eBGP)<code>as-num-dot</code> — Remote AS number (1 to 65535 for 2 byte; 1 to 4294967295 for 4 byte)
Modes	<ul style="list-style-type: none">BGP-NEIGHBORBGP-PEER-GROUP
Usage	Use this command to create the required remote AS configuration. You must configure the remote AS immediately after creating the BGP neighbor.

Examples

```
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# remote-as 65100
```

```
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# remote-as 65200
```

```
sonic(config-router-bgp-neighbor)# no remote-as 65100
sonic(config-router-bgp-pg)# no remote-as 65200
```

Releases

3.0 or later

remove-private-as

Configures BGP to remove private AS numbers from the AS-path in outbound updates to neighbors or peer-groups.

Command `remove-private-as [all] [replace-as]`**Options** • `all` — (Optional) Replace all private ASNs

- `replace-AS` — (Optional) Replace private ASN with local ASN

Modes • NEIGHBOR-ADDRESS-FAMILY

- PEER-GROUP-ADDRESS-FAMILY

Usage

Use this command at the boundary of your BGP network to remove the internal/private AS numbers from outbound route updates. You can optionally choose to replace a private AS number by the local AS number.

Examples

```
sonic(config-router-bgp-neighbor-af)# remove-private-as all
```

```
sonic(config-router-bgp-pg-af)# remove-private-as all
```

```
sonic(config-router-bgp-pg-af)# no remove-private-as all
```

Releases

3.1 or later

renew dhcp-lease

Renews the DHCP lease.

Command `renew dhcp-lease interface {Management mgmt-if-id}`**Options** Management *mgmt-if-id*—Management interface ID**Modes** EXEC**Usage**

Use this command to force the DHCP renewal on the management interface before the lease expires. The Management IP address that is obtained from a DHCP server is automatically renewed when the DHCP lease expires. The amount of lease time is configured on the DHCP server.

Example

```
sonic# renew dhcp-lease interface Management 0
```

Releases

3.1 or later

request-data-size

Sets the ICMP echo request data size.

Command	<code>request-data-size <i>data-size</i></code>
Options	<code><i>data-size</i></code> — ICMP echo request payload size in bytes. The range is from 28 to 1472.
Modes	IP-SLA-ICMP
Usage	Use this command to modify the ICMP echo request packet data size.
Examples	<pre>sonic(config-ipsla-10)# icmp-echo 30.30.1.2 sonic(config-ipsla-10-icmp)# request-data-size 128 sonic(config-ipsla-10-icmp)# no request-data-size</pre>
Releases	3.1 or later

revision

Configures the revision number for the MST.

Command	<code>revision <i>number</i></code>
Options	<code><i>number</i></code> —Enter the MST revision number (0 to 65535; default is 0)
Modes	SPANNING-TREE MST
Usage	Tracking changes to MST region configuration could be done using revision number. All switches in the same MST region should have identical revision numbers.
Examples	<pre>sonic-cli(config)# spanning-tree mst configuration sonic-cli(config-mst)# revision 10 sonic-cli(config)# spanning-tree mst configuration sonic-cli(config-mst)# no revision</pre>
Releases	4.0 or later

roce enable

Enables RoCEv2 with the default RoCEv2/ISCSI lossless buffer settings and the default WRED/ECN, scheduling, and `qos map` configurations defined for a switch

Command	<code>roce enable [force-defaults pfc-priority <i>priority1,priority2</i>]</code>
Options	<ul style="list-style-type: none"><code>force-defaults</code> — Enable RoCEv2 default configurations for lossless buffer pools and lossless buffer profiles, and deletes any existing configurations that conflict with the default settings.<code>pfc-priority <i>priority1,priority2</i></code> — Configure different priority settings on Trident4 (TD4, such as Z9432F-ON), Tomahawk4 (TH4, such as Z9664F-ON), and Tomahawk5 (TH5, such as Z9864F-ON) switches (0-7; default 3,4). Enter two PFC priorities. Separate PFC priority values using a comma (,); for example, 2, 7. The first PFC priority that you enter is mapped to PG3; the second PFC priority that you enter is mapped to PG4. For example, if you enter <code>roce enable pfc-priority 2, 7</code>, priority 2 is mapped to PG3 and priority 7 is mapped to PG4.
Modes	CONFIGURATION
Usage	The <code>roce enable</code> and <code>buffer init lossless</code> commands are mutually exclusive. Use the <code>roce enable</code> command to enable the default QoS map, scheduler, and WRED settings for RoCEv2 operation on a

switch. To remove the RoCEv2 QoS configurations and all lossless buffer initializations, use the `no roce enable` command.

i **NOTE:** In Release 4.4.0 and later, the `roce enable pfc-priority` command allows you to reconfigure the default PFC priority values. The reconfigured PFC priorities are applied across all ports and affect other configurations on the switch, such as QoS maps and port PFC priorities. If you modify the default RoCEv2 settings (QoS maps, scheduler, WRED, port PFC priorities), it is your responsibility to maintain the new configuration. It is possible to revert to the RoCEv2 defaults values by using the `roce enable force-defaults` command.

Examples

```
sonic(config)# roce enable  
sonic(config)# roce enable pfc-priority 1,7
```

Releases

4.1.0 or later

route-map

Configures routing policies

Command

`route-map route-name-name {permit | deny} seq-nu`

Options

- `route-name-name`—Enter the name of the configured route-map
- `seq-nu`—Enter the sequence number

Modes

CONFIGURATION

Usage

Use this command to configure route-map to filter or apply actions to routes using match and set commands.

Examples

```
sonic(config)# route-map rtemap1 permit 20  
sonic(config)# no route-map rtemap1 permit 20
```

Releases

3.0 or later

route-map

Applies an established route-map to either incoming or outgoing routes of a BGP neighbor or peer-group.

Command

`route-map route-name-str {in | out}`

Options

- `route-name-str` — Name of the configured route-map
- `in` — Attaches the route-map as the inbound policy
- `out` — Attaches the route-map as the outbound policy

Modes

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY

Usage

The policy can be applied in an inbound or outbound direction. The policy dictates if a subset of routes need to be filtered out or/and if attributes of some routes needs to be modified.

Examples

```
sonic(config-router-bgp)# neighbor 20.20.20.2  
sonic(config-router-bgp-neighbor)# remote-as 300
```

```

sonic(config-router-bgp-neighbor)# address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af)# route-map rmap_filter_intra_routes in

sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# address-family ipv4 unicast
sonic(config-router-bgp-pg-af)# route-map RM_Blk_192 in

sonic(config-router-bgp)# neighbor 20.20.20.2
sonic(config-router-bgp-neighbor)# remote-as 300
sonic(config-router-bgp-neighbor)# address-family 12vpn evpn
sonic(config-router-bgp-neighbor-af)# route-map rmap_filter_intra_routes in

sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# address-family 12vpn evpn
sonic(config-router-bgp-pg-af)# route-map RM_Blk_192 in

sonic(config-router-bgp-neighbor-af)# no route-map rmap_filter_intra_routes in
sonic(config-router-bgp-pg-af)# no route-map RM_Blk_192 in

```

Releases 3.0 or later

route-map delay-timer

Sets the route-map delay interval.

Command `route-map delay-timer delaytm`

Options `delay-timer delaytm` — Delay timer value in seconds (0 to 600; no default)

Modes ROUTER-BGP

Usage Use this command to set the interval in seconds to wait before processing a route-map change. You can apply a route map to filter the exchange of incoming and outgoing BGP IPv4 or IPv6 routes. Configure the time interval (in seconds) to wait before processing received filtered routes in the BGP routing table.

Examples

```

sonic(config-router-bgp)# route-map delay-timer 60

sonic(config-router-bgp)# no route-map delay-timer

```

Releases 3.0 or later

route-reflector allow-outbound-policy

Sets the outbound policy for route-reflector neighbors.

Command `route-reflector allow-outbound-policy`

Options None

Modes ROUTER-BGP

Usage Use this command for route-map to work on reflected routes in the route-reflector.

Examples

```

sonic(config-router-bgp)# route-reflector allow-outbound-policy

sonic(config-router-bgp)# no route-reflector allow-outbound-policy

```

Releases 3.0 or later

route-reflector-client

Configures a BGP neighbor or neighbors in a peer-group as a member of a route-reflector cluster.

Command route-reflector-client

Options None

Modes

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY

Usage This command will implicitly make the local router a route-reflector server.

Examples

```
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af) # route-reflector-client
```

```
sonic(config-router-bgp) # peer-group PG_Int
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # route-reflector-client
```

```
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family 12vpn evpn
sonic(config-router-bgp-neighbor-af) # route-reflector-client
```

```
sonic(config-router-bgp) # peer-group PG_Int
sonic(config-router-bgp-pg) # address-family 12vpn evpn
sonic(config-router-bgp-pg-af) # route-reflector-client
```

```
sonic(config-router-bgp-neighbor-af) # no route-reflector-client
sonic(config-router-bgp-pg-af) # no route-reflector-client
```

Releases 3.0 or later

route-scale routes

Increases (scales) the maximum number of IPv4 and IPv6 route prefixes supported in the forwarding table.

Command route-scale routes {max | max-v6}

Options

- max — Scale IPv4 routes.
- max-v6 — Scale IPv6 routes.

(i) NOTE: The route-scale max-v6 profile is not supported on Dell PowerSwitch platforms.

Modes SWITCH-RESOURCE

Usage This command enables Algorithmic Lower Prefix Match (ALPM) and carves out more space for IPv4 or IPv6 routes. Use this command only when you want to increase the number of supported routes.

Examples

```
sonic(config) # switch-resource
sonic(config-switch-resource) # route-scale routes max
```

```
sonic(config-switch-resource) # no route-scale routes
```

Releases 3.2 or later

route-scale hosts

Increases (scales) the maximum number of hosts supported on a switch.

Command	route-scale hosts {layer2-layer3 layer2-layer3-balanced}
Options	<ul style="list-style-type: none">• layer2-layer3 — Enable Hosts layer2-layer3 mode on a S5232F-ON, S5248F-ON, or S5296F-ON switch.• layer2-layer3-balanced — Enable Hosts layer2-layer3-balanced mode on a Z9432F-ON or S5448F-ON switch.
Modes	SWITCH-RESOURCE
Usage	Use the <code>route-scale hosts</code> command to scale MAC address and L3 host entries on a supported switch. For more information about route-scaling hosts, see L2/L3 host and route scaling in the <i>Enterprise SONiC User Guide</i> .
Examples	<pre>sonic# configure terminal sonic(config)# switch-resource sonic(config-switch-resource)# route-scale hosts layer2-layer3</pre>
Releases	3.5 or later

route-server-client

Configures BGP neighbors or neighbors in a peer-group as route server client.

Command	route-server-client
Options	None
Modes	NEIGHBOR-ADDRESS-FAMILY
Usage	Use this command to configure the neighbor as route server client. BGP attributes (AS path, next hop, MED) announced to that neighbor are not modified.
Example	<pre>sonic(config-router-bgp)# neighbor 20.20.20.2 sonic(config-router-bgp-neighbor)# remote-as 300 sonic(config-router-bgp-neighbor)# address-family ipv4 unicast sonic(config-router-bgp-neighbor-af)# route-server-client sonic(config-router-bgp)# peer-group PG_Int sonic(config-router-bgp-pg)# address-family ipv4 unicast sonic(config-router-bgp-pg-af)# route-server-client sonic(config-router-bgp)# neighbor 20.20.20.2 sonic(config-router-bgp-neighbor)# remote-as 300 sonic(config-router-bgp-neighbor)# address-family l2vpn evpn sonic(config-router-bgp-neighbor-af)# route-server-client sonic(config-router-bgp)# peer-group PG_Int sonic(config-router-bgp-pg)# address-family l2vpn evpn sonic(config-router-bgp-pg-af)# route-server-client sonic(config-router-bgp-neighbor-af)# no route-server-client sonic(config-router-bgp-pg-af)# no route-server-client</pre>
Releases	3.0 or later

route-target

Configures the route-target or community to attach while exporting routes from the current VRF for a specified VNI.

Command `route-target rttype rt`

- Options**
- *rttype* — Advertise options; both, import, or export
 - *rt* — Route target to match in A.B.C.D:NN, MMM:NN, or NN:MMMM format

Modes

- BGP-ADDRESS-FAMILY
- BGP-ADDRESS-FAMILY-VNI

Usage Use this command to specify the route-target to be matched when importing routes into the current VRF, or for a specific address-family or VNI.

Examples

```
sonic(config)# router bgp 100 vrf Vrf1
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)# route-target import 11:11
sonic(config-router-bgp-af)# route-target export 22:22
sonic(config-router-bgp-af)# route-target both 33:33
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# address-family l2vpn evpn
sonic(config-router-bgp-af)# vni 100
sonic(config-router-bgp-af-vni)# route-target import 11:11
sonic(config-router-bgp-af-vni)# route-target export 22:22
sonic(config-router-bgp-af-vni)# route-target both 33:33
```

```
sonic(config-router-bgp-af)# no route-target import 11:11
sonic(config-router-bgp-af)# no route-target export 22:22
sonic(config-router-bgp-af)# no route-target both 33:33
```

Releases 3.0 or later

router bgp

Assigns an AS number and enters ROUTER-BGP mode.

Command `router bgp {as-num-dot {[vrf] vrf-name}}`

- Options**
- *as-num-dot* — AS number range (1 to 65535 in 2 byte; 1 to 4294967295 in 4 byte)
 - *vrf vrf-name* — (Optional) VRF instance name (up to 15 characters)

Modes CONFIGURATION

Usage Use this command to create a BGP routing instance in a VRF. If the VRF key is not specified, the default VRF is used. Only one AS number is supported per system. If you enter a 4-byte AS number, 4-byte AS support is automatically enabled.

Examples

```
sonic(config)# router bgp 65300
```

```
sonic(config)# no router bgp
```

Releases 3.0 or later

router ospf

Configures an OSPFv2 router within a VRF.

Command `router ospf [Vrf vrf-name]`

Options	vrf <i>vrf-name</i> — (Optional) VRF name prefixed by Vrf (up to 15 characters)
Modes	CONFIGURATION
Usage	Use this command to enter ROUTER-OSPF mode. If the VRF name is not specified, the default VRF is used.
Examples	<pre>sonic(config)# router ospf</pre> <pre>sonic(config)# router ospf vrf Vrf-blue</pre> <pre>sonic(config)# no router ospf</pre>
Releases	3.1 or later

router-id

Configures the router ID for an instance of BGP protocol.

Command	router-id <i>ip-addr</i>
Options	<i>ip-addr</i> — IPv4 address in A.B.C.D format
Modes	ROUTER-BGP
Usage	BGP automatically selects one interface IP address as the router ID if not configured explicitly. Changing the router-id resets the peer-sessions.
Examples	<pre>sonic(config)# router bgp 65300</pre> <pre>sonic(config-router-bgp)# router-id 163.134.6.97</pre> <pre>sonic(config-router-bgp)# no router-id</pre>
Releases	3.0 or later

S to show priority-group commands

Topics:

- sampler
- sampling-interval
- scheduler-policy
- send-community
- seq
- seq
- server-key
- service-policy
- session
- session-timeout
- session-vrf
- set ars disable
- set ars-object
- set as-path
- set comm-list delete
- set community
- set copp-action
- set dscp
- set extcommunity
- set interface
- set ip
- set ip
- set ipv6
- set ipv6 next-hop
- set local-preference
- set metric
- set mirror-session
- set origin
- set pcp
- set traffic-class
- set trap-action
- set trap-priority
- set trap-queue
- set weight
- sflow agent-id
- sflow collector
- sflow enable
- sflow polling-interval
- sflow sampling-rate
- show aaa
- show access-group
- show alarm
- show ars bind
- set ars disable
- show ars nhg-statistics
- show ars object
- show ars port-profile

- show ars port-quality
- show ars profile
- show audit-log
- show auditd-system log
- show auditd-system rules
- show authentication
- show authentication authentication-history
- show authentication clients
- show authentication interface
- show ip rest authentication
- show ip telemetry authentication
- show bfd peer
- show bfd peer counters
- show bfd peers
- show bfd profile
- show bgp all
- show bgp as-path-access-list
- show bgp community-list
- show bgp ext-community-list
- show bgp ipv4
- show bgp ipv6
- show bgp l2vpn evpn es
- show bgp l2vpn evpn es-evi
- show bgp l2vpn evpn es-vrf
- show bgp l2vpn evpn next-hops
- show bgp l2vpn evpn route
- show bgp l2vpn evpn route detail type
- show bgp l2vpn evpn route rd
- show bgp l2vpn evpn route type
- show bgp l2vpn evpn route vni
- show bgp l2vpn evpn summary
- show bgp l2vpn evpn vni
- show buffer interface
- show buffer-pool
- show buffer profile
- show ca-crypto cert
- show cable-diagnostics
- show class-map
- show clock
- show config-key password-encrypt
- show configuration
- show consistency-check status
- show copp
- show core config
- show core info
- show core list
- show crm
- show crm resources
- show crm thresholds
- show crypto ca-cert file
- show crypto cert
- show crypto cert file
- show crypto security-profile
- show crypto ssh-key
- show crypto trust-store
- show current

- show database map
- show device
- show dot1x
- show dot1x detail
- show dropcounters capabilities
- show dropcounters configuration
- show dropcounters configuration detail
- show errdisable link-flap
- show errdisable recovery
- show error-database
- show event
- show evpn
- show evpn arp-cache vni
- show evpn arp-cache vni all
- show evpn es
- show evpn es startup-delay
- show evpn es-evi
- show evpn I2-nh
- show evpn mac vni
- show evpn mac vni all
- show evpn next-hops vni
- show evpn next-hops vni all
- show evpn rmac vni
- show evpn rmac vni all
- show evpn vni
- show evpn vni detail
- show fips status
- show hardware tcam allocation
- show hardware tcam key-profile
- show histogram memory system
- show hosts
- show image firmware
- show image firmware status
- show image list
- show image patch history
- show image patch list
- show image patch status
- show image status
- show in-memory-logging
- show in-memory-logging count
- show in-memory-logging lines
- show interface
- show interface advertise
- show interface breakout
- show interface counters
- show interface description
- show interface dropcounters
- show interface Ethernet
- show interface link-training
- show interface loopback
- show interface management
- show interface-naming
- show interface phy counters
- show interface phy status
- show interface portchannel
- show interface port-locator

- show interface status
- show interface transceiver
- show interface transceiver wattage
- show interface transceiver summary
- show interface unreliable-los status
- show interface vlan-mappings
- show interface vlan-mappings dot1q-tunnel
- show ip access-group
- show ip access-lists
- show ip arp
- show ip arp interface
- show ip dhcp snooping
- show ip dhcp snooping binding
- show ip dhcp snooping statistics
- show ip dhcp snooping statistics detail
- show ip dhcp-relay
- show ip forward-protocol
- show ip helper-address
- show ip helper-address statistics
- show ip igmp snooping
- show ip igmp groups
- show ip igmp interface
- show ip igmp join
- show ip igmp sources
- show ip igmp statistics
- show ip igmp vrf
- show ip interfaces
- show ip load-share
- show ip mroute
- show ip ospf
- show ip ospf graceful-restart helper
- show ip ospf neighbor detail
- show ip ospf route
- show ip pim
- show ip prefix-list
- show ip rest
- show ip rest authentication
- show ip rest cipher-suite
- show ip route
- show ip sla
- show ip static-anycast-gateway
- show ip telemetry
- show ip vrf
- show ipv6 access-group
- show ipv6 access-lists
- show ipv6 dhcp snooping
- show ipv6 dhcp snooping binding
- show ipv6 dhcp snooping statistics
- show ipv6 dhcp snooping statistics detail
- show ipv6 dhcp-relay
- show ipv6 interfaces
- show ipv6 nd ra-interfaces
- show ipv6 neighbors
- show ipv6 neighbors interface
- show ipv6 prefix-list
- show ipv6 route

- show ipv6 static-anycast-gateway
- show kdump files
- show kdump log
- show kdump memory
- show kdump num-dumps
- show kdump status
- show ldap-server
- show link state tracking
- show lldp neighbor
- show lldp statistics
- show lldp table
- show locator-led chassis
- show logging
- show logging count
- show logging filter
- show logging lines
- show logging servers
- show mab
- show mab interface
- show mac access-group
- show mac access-lists
- show mac address-table
- show mac address-table address
- show mac address-table aging-time
- show mac address-table count
- show mac address-table dynamic
- show mac address-table interface
- show mac address-table static
- show mac address-table Vlan
- show mac dampening
- show mac dampening-disabled-ports
- show mclag brief
- show mclag mac remote
- show mclag interface
- show mclag peer-gateway-interfaces
- show mclag separate-ip-interfaces
- show mirror-session
- show nat
- show neighbor-suppress-status
- show ntp associations
- show ntp global
- show ntp server
- show object-groups
- show pbf next-hop-group
- show pbf next-hop-group status interface
- show pbf next-hop-group status Switch
- show pbf replication-group
- show pbf replication-group status interface
- show pbf replication-group status Switch
- show pending
- show platform environment
- show platform fanstatus
- show platform firmware
- show platform firmware detail
- show platform psustatus
- show platform psusummary

- show platform sbstatus
- show platform ssdhealth
- show platform syseprom
- show platform temperature
- show platform temperature detail
- show poe
- show poe port configuration
- show poe port info
- show policy-map
- show PortChannel summary
- show port-group
- show port-security
- show port-security interface
- show priority-flow-control
- show priority-group

sampler

Creates a sampler session that co-relates a sampling rate with a session name.

Command	<code>sampler <i>name</i> rate <i>sampler_rate</i></code>
Options	<ul style="list-style-type: none"> • <i>name</i> — Sampler name (up to 63 characters) • <i>rate-name</i> — Rate name (1 to 4294967295)
Modes	CONFIGURATION
Usage	The sample session is identified by the name and can be used by multiple features to indicate sampling configuration. One packet in every rate packets will be sampled.
Examples	<pre>sonic(config-tam)# sampler s34 rate 1000 sonic# show tam samplers Name Sample Rate ----- ----- s1 1 s34 1000</pre> <pre>sonic(config)# no sample s34</pre>
Releases	3.1 or later

sampling-interval

Sets the data sampling interval for quality measure computation.

Command	<code>sampling-interval <i>sampling-interval</i></code>
Options	<i>sampling-interval</i> —The data sampling interval in microseconds. The range is from 1 to 255. The default value is 16 microseconds.
Modes	ARS-PROFILE
Usage	Use this command to set the data sampling interval for quality measure computation.
Examples	<pre>sonic(config-ars-profile)# sampling-interval 8</pre>
Releases	4.4.0 or later

scheduler-policy

Configures the scheduler policy of the interface.

Command `scheduler-policy sp_name`

Options `sp_name`—Enter the scheduler policy name (up to 32 characters)

Modes INTERFACE

Usage Use this command to apply the scheduler policy to the physical and CPU interfaces.

Examples

```
sonic# configure terminal
sonic(config)# interface Ethernet 28
sonic(config-if-Ethernet28)# scheduler-policy scheduler_cpu
```

```
sonic(config-if-Ethernet28)# no scheduler-policy
```

Releases 3.1 or later

send-community

Sends a community attribute to a BGP neighbor or peer-group.

Command `send-community {standard | extended | both | large | all | none}`

Options • standard — Standard community attribute

• extended — Extended community attribute

• both — Both standard and extended community attributes

• large — Large community attributes

• all — All community attributes

• none — No attributes

Modes ADDRESS-FAMILY

Usage Use this command to enable sending of community attribute to a BGP neighbor or peer-group. A community attribute indicates that all routes with the same attribute belong in the same community grouping. The command option provides the flexibility to enable sending of standard, extended, and large communities.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 20.20.20.2
sonic(config-router-bgp-neighbor) # remote-as 300
sonic(config-router-bgp-neighbor) # address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af) # send-community
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Int
sonic(config-router-bgp-pg) # address-family ipv4 unicast
sonic(config-router-bgp-pg-af) # send-community
```

```
sonic(config-router-bgp-neighbor-af) # no send-community
sonic(config-router-bgp-pg-af) # no send-community
```

Releases 3.0 or later

seq

Assigns a sequence number to deny or permit IPv4 or IPv6 addresses while creating the filter.

Command

```
seq seq-no {{deny | discard | permit | transit | do-not-nat | {remark  
remark-val}} {ip-protocol-val | icmp | ip | tcp | udp} {src-ip-prefix |  
src-ip-any | {src-ip-host src-ip}} {[src-eq src-port1]} | {[src-gt src-  
port1]} | {[src-lt src-port1]} | {[src-range src-port1 src-port2]}} {dst-  
ip-prefix | dst-ip-any | {dst-ip-host dst-ip}} {[dst-eq dst-port1]} |  
{[dst-gt dst-port1]} | {[dst-lt dst-port1]} | {[dst-range dst-port1 dst-  
port2]}} {[dscp {default | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 |  
af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |  
af42 | af43 | ef | voice-admit | dscp-val]} [tcp-established] {[fin] |  
[not-fin]} {[syn] | [not-syn]} {[rst] | [not-rst]} {[psh] | [not-psh]}  
|[ack] | [not-ack]} {[urg] | [not-urg]} {[type TYPE]} {[code CODE]}  
{[vlan vlan-val]} {[remark remark-val]}}
```

Options

- *seq-no* — Sequence number to identify the ACL for editing and sequencing number
- *remark-val* — Remark value (up to 256 characters)
- *ip-protocol-val* — IP protocol value
- *src-ip-prefix* — Source IP prefix in A.B.C.D/mask or A::B/mask format
- *src-ip* — Source IP in A.B.C.D or AA::NN format
- *src-port1* — (Optional) Source port 1 value
- *src-port2* — (Optional) Source port 2 value
- *dst-ip-prefix* — Destination IP prefix in A.B.C.D/mask or A::B/mask format
- *dst-ip* — Destination IP in A.B.C.D or A::B format
- *dst-port1* — (Optional) Destination port 1 value
- *dst-port2* — (Optional) Destination port 2 value
- *dscp-val* — (Optional) DSCP value
- *TYPE* — (Optional) Type value
- *CODE* — (Optional) Code value
- *vlan-val* — (Optional) VLAN ID (1 to 4094)

Modes

- IPV4-ACCESS-LIST
- IPV6-ACCESS-LIST

Usage

The rule will be created if there is no existing rule with the same sequence number. An ACL rule cannot be updated. You must first delete the rule, then add the rule with new parameters.

Examples

```
sonic(config-ip-acl)# seq 10 permit ip host 10.1.1.1 host 20.1.1.1
```

```
sonic(config-ipv6-acl)# seq 100 permit ipv6 host abcd::1 host bcde::1
```

```
sonic(config-ip-acl)# no seq 10
```

Releases

3.1 or later

seq

Assigns a sequence number to deny or permit IPv4 addresses while creating the filter.

Command

```
seq seq-no {{deny | discard | permit | transit | do-not-nat | {remark  
remark-val}} {{src-mac-addr src-mac-mac} | src-mac-any | {src-mac-host  
src-mac-addr}} {{dst-mac-addr dst-mac-mask} | dst-mac-any | {dst-mac-host  
dst-mac-addr}} {[ethertype-ip] | [ethertype-ipv6] | [ethertype-arp] |  
[ETHERTYPE]} {[pcp {pcp-be | pcp-bk | pcp-ee | pcp-ca | pcp-vi | pcp-vo  
| pcp-ic | pcp-nc | {pcp-val {[pcp-mask pcp-val-mask]}}}} {[dei dei-val]  
{[vlan vlan-val]} {[remark remark-val]}}}}
```

Options	<ul style="list-style-type: none"> • <i>seq-no</i> — Sequence number to identify the ACL for editing and sequencing number • <i>remark-val</i> — Remark value (up to 256 characters) • <i>src-mac-address</i> — Source MAC address • <i>src-mac-mac</i> — Source MAC address • <i>dst-mac-addr</i> — Destination MAC address • <i>dst-mac-mac</i> — Destination MAC address • <i>ETHERTYPE</i> — (Optional) Ethertype (0x600 to 0xffff) • <i>pcp-val</i> — (Optional) PCP value (0 to 7) • <i>pcp-val-mask</i> — (Optional) PCP value mask (0 to 7) • <i>dei-val</i> — (Optional) DEI value (0 to 1) • <i>vlan-val</i> — (Optional) VLAN ID (1 to 4094)
Modes	MAC-ACCESS-LIST
Usage	The rule will be created if there is no existing rule with the same sequence number. An ACL rule cannot be updated. You must first delete the rule, then add the rule with new parameters.
Examples	<pre>sonic(config-mac-acl)# seq 10 permit host 00:00:10:00:00:01 host 00:00:20:00:00:01</pre> <pre>sonic(config-mac-acl)# no seq 10</pre>
Releases	3.1 or later

server-key

Configure a global shared secret that is used for all dynamic authorization clients that do not have an individual shared secret key configured.

Command	server-key <i>key-string</i> [encrypted]
Options	<ul style="list-style-type: none"> • <i>key-string</i>—Specify the key string. • <i>encrypted</i>—Specify that the server key is encrypted.
Modes	RADIUS-DA
Usage	Use this command to configure a global shared secret that is used for all dynamic authorization clients that do not have an individual shared secret key configured. The encrypted keyword is hidden.
Examples	<pre>sonic(config-radius-da)# server-key test123</pre>
Releases	4.1.0 or later

service-policy

Applies an ingress or egress service policy.

Command	service-policy type {qos monitoring forwarding acl-copp} {in out} <i>policy-name</i>
Options	<ul style="list-style-type: none"> • <i>qos</i>—QoS • <i>monitoring</i>—Monitoring • <i>forwarding</i>—Forwarding • <i>acl-copp</i>—CoPP • <i>in</i>—In • <i>out</i>—Out • <i>policy-name</i>—FBS policy name (up to 63 characters)
Modes	INTERFACE

Usage Apply a policy map on the ingress CPU interface. To remove a policy from an interface, enter the no version of the command. You can only apply an ACL-CoPP policy on the CPU.

Examples

```
sonic# configure terminal  
sonic(config)# interface Vlan 100  
sonic(config-if-Vlan100)# service-policy type forwarding in policy_vrf  
  
sonic(config-if-Vlan100)# no service-policy type forwarding in
```

Releases 3.1 or later

session

Creates an inband flow analyzer (IFA) monitoring session.

Command `session session_name flowgroup flowgroup_name [collector collector_name] [sampler sampler_name] node-type node_type`

Options

- *session_name* — Session name
- *flowgroup_name* — Flow-group name
- *collector_name* — (Optional) Collector name
- *sampler_name* — (Optional) Sampler name
- *node_type* — Node role; select ingress or egress

Modes

- TAM-IFA
- DROP-MONITOR
- TAIL-STAMPING

Usage Use this command to create an IFA monitoring session that is associated with a defined flow-group. Use [show tam ifa sessions](#) to view the TAM IFA session configuration. Use [show tam drop-monitor sessions](#) to view the TAM drop-monitor session configuration. Use [show tam tail-stamping sessions](#) to view the TAM tail stamping session configuration.

Examples

```
sonic(config-tam-ifia)# session ss1 flowgroup f9 sampler s1 node-type ingress  
  
sonic(config-tam-dm)# session ss91 flowgroup f9 collector c2 sampler s1  
  
sonic(config-tam-ts)# session ss66 flowgroup f9 node-type ifa  
  
sonic(config-tam-ifia)# no session ss1
```

Releases 3.1 or later

session-timeout

Sets the MLAG session timeout value.

Command `session-timeout ST`

Options `session-timeout ST`—Enter the session timeout value in seconds (1 to 3600; default is 30)

Modes MLAG-DOMAIN

Usage Session timeout value is the time to wait before shutting down an MLAG session with a remote peer if no keepalive reply is received.

Examples

```
sonic# configure terminal  
sonic(config)# mclag domain 100  
sonic(config-mclag-domain-100)# session-timeout 100  
  
sonic(config-mclag-domain-100)# no session-timeout
```

Releases

3.0 or later

session-vrf

Assign an MLAG domain to the management VRF or a nondefault VRF.

Command

`session-vrf vrf-name`

Options

`session-vrf vrf-name` — Assign an MLAG domain to the management VRF or a nondefault VRF.

Modes

MCLAG-DOMAIN

Usage

Before assigning an MLAG domain to a VRF, create the VRF. If you do not use the `session-vrf` option, MLAG is created in the default VRF. Use the `no session-vrf` command for the MLAG domain to use the Default VRF.

Examples

```
sonic(config)# ip vrf VRF-Red  
sonic(config)#  
sonic(config)# mclag domain 1  
sonic(config-mclag-domain-1)# session-vrf VRF-Red  
  
sonic(config)# ip vrf mgmt  
sonic(config)#  
sonic(config)# mclag domain 1  
sonic(config-mclag-domain-1)# session-vrf mgmt
```

Releases

4.2 or later

set ars disable

Disables ARS forwarding for the flows.

Command

`set ars disable`

Options

None

Modes

POLICY-MAP

Usage

Use this command to disable the ARS forwarding for the classified traffic.

Example

```
sonic(config)# policy-map policy_ars type forwarding  
sonic(config-policy-map)# class class_disable_ars priority 10  
sonic(config-policy-map-flow)# set ars disable  
sonic(config-policy-map-flow)# no set ars disable
```

Releases

4.4.0 or later

set ars-object

Sets ARS object to the routes.

Command

`set ars-object object-name`

Options

- *object-name*—ARS object name.

Modes**Usage**

Create a route-map with a permit rule and set an ARS object as action. If your configuration already contains the Loopback 0 interface that is assigned with an IP or IPv6 address, create a route-map with these standard names RM_SET_SRC and RM_SET_SRC6 and use the `set ars-object` command and specify the ARS object name. Set the route-map in the router filter configuration using the `ip protocol any route-map route_map_name [vrf vrf_name]` or `ipv6 protocol any route-map route_map_name [vrf vrf_name]` command.

Example

```
sonic(config)# route-map ars-map permit 10
sonic(config-route-map)# set ars-object default
sonic(config-route-map)# exit
```

If Loopback 0 is configured, use the following route-map configuration to ensure that the ARS object is correctly set for the NHG of routes that are learned through BGP.

```
sonic(config)# route-map RM_SET_SRC permit 10
sonic(config-route-map)# set ars-object default
sonic(config)# route-map RM_SET_SRC6 permit 10
sonic(config-route-map)# set ars-object default
```

Releases

4.4.0 or later

set as-path

Sets the BGP AS path attribute.

Command

```
set as-path {prepend {as-number_list}}
```

Options

prepend as-number_list—Enter the comma-separated AS number list

Modes

ROUTE-MAP

Usage

Use this command to set the AS path to prepend.

Examples

```
sonic(config)# route-map map1 permit 10
sonic(config-route-map)# set as-path prepend 6000
```

```
sonic(config-route-map)# set as-path prepend 6500,6510,6520
```

```
sonic(config-route-map)# no set as-path prepend
```

Releases

3.0 or later

set comm-list delete

Specifies the BGP community to be removed from the community attribute of a matching inbound or outbound route update.

Command

```
set comm-list community-list-name delete
```

Options

community-list-name—Enter a standard BGP community-list name.

Modes

ROUTE-MAP

Usage

When a BGP route has the specified *community-list-name*, the community value is removed from the community attribute in the route update. When all community values are configured in a route map with the `set comm-list delete` command, updates for the BGP community attribute in matching routes are not saved.

Examples

```
sonic(config)# route-map map1 permit 10
sonic(config-route-map)# set comm-list COM1 delete
```

To undo the community name removed with the `set comm-list community-list-name delete` command, enter the `no set comm-list` command; for example:

```
sonic(config)# bgp community-list standard COM1 permit 45:56
sonic(config)# route-map RTMAP1 permit 10
sonic(config-route-map)# set comm-list COM1 delete
sonic(config-route-map)# do show route-map
Route map RTMAP1:
    permit, sequence 10
    Match clauses:
    Set clauses:
        comm-list COM1 delete
    Call clauses:
    Actions:
        Exit routemap

sonic(config-route-map)# no set comm-list
sonic(config-route-map)# do show route-map
Route map RTMAP1:
    permit, sequence 10
    Match clauses:
    Set clauses:
    Call clauses:
    Actions:
        Exit routemap
```

Releases

4.0.1 or later

set community

Sets the community attribute in BGP updates.

Command

```
set community {{[comm-num1 {[comm-num2 {[comm-num3 {[comm-num4 {[comm-num5
[local-as] [no-advertise] [no-export] [no-peer] [additive]}] [local-as]
[no-advertise] [no-export] [no-peer] [additive]}]} [local-as] [no-advertise]
[no-export] [no-peer] [additive]}]} [local-as] [no-advertise] [no-export]
[no-peer] [additive]}]} [local-as] [no-advertise] [no-export] [no-peer]
[additive]} | {[local-as [no-advertise] [no-export] [no-peer] [additive]}]
| {[no-advertise [local-as] [no-export] [no-peer] [additive]}]} | {[no-
export [local-as] [no-advertise] [no-peer] [additive]}]} | {[no-peer [local-
as] [no-advertise] [no-export] [additive]}]}
```

Options

- *comm-num1*—(Optional) Community name in AA::NN format
- *comm-num2*—(Optional) Community name in AA::NN format
- *comm-num3*—(Optional) Community name in AA::NN format
- *comm-num4*—(Optional) Community name in AA::NN format
- *comm-num5*—(Optional) Community name in AA::NN format

Modes

ROUTE-MAP

Usage

Use this command to set the BGP community attribute to the BGP routes.

Examples

```
sonic(config)# route-map map1 permit 10
sonic(config-route-map)# set community 200:300 local-as
```

```
sonic(config-route-map)# no set community local-as
```

Releases

3.1 or later

set copp-action

Binds a CoPP action group to the classifier.

Command	set copp-action <i>copp-action-name</i>
Options	<i>copp-action-name</i> —Specify a CoPP action name (up to 63 characters)
Modes	POLICY-MAP
Usage	Use this command to bind a custom CoPP action group to the class map in the CoPP policy.
Example	<pre>sonic(config)# policy-map copp-system-policy type copp sonic(config-policy-map)# class copp-system-arp sonic(config-policy-map-flow)# set copp-action copp-system-arp</pre>
Releases	3.1 or later

set dscp

Sets DSCP remarking.

Command	set dscp <i>dscp-value</i>
Options	<i>dscp-value</i> —DSCP value (0 to 63)
Modes	POLICY-MAP
Usage	Use this command to set the DSCP value in IP packet headers. For example, set dscp 10 resets the six most significant bits of the DiffServ field to 001 010 for low drop probability. For descriptions of other DSCP values, see RFC 2475. To remove the configured DSCP remarking value, enter the no set dscp command.
Examples	<pre>sonic(config)# policy-map change_dscp_test type qos sonic(config-policy-map)# class my_traffic_test priority 100 sonic(config-policy-map-flow)# set dscp 10</pre> <pre>sonic(config-policy-map-flow)# no set dscp</pre>
Releases	3.1 or later

set extcommunity

Sets the extended community attributes in a route-map for BGP updates.

Command	set extcommunity {{rt <i>value</i> } {soo <i>value</i> }}
Options	<ul style="list-style-type: none">• <i>rt value</i>—Route target value in ASN:NN_OR_IP-ADDRESS:NN format• <i>soo value</i>—Route origin or site-of-origin value
Modes	ROUTE-MAP
Usage	Use this command to set the route target-extended community or site-of-origin extended community to BGP routes.
Examples	<pre>sonic(config)# route-map set_ext_community_to_routes permit 1 sonic(config-route-map)# set extcommunity so 65000:1 sonic(config-route-map)# set extcommunity rt 10.10.10.2:325</pre> <pre>sonic(config-route-map)# no set extcommunity rt 10.10.10.2:325</pre>

Releases	3.0 or later
-----------------	--------------

set interface

Configures an IP interface for forwarding flow.

Command	<code>set interface {null {Ethernet <i>port-id</i>} {PortChannel <i>portchannel-id</i>} } [<i>priority priority-value</i>]</code>
Options	<ul style="list-style-type: none"> • <i>port-id</i> — Port ID (0 to 255) • <i>portchannel-id</i> — PortChannel ID (1 to 128) • <i>priority-value</i> — (Optional) Priority value
Modes	POLICY-MAP
Usage	Egress interfaces configuration is valid only if the classifier uses MAC/L2 ACL for match. Only L2 switched traffic is forwarded to the configured egress interface. Combining egress interface with IPv4 or IPv6 next-hops is not permitted. Drop action (set interface to null) if configured is of the lowest priority and is chosen if none of the configured next-hops or egress interfaces can be used for forwarding.
Examples	<pre>sonic(config) # policy-map policy_vrf type forwarding sonic(config-policy-map)# class class10 priority 10 sonic(config-policy-map-flow)# set interface Eth 1/9 sonic(config-policy-map-flow)# set interface null</pre> <pre>sonic(config-policy-map-flow)# no set interface null</pre>

Releases	3.1 or later
-----------------	--------------

set ip

Configures an IPv4 address as the next-hop.

Command	<code>set ip next-hop <i>ip-addr</i></code>
Options	<i>next-hop ip-addr</i> —IP address in A.B.C.D format
Modes	ROUTE-MAP
Usage	Use this command to set the next hop for the BGP routes.
Examples	<pre>sonic(config) # route-map change_nh permit 1 sonic(config-route-map)# set ip-next-hop 10.10.10.2</pre> <pre>sonic(config-route-map)# no set ip next-hop 10.10.10.2</pre>

Releases	3.0 or later
-----------------	--------------

set ip

Configures the IP next-hop for the forwarding flow.

Command	<code>set ip {{next-hop <i>ip-address</i> {[vrf <i>vrf-name</i> default]}} {next-hop-group <i>pbf-nh-grp</i>} {replication-group <i>pbf-repl-grp</i>} } [<i>priority priority-value</i>]</code>
Options	<ul style="list-style-type: none"> • <i>ip-address</i> — IP address in A.B.C.D format • <i>vrf-name</i> — (Optional) VRF name prefixed by Vrf (up to 15 characters) • <i>pbf-nh-grp</i> — Next-hop group name (up to 15 characters)

- *pbf-repl-grp* — Replication group of next-hop
- *priority-value* — (Optional) Priority of the next-hop (1 to 65535; default 0)

Modes

POLICY-MAP

Usage

If the VRF name is not specified, it is derived from the VRF of the interface on which the policy is applied or the default is used globally. The next-hop with the higher priority is picked up for forwarding first. If more than one next-hop has the same priority, the next-hop which is configured first is used.

Examples

```
sonic(config)# policy-map policy_vrf type forwarding
sonic(config-policy-map)# class class_permit_ip priority 10
sonic(config-policy-map)# set ip next-hop 12.12.2.2 vrf Vrf-BLUE priority 20

sonic(config-policy-map)# no set ip next-hop 12.12.2.2 vrf Vrf-BLUE priority 20

sonic(config)# policy-map pmap-ftb-1 type forwarding
sonic(config-policy-map)# class cmap-ipv4-ftb priority 100
sonic(config-policy-map-flow)# set ip replication-group rg-ipv4-anycast-1
```

Releases

3.2 or later

set ipv6

Sets an IPv6 address as the next-hop.

Command

```
set ipv6 {{next-hop ip-address {[vrf {vrf-name | default}]} } | {next-hop-group pbf-nh-grp} } [priority priority-value]
```

Options

- *ip-address* — IPv6 address in A::B format
- *vrf-name* — VRF name prefixed by Vrf (up to 15 characters)
- *pbf-nh-grp* — Next-hop group name (up to 15 characters)
- *priority-value* — Priority value (1 to 65535; default 0)

Modes

POLICY-MAP

Usage

If the VRF name is not specified, it is derived from the VRF of the interface on which the policy is applied or default is used globally. The next-hop with the higher priority is picked up for forwarding first. If more than one next-hop has the same priority, then the next-hop which is configured first is used.

Examples

```
sonic(config)# policy-map policy_vrf type forwarding
sonic(config-policy-map)# class class_permit_ipv6 priority 10
sonic(config-policy-map)# set ipv6 next-hop 1211::2 priority 20

sonic(config-policy-map)# no set ipv6 next-hop 1211::2 priority 20
```

Releases

3.1 or later

set ipv6 next-hop

Sets IPv6 next-hop for the forwarding flow.

Command

```
set ipv6 next-hop {{next-hop ip-address {[vrf vrf-name | default]}} } | {next-hop-group pbf-nh-grp} | {replication-group pbf-repl-grp} } [priority priority-value]
```

Options

- *ip-address* — IPv6 address in A::B format
- *vrf-name* — (Optional) VRF name prefixed by Vrf (up to 15 characters)
- *pbf-nh-grp* — Next-hop group name (up to 15 characters)
- *pbf-repl-grp* — Replication group of next-hop
- *priority-value* — (Optional) Priority of the next-hop (1 to 65535; default is 0)

Modes	ROUTE-MAP
Usage	If the VRF name is not specified, it is derived from the VRF of the interface on which the policy is applied or the default is used globally. The next-hop with the higher priority is picked up for forwarding first. If more than one next-hop has the same priority, the next-hop which is configured first is used.
Examples	<pre>sonic(config)# policy-map policy_vrf type forwarding sonic(config-policy-map)# class class_permit_ipv6 priority 10 sonic(config-policy-map)# set ipv6 next-hop 1211::2 priority 20</pre> <pre>sonic(config)# policy-map pmap-ftb-1 type forwarding sonic(config-policy-map)# class cmap-ipv6-ftb priority 90 sonic(config-policy-map-flow)# set ipv6 replication-group rg-ipv6- anycast-1</pre> <pre>sonic(config-policy-map)# no set ipv6 next-hop global 1211::2</pre>
Releases	3.1 or later

set local-preference

Sets the preference value for the AS path.

Command	set local-preference <i>pvalue</i>
Options	local-preference <i>pvalue</i> — LOCAL_PREF attribute value
Modes	ROUTE-MAP
Usage	Use this command to set the LOCAL_PREF attribute for routes meeting the route-map criteria.
Examples	<pre>sonic(config-route-map)# set local-preference 200</pre> <pre>sonic(config-route-map)# no set local-preference 200</pre>
Releases	3.0 or later

set metric

Sets a metric value for a routing protocol.

Command	set metric { <i>metric</i> <i>rtt</i> + <i>rtt</i> - <i>rtt</i> }
Options	<ul style="list-style-type: none"> • <i>metric</i>—Metric value • <i>rtt</i>—Metric value (0 to 4294967295) • +<i>rtt</i>—+Metric value (0 to 4294967295) • -<i>rtt</i>—-Metric value (0 to 4294967295)
Modes	ROUTE-MAP
Usage	Use this command to set the route metric. Provide a specific value to set the BGP attribute MED or use +/- to add or subtract the specified value to/from the existing MED. Use <i>rtt</i> to set the MED to the round-trip time or + <i>rtt</i> /- <i>rtt</i> to add or subtract the round-trip time to/from the MED.
Examples	<pre>sonic(config-route-map)# set metric +100 sonic(config-route-map)# set metric -200 sonic(config-route-map)# set metric 300 sonic(config-route-map)# set metric +rtt</pre>

```
sonic(config-route-map)# set metric -rtt  
sonic(config-route-map)# set metric rtt  
  
sonic(config-route-map)# no set metric 10
```

Releases 3.0 or later

set mirror-session

Sets mirror session results.

Command `set mirror-session session-name`
Options *session-name*—Specify a mirror session name
Modes POLICY-MAP
Usage Use this command to set the mirror session for classified traffic in flow-based port monitoring.

Examples

```
sonic(config)# policy-map policy_mirror type monitoring  
sonic(config-policy-map)# class class1 priority 10  
sonic(config-policy-map-flow)# set mirror-session mirror1  
  
sonic(config-policy-map-flow)# no set mirror-session mirror1
```

Releases 3.1 or later

set origin

Sets the origin of advertised routes.

Command `set origin {egp | igrp | incomplete}`
Options

- *egp*—Adds an existing community
- *igrp*—Sends inside the local-AS
- *incomplete*—Not advertised to peers

Modes ROUTE-MAP
Usage Use this command to set the BGP route origin to *egp*, *igrp*, or *incomplete*.

Examples

```
sonic(config)# route-map map1 permit 10  
sonic(config-route-map)# set origin egp  
  
sonic(config-route-map)# no set origin egp
```

Releases 3.0 or later

set pcp

Sets priority code point (PCP) remarkings for QoS flow.

Command `set pcp pcp-value`
Options *pcp-value*—Enter the PCP value (0 to 7)
Modes POLICY-MAP
Usage Use this command to set the PCP for the classified traffic.

Examples

```
sonic(config) # policy-map policy_qos type qos
sonic(config-policy-map)# class class_permit_ip priority 10
sonic(config-policy-map-flow)# set pcp 1
```

```
sonic(config-policy-map-flow)# no set pcp
```

Releases

3.1 or later

set traffic-class

Sets the traffic class.

Command `set traffic-class tc-value`**Options** `tc-value`—Traffic class value (0 to 7)**Modes** POLICY-MAP**Usage** Use this command to set the traffic class for the classified traffic.**Examples**

```
sonic(config) # policy-map policy_qos type qos
sonic(config-policy-map)# class class_permit_ip priority 10
sonic(config-policy-map-flow)# set traffic-class 1
```

```
sonic(config-policy-map-flow)# no set traffic-class
```

Releases

3.1 or later

set trap-action

Sets the CoPP trap action.

Command `set trap-action trap-action-value`**Options** `trap-action-value`—Trap actions; select drop, forward, copy, copy_cancel, trap, log, deny, or transit**Modes** COPP-ACTION**Usage** Use this command to set the trap action to take on CPU traffic. The default value is `trap`. The following are the trap action values:

- `drop`—Drop Packet in data plane.
- `forward`—Forward Packet in data plane.
- `copy`—Copy Packet to CPU without interfering with the original packet action in the pipeline.
- `copy_cancel`—Cancel copy the packet to CPU.
- `trap`—A copy of the original packet is sent to CPU port, the original packet is forcefully dropped from the pipeline.
- `log`—A copy of the original packet is sent to CPU port, the original packet, if it was to be dropped in the original pipeline, change the pipeline action to forward (cancel drop).
- `deny`—A combination of `copy_cancel` and `drop`
- `transit`—A combination of `copy_cancel` and `forward`

Examples

```
sonic(config) # copp-action copp-user-arp
sonic(config-copp-action)# set trap-action drop
```

```
sonic(config-copp-action)# no set trap-action
```

Releases

3.1 or later

set trap-priority

Sets CoPP trap priority.

Command	<code>set trap-priority <i>trap-priority-value</i></code>
Options	<code><i>trap-priority-value</i></code> —CoPP trap priority (0 to 1023; default is 1).
Modes	COPP-ACTION
Usage	Use this command to specify the priority in which trap actions in the action group are performed in case CPU protocol traffic matches more than one CoPP class map.
Examples	<pre>sonic(config-copp-action)# set trap-priority 3</pre> <pre>sonic(config-copp-action)# no set trap-priority</pre>
Releases	3.1 or later

set trap-queue

Sets the CoPP queue identifier.

Command	<code>set trap-queue <i>queue-id-value</i></code>
Options	<code><i>queue-id-value</i></code> —Enter the Queue ID numbers (0 to 31; default is 0)
Modes	COPP-ACTION
Usage	Use the <code>set trap-queue</code> command to configure the CPU queue to which matching traffic in the action group is assigned. To reset a trap queue to the default queue 0, enter the <code>no set trap-queue</code> command.
Examples	<pre>sonic(config)# copp-action copp-user-arp</pre> <pre>sonic(config-copp-action)# set trap-queue 3</pre> <pre>sonic(config-copp-action)# no set trap-queue</pre>
Releases	3.1 or later

set weight

Sets BGP weight for the routing table.

Command	<code>set weight <i>value</i></code>
Options	<code><i>value</i></code> — Weight value (0 to 4294967295)
Modes	ROUTE-MAP
Usage	This command is used in route-map mode to set weight for a BGP prefix.
Examples	<pre>sonic(config)# route-map map1 permit 2</pre> <pre>sonic(config-route-map)# set weight 5267</pre> <pre>sonic(config-route-map)# no set weight</pre>
Releases	4.0 or later

sflow agent-id

Configures an sFlow agent interface.

Command `sflow agent-id {phy-if-name | vlan-if-name | loop-if-name}`

- Options**
- `phy-if-name` — Ethernet interface name
 - `vlan-if-name` — VLAN interface name
 - `loop-if-name` — Loopback interface name

Modes CONFIGURATION

Usage The interface name provides the IPv4 or IPv6 address for the collector to uniquely identify the source of packets it receives.

Examples

```
sonic(config)# sflow agent-id Ethernet0
```

```
sonic(config)# no sflow agent-id
```

Releases 3.0 or later

sflow collector

Adds an sFlow collector.

Command `sflow collector ip [port] [vrf vrf_name]`

- Options**
- `ip` — Collector IPv4 or IPv6 address in A.B.C.D or A:B:C:D:E:F:G:H format
 - `port` — (Optional) UDP port of the collector (0 to 65535, default 6343)
 - `vrf_name` — (Optional) VRF name prefixed by Vrf (up to 15 characters)

Modes CONFIGURATION

Usage Use this command to configure an sFlow collector IP address where sFlow datagrams are forwarded. You must enter a valid and reachable IPv4 or IPv6 address. If you configure two collectors, traffic samples are sent to both (up to two sFlow collectors is allowed).

Examples

```
sonic(config)# sflow collector 1.1.1.1
```

```
sonic(config)# sflow collector 1.1.1.2 4451
```

```
sonic(config)# sflow collector 1.1.1.2 4451 vrf mgmt
```

```
sonic(config)# no sflow collector 1.1.1.1
sonic(config)# no sflow collector 1.1.1.2 4451
sonic(config)# no sflow collector 1.1.1.2 4451 vrf mgmt
```

Releases 3.0 or later

sflow enable

Enables sFlow configuration.

Command `sflow enable`

Options None

- Modes**
- CONFIGURATION
 - INTERFACE

Usage	Use this command to enable sFlow globally or on a specific interface.
Examples	<pre>sonic(config) # sflow enable</pre> <pre>sonic(config) # no sflow enable</pre>
Releases	3.0 or later

sflow polling-interval

Sets the sFlow polling interval.

Command	<code>sflow polling-interval <i>interval</i></code>
Options	<i>interval</i> — Polling interval size (5 to 300, default 20, 0 to disable)
Modes	CONFIGURATION
Usage	The polling interval for an interface is the number of seconds between successive samples of counters sent to the collector. You can configure the duration for polled interface statistics.
Examples	<pre>sonic(config) # sflow polling-interval 44</pre> <pre>sonic(config) # no sflow polling-interval</pre>
Releases	3.0 or later

sflow sampling-rate

Sets the sFlow sampling rate.

Command	<code>sflow sampling-rate <i>sampling-rate</i></code>
Options	<i>sampling-rate</i> <i>sampling-rate</i> — The range is from 256 to 8388608. The default sFlow sampling rates are:
	<ul style="list-style-type: none"> • 1G link — 1 packet in 1000 • 10G link — 1 packet in 10,000 • 40G link — 1 packet in 40,000 • 50G link — 1 packet in 50,000 • 100G link — 1 packet in 100,000
Modes	<ul style="list-style-type: none"> • INTERFACE • CONFIGURATION
Usage	You can configure the sampling globally, on an interface, or a range of interfaces. When you configure the sampling rate for an interface or a range of interfaces, the value takes precedence over the global configuration. When you undo the global configuration using the <code>no sflow sampling-rate</code> command, the sampling rate of all interfaces that do not have an interface-level sampling rate configuration is reset to the default value. <div style="border-left: 2px solid #ccc; padding-left: 10px; margin-top: 10px;"> NOTE: Reconfigure the sFlow sampling rate for packets only in exceptional cases. The sampling rate collects one packet in the specified number of packets (256 to 8388608). For example, if you configure a sampling rate of 256, the system samples one packet out of 256 packets. The default detects a new flow of 10% of the link bandwidth in less than one second and depends on the interface speed. It is recommended that you do not change the default setting. </div>

Examples

```
sonic(config-if-Ethernet28)# sflow sampling-rate 4400  
  
sonic(config-if-Ethernet28)# no sflow sampling-rate  
  
sonic(config)# sflow sampling-rate 4400  
  
sonic(config)# no sflow sampling-rate
```

Releases

3.0 or later

show aaa

Displays authentication, authorization, and accounting (AAA) configuration information.

Command show aaa

Options None

Modes EXEC

Usage Use this command to view AAA information including if failthrough is enabled, and the configured login method (local, TACACS+, or LDAP).

Example

```
sonic# show aaa  
-----  
AAA Authentication Information  
-----  
failthrough : True  
login-method : ldap, local
```

Releases

3.1 or later

show access-group

Displays the ACL binding summary.

Command show access-group

Options None

Command mode EXEC

Usage None

Example

```
sonic# show access-group  
Ingress IPV6 access-list ipv6acl-example on Ethernet0  
Ingress IP access-list ipacl-example on PortChannel11  
Ingress MAC access-list macacl-example on Vlan100
```

Releases

3.1 or later

show alarm

Displays only the active alarms in the system.

Command sonic# show alarm [acknowledged | all | detail | summary | severity level | start timestamp end timestamp | recent {5min|60min|24hr} | id event-id | from event-id to event-id]

Options

- acknowledged — Displays only acknowledged alarms.
- all — Displays information about all logged alarms, including acknowledged alarms.
- detail — Displays detailed alarm information.
- summary — Displays summary information about logged alarms.
- severity level — Displays information for alarms with the specified severity level: critical, major, minor, warning, or informational. The default is warning.
- start timestamp end timestamp — Displays the alarms that are logged between the specified times. Enter the timestamp in the format *yyyy-mm-hhTmm:ss:msZ*, where *yyyy* is a 4-digit year, *mm* is a 2-digit month, *hh* is a 2-digit hour, and *Tmm:ss:msZ* is the hour-second-millisecond in the timestamp.
- recent {5min|60min|24hr} — Displays the most recent alarms that are logged in the last 5 minutes, hour, or day.
- id event-id — Displays information about the specified alarm ID.
- from event-id to event-id - Displays information for the alarms in the range of the specified event IDs in show event log output.

Modes

EXEC

Usage

Use the `show alarm` command to filter events so that only alarms that can be corrected and cleared are displayed. By default, the `show alarm` output displays only active alarm events. Acknowledged alarms are not shown by default in `show alarm` output. Acknowledged alarms are re-triggered after a reboot, fast-reboot, or power cycle and displayed in `show alarm` output if the alarm condition still exists.

Example

```
sonic# show alarm
-----
Id Severity Name Source Timestamp Description
-----
2 WARNING PSU_REMOVED PSU 3 2023-10-20T09:17:54.488Z PSU 3
3 WARNING FAN_REMOVED FAN 1 2023-10-20T09:17:56.985Z PSU 2 FAN 1
20 WARNING PSU_POWER_STATUS PSU 1 2024-02-08T07:29:06.395Z PSU 1 is out of power
```

i **NOTE:** Acknowledged alarms are not shown by default in `show alarm` output. Acknowledged alarms are retriggered after a reboot, fast-reboot, or power cycle and displayed in the `show alarm` output if the alarm condition still exists.

```
sonic# show alarm all
-----
Id Severity Name Source Timestamp Description
-----
1 WARNING PSU_REMOVED PSU 2 2023-10-20T09:17:54.479Z PSU 2
2 WARNING PSU_REMOVED PSU 3 2023-10-20T09:17:54.488Z PSU 3
3 WARNING FAN_REMOVED FAN 1 2023-10-20T09:17:56.985Z PSU 2 FAN 1
```

```
sonic# show alarm id 10
Id: 10
Severity: WARNING
Type: PSU_VOLTAGE_STATUS
Timestamp: 2019-03-01T08:26:42.384Z
Description: PSU 2: voltage out of range, current voltage=11.0, valid range=[None, None].
Source: PSU 2
Acknowledged: False
Acknowledged time: -
```

```
sonic# show alarm detail
-----
Alarm Details - 1
-----
Id: 1
Severity: WARNING
Type: PSU_REMOVED
Timestamp: 2023-10-20T09:17:54.479Z
Description: PSU 2
Source: PSU 2
Acknowledged: True
```

```

Acknowledged time: 2023-10-20T09:53:47.425Z
-----
Alarm Details - 2
-----
Id: 2
Severity: WARNING
Type: PSU REMOVED
Timestamp: 2023-10-20T09:17:54.488Z
Description: PSU 3
Source: PSU 3
Acknowledged: False
Acknowledged time: -
-----
Alarm Details - 3
-----
Id: 3
Severity: WARNING
Type: FAN REMOVED
Timestamp: 2023-10-20T09:17:56.985Z
Description: PSU 2 FAN 1
Source: PSU 2 FAN 1
Acknowledged: False
Acknowledged time: -

```

```

sonic# show alarm from 2 to 3
-----
Id Severity Name Source Timestamp Description
-----
2 WARNING PSU_REMOVED PSU 3 2023-10-20T09:17:54.488Z PSU 3
3 WARNING FAN_REMOVED FAN 1 2023-10-20T09:17:56.985Z PSU 2 FAN 1

```

```

sonic# show alarm summary
Alarm summary
-----
Total: 2
Critical: 0
Major: 0
Minor: 0
Warning: 2
Acknowledged: 1

```

Releases

4.2.0 or later

show ars bind

Displays the ARS binding information

Command show ars bind

Options None.

Modes EXEC

Usage This command displays ARS bind information.

Example

```

sonic# show ars bind

ARS Profile binding Info (Switch Name : Profile Name):
SWITCH: ARS_PROF

Port Profile binding Info (Port Profile Name : Interfaces):
    ARS_PRT_PROF : Eth1/46/1, Eth1/46/2, Eth1/48/1, Eth1/48/2,
    Eth1/58/1, Eth1/58/2, Eth1/60/1, Eth1/60/2

ARS Object binding Info (Routemap, Seq.No : Object Name):
    ARS_RMAP, 1 : ARS_OBJ

```

Releases	4.4.0 or later
-----------------	----------------

set ars disable

Disables ARS forwarding for the flows.

Command	set ars disable
----------------	-----------------

Options	None
----------------	------

Modes	POLICY-MAP
--------------	------------

Usage	Use this command to disable the ARS forwarding for the classified traffic.
--------------	--

Example	
----------------	--

```
sonic(config)# policy-map policy_ars type forwarding
sonic(config-policy-map)# class class_disable_ars priority 10
sonic(config-policy-map-flow)# set ars disable
sonic(config-policy-map-flow)# no set ars disable
```

Releases	4.4.0 or later
-----------------	----------------

show ars nhg-statistics

Displays information about ARS next-hop group statistics information: .

Command	show ars nhg-statistics [<i>nexthop-group-id</i>]
----------------	---

Options	<i>nexthop-group-id</i> —Enter the next-hop group ID of the routes. The range is from range 0 to 4294967295.
----------------	--

Modes	EXEC
--------------	------

Usage	<ul style="list-style-type: none">This command displays all information about ARS next-hop group statistics.Use the <code>show ip</code> or <code>ipv6 route</code> <code>nexthop-group</code> commands to find the NHG ID for routes. Use the <code>clear ars nhg-statistics</code> command to clear the statistics.
--------------	--

Example	
----------------	--

```
sonic#show ars nhg-statistics

ARS NHG Statistics Info:

NHG ID: 200
Number of packet drops: 50
Number of next hop reassigned: 40
Number of port reassigned: 30
```

Releases	4.4.0 or later
-----------------	----------------

show ars object

Displays information about ARS object.

Command	show ars object [<i>ars-object-name</i>]
----------------	--

Options	<i>ars-object-name</i> —Enter the name of the ARS object.
----------------	---

Modes	EXEC
--------------	------

Usage	This command displays all information about an ARS object.
--------------	--

Example	
----------------	--

```
sonic# show ars object default

ARS Object Attributes Info:
```

```
ARS Object Name: default
Idle duration to classify a flow-let in a macro flow: 80
microsecond(s)
Maximum flow size: 256
ARS path (re)assignment mode: Per flow-let quality
```

Releases 4.4.0 or later

show ars port-profile

Displays information about ARS port profile.

Command	show ars port-profile [<i>ars-port-profile-name</i>]
Options	<i>ars-port-profile-name</i> —Enter the name of the ARS port profile.
Modes	EXEC
Usage	This command displays all information about an ARS port profile.
Example	<pre>sonic# show ars port-profile default Port Attributes Info: Port Profile Name: default ARS for a port is: Enabled Port load scaling factor: 0 Past port load quality weight in percent: 80 Future port load quality weight in percent: 10</pre>

Releases 4.4.0 or later

show ars port-quality

Displays the ARS quality on egress ports.

Command	show ars port-quality [<i>interface-name</i>]
Options	• <i>interface-name</i> —Enter the name of the Ethernet interface.
Modes	EXEC
Usage	This command displays the quality of a port. 0 is the lowest quality and 7 is the highest quality.
Examples	<pre>sonic# show ars port-quality DLB Quality on egress ports: PortName Quality [0-7] ----- Eth1/37 5 Eth1/38 5 Eth1/39 5 Eth1/40/1 4 sonic#</pre>

Releases 4.4.0 or later

show ars profile

Displays information about ARS profile.

Command	show ars profile [<i>ars-profile-name</i>]
Options	<i>ars-profile-name</i> —Enter the name of the ARS profile.
Modes	EXEC
Usage	This command displays all information about an ARS profile.
Example	<pre>sonic# show ars profile ars-profile-name Switch Attributes Info: Profile Name: default ARS algorithm used for quality computation: EWMA Sampling interval of data for quality measure computation: 16 microsecond(s) Random seed: 10 Past port load as the quality parameter: Enabled Past port load weight: 2 Future port load as the quality parameter: Enabled Future port load weight: 2 Current port load calculation: Disabled Exponential port load value: 2 Minimum past load threshold value: 3000 Maximum past load threshold value: 6000 Minimum future load threshold value: 2097152 Maximum future load threshold value: 12582912 Minimum current load threshold value: 1048576 Maximum current load threshold value: 6291456</pre>
Releases	4.4.0 or later

show audit-log

Displays the audit log.

Command	show audit-log [all]
Options	all—(Optional) Displays all audit logs
Modes	EXEC
Usage	This command prints up to 20 lines of log. To view all the logs, use show audit-log all command.
Example	<pre>sonic# show audit-log Dec 3 00:45:34.449724 2020 leaf2 INFO mgmt-framework#klish[78]: User "admin" command "show ipv6 route" status - success Dec 3 00:45:30.608482 2020 leaf2 INFO mgmt-framework#klish[78]: User "admin" command "show ipv6" status - success Dec 3 00:37:54.957349 2020 leaf2 INFO mgmt-framework#klish[78]: User "admin" command "startup" status - success Dec 3 00:37:47.495638 2020 leaf2 INFO sshd[7326]: pam_unix(sshd:session): session opened for user admin by (uid=0) Dec 3 00:37:47.465825 2020 leaf2 INFO sshd[7326]: Accepted password for admin from 10.14.1.95 port 45310 ssh2 Dec 2 20:25:56.648421 2020 leaf2 INFO sshd[13620]: pam_unix(sshd:session): session closed for user admin</pre>
Releases	3.1 or later

show auditd-system log

Displays the currently logged Auditd system messages.

Command	sonic# show auditd-system log [all]
Options	all — Display the complete Auditd log output. The show auditd-system log command displays the last 20 lines.
Modes	EXEC
Usage	System administrators can access the Auditd logs for security-related analysis. Debian packages such as aureport and ausearch can be used to read and analyze the logs. Users can also configure the system to stream Auditd logs to a remote server (logging server command). Only the secadmin role can configure and view Auditd system rules.
Example	<pre>sonic# show auditd-system log ----- Audit rules profile: basic ----- -w /var/run/utmp -p wa -k session -w /var/log/btmp -p wa -k session -w /var/log/wtmp -p wa -k session -w /usr/bin/dpkg -p x -k software_mgmt -w /usr/bin/apt-add-repository -p x -k software_mgmt -w /usr/bin/apt-get -p x -k software_mgmt -w /usr/bin/aptitude -p x -k software_mgmt</pre>
Releases	4.4.0 or later

show auditd-system rules

Displays the Auditd rules used in the Linux kernel.

Command	sonic# show auditd-system rules
Options	None
Modes	EXEC
Usage	To configure rules for the Linux Audit logging service (Auditd system), use the auditd-system rules command.
Example	<pre>sonic# show auditd-system rules ----- Audit rules profile: basic ----- -w /var/run/utmp -p wa -k session -w /var/log/btmp -p wa -k session -w /var/log/wtmp -p wa -k session -w /usr/bin/dpkg -p x -k software_mgmt -w /usr/bin/apt-add-repository -p x -k software_mgmt -w /usr/bin/apt-get -p x -k software_mgmt -w /usr/bin/aptitude -p x -k software_mgmt</pre>
Releases	4.4.0 or later

show authentication

Displays the authentication manager global information and the number of authenticated clients.

Command	show authentication
Options	None
Modes	EXEC

Usage

This command displays the authentication manager global information and the number of authenticated clients.

Example

```
sonic# show authentication
-----
PAC Global configuration
-----
Authentication Monitor Mode ..... Enabled
-----
Number of PAC Clients
-----
Number of Authenticated clients ..... 0
Number of clients in Monitor mode ..... 0
```

Table 3. show authentication Output

Field	Description
Authentication Monitor Mode	The admin status of Monitor mode on the switch. This is a global configuration.
Number of Authenticated clients	The total number of clients authenticated on the switch except the ones in Monitor Mode
Number of clients in Monitor Mode	The number clients authorized by Monitor mode on the switch

Releases

3.1 or later

show authentication authentication-history

Displays the authentication manager authentication history log.

Command

```
show authentication authentication-history {all | Ethernet port}
```

Options

- *all*—All ports
- *port*—Physical interface ID

Modes

EXEC

Usage

Use the command `show authentication authentication-history all` to view all the authentication manager authentication history logs. To view the authentication history for a specific interface, use the `show authentication authentication-history Ethernet port` command.

Examples

```
sonic# show authentication authentication-history Ethernet 2

Timestamp                Interface  MAC-Address      Auth Status   Method
-----                  -----      -----          -----        -----
May 07 2020 13:02:41    Eth2       58:05:94:1C:00:00  Unauthorized  802.1X
May 07 2020 13:01:33    Eth2       58:05:94:1C:00:00  Unauthorized  802.1X
```

Releases

4.0 or later

show authentication clients

Displays the details of the dot1x configuration for a specified port.

Command

```
show authentication clients { all | Ethernet port }
```

Options

- *all*—All ports
- *port*—Physical interface ID

Modes	EXEC																																																						
Usage	Use this command to view the dot1x authentication clients for all interface or a specific interface.																																																						
Examples	<pre>sonic# show authentication clients all</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>MAC-Address</th> <th>Method</th> <th>Host Mode</th> <th>Control Mode</th> <th>VLAN</th> </tr> <tr> <th>Assigned Reason</th> <th></th> <th></th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>Eth16</td> <td>10:8D:B6:C6:00:00</td> <td>802.1X</td> <td>multi-host</td> <td>auto</td> <td>RADIUS</td> </tr> <tr> <td>Assigned VLAN (10)</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <pre>sonic# show authentication clients interface Ethernet 1</pre> <table border="1"> <tbody> <tr> <td>Mac Address.....</td> <td>58:05:94:1C:00:00</td> </tr> <tr> <td>User Name.....</td> <td>testixia</td> </tr> <tr> <td>VLAN Assigned Reason.....</td> <td>Voice VLAN (100)</td> </tr> <tr> <td>Host Mode</td> <td>Multi-auth</td> </tr> <tr> <td>Method.....</td> <td>802.1X</td> </tr> <tr> <td>Control Mode.....</td> <td>Auto</td> </tr> <tr> <td>Session time ..</td> <td>10</td> </tr> <tr> <td>Session timeout</td> <td>100</td> </tr> <tr> <td>Time left for Session Termination Action.....</td> <td>90</td> </tr> <tr> <td>Session Termination Action.....</td> <td>Default</td> </tr> <tr> <td>Filter-Id</td> <td>None</td> </tr> <tr> <td>ACS ACL Name.....</td> <td>xACSAACLx-IP-</td> </tr> <tr> <td>FP_ACL-5ee227a2</td> <td></td> </tr> <tr> <td>DACL.....</td> <td>None</td> </tr> <tr> <td>Session Termination Action.....</td> <td>Default</td> </tr> </tbody> </table>	Interface	MAC-Address	Method	Host Mode	Control Mode	VLAN	Assigned Reason						Eth16	10:8D:B6:C6:00:00	802.1X	multi-host	auto	RADIUS	Assigned VLAN (10)						Mac Address.....	58:05:94:1C:00:00	User Name.....	testixia	VLAN Assigned Reason.....	Voice VLAN (100)	Host Mode	Multi-auth	Method.....	802.1X	Control Mode.....	Auto	Session time ..	10	Session timeout	100	Time left for Session Termination Action.....	90	Session Termination Action.....	Default	Filter-Id	None	ACS ACL Name.....	xACSAACLx-IP-	FP_ACL-5ee227a2		DACL.....	None	Session Termination Action.....	Default
Interface	MAC-Address	Method	Host Mode	Control Mode	VLAN																																																		
Assigned Reason																																																							
Eth16	10:8D:B6:C6:00:00	802.1X	multi-host	auto	RADIUS																																																		
Assigned VLAN (10)																																																							
Mac Address.....	58:05:94:1C:00:00																																																						
User Name.....	testixia																																																						
VLAN Assigned Reason.....	Voice VLAN (100)																																																						
Host Mode	Multi-auth																																																						
Method.....	802.1X																																																						
Control Mode.....	Auto																																																						
Session time ..	10																																																						
Session timeout	100																																																						
Time left for Session Termination Action.....	90																																																						
Session Termination Action.....	Default																																																						
Filter-Id	None																																																						
ACS ACL Name.....	xACSAACLx-IP-																																																						
FP_ACL-5ee227a2																																																							
DACL.....	None																																																						
Session Termination Action.....	Default																																																						

Table 4. show authentication clients output

Field	Description
Interface	The interface for which authentication configuration information is displayed.
Mac Address	The MAC address of the client.
User Name	The username associated with the client.
VLAN Assigned Reason	This can take one of the following values. <ul style="list-style-type: none"> • Default VLAN—The client has been authenticated on the port default VLAN and the authentication server is not RADIUS. • RADIUS—RADIUS is used for authenticating the client. • Voice VLAN—The client is identified as a Voice device. • Unauthenticated VLAN—The client has been authenticated on the Unauthenticated VLAN. • Guest VLAN—The client has been authenticated on the Guest VLAN. • Monitor Mode—The client has been authenticated by Monitor mode.
Host Mode	The authentication host mode configured on the interface. The possible values are multi-auth, multi-domain, multi-host, and single-host.
Method	The method used to authenticate the client on the interface. The possible values are 802.1x, MAB, Captive Portal, and None.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized, auto, and unauthorized.

Table 4. show authentication clients output (continued)

Field	Description
Session time	The amount of time the client session has been active.
Session timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port.
Time left for Session Termination Action	This value indicates the time that is left for the session termination action to occur. This field is valid only when the “authentication periodic” is configured.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured ACL name on the switch.
ACS ACL name	The dynamic ACL names assigned to the interface as per the attributes sent from the External RADIUS server.
DACL	Identifies the Dynamic ACL returned by the RADIUS server when the client was authenticated.
Session Termination Action	This is used by Authenticator to reauthenticate a supplicant on the port.

Releases

4.0 or later

show authentication interface

Displays the authentication manager information for the interface.

Command `show authentication interface {all | Ethernet port}`

- Options**
- *all*—All ports
 - *port*—Physical interface ID

Modes EXEC

Usage Use this command to view the authentication manager information for the interface.

Examples

```
sonic# show authentication interface all

Interface ..... Ethernet46
Port Control Mode..... auto
Host Mode..... multi-auth
Open Authentication..... Disabled
Configured method order..... dot1x mab
Enabled method order..... dot1x mab
Configured method priority..... dot1x mab
Enabled method priority..... dot1x mab
Reauthentication Enabled..... TRUE
```

Reauthentication Session timeout from server ..	FALSE
Reauthentication Period (secs).....	15
Maximum Users.....	25
Guest VLAN ID.....	0
Unauthenticated VLAN ID.....	0
Authentication retry attempts.....	1

Table 5. show authentication interface output

Field	Description
Interface	The interface for which authentication configuration information is being displayed.
Port Control Mode	The configured control mode for this port. Possible values are force-unauthorized.
Host Mode	The authentication host mode configured on the interface.
Open Authentication	Indicates if Open Authentication is enabled on the interface.
Authentication Restart timer	This is the quite period timer. The quite period is time in seconds before reattempting authentication for a failed client.
Configured method order	The order of authentication methods used on the interface.
Enabled method order	The order of authentication methods used on the interface.
Configured method priority	The priority for the authentication methods used on the interface.
Enabled method priority	The priority for the authentication methods used on the interface.
Reauthentication Enabled	Indicates whether reauthentication is enabled on the interface.
Reauthentication Period	The period after which all clients on the interface will be reauthenticated.
Maximum Users	The maximum number of clients that can be authenticated on the interface if the interface is configured as multi-auth host mode.
Guest VLAN ID	The VLAN ID to be used to authorize clients that time out or fail authentication due to invalid credentials. This is applicable only for 802.1x unaware clients.
Unauthenticated VLAN ID	The VLAN ID to be used to authorize clients that time out or fail authentication due to invalid credentials. This is applicable only for 802.1x clients.
Authentication retry attempts	The number of the times authentication is reattempted by the client before a port moves to the authentication fail state.

Releases

4.0 or later

show ip rest authentication

Displays REST authentication modes.

Command	show ip rest authentication
Options	None
Modes	EXEC
Usage	<p>Use this command to display the REST authentication modes.</p> <ul style="list-style-type: none">• <code>password</code>—HTTP password authentication.• <code>jwt</code>—JSON web token (JWT) token-based authentication.• <code>cert</code>—Client certificate authentication.

Example	<pre>sonic# show ip rest authentication Client authentication mode is password,jwt</pre>
----------------	--

Releases	3.1 or later
-----------------	--------------

show ip telemetry authentication

Displays telemetry authentication modes.

Command	show ip telemetry authentication
Options	None
Modes	EXEC
Usage	<p>Use this command to display the telemetry authentication modes.</p> <ul style="list-style-type: none">• <code>password</code>—HTTP password authentication.• <code>jwt</code>—JSON web token (JWT) token-based authentication.• <code>cert</code>—Client certificate authentication.

Example	<pre>sonic# show ip telemetry authentication ----- Telemetry Client Authentication Modes ----- client_auth: password,jwt</pre>
----------------	--

Releases	3.1 or later
-----------------	--------------

show bfd peer

Displays single hop and multihop BFD peer information.

Command	show bfd peer { <i>peer_ipv4</i> <i>peer_ipv6</i> } [<i>vrf</i>] <i>vrfname</i> [<i>multihop</i>] [<i>local-address</i>] { <i>local_ipv4</i> <i>local_ipv6</i> } [<i>interface</i>] <i>interfacename</i>
Options	<ul style="list-style-type: none">• <i>peer_ipv4</i>—Peer IPv4 address in A.B.C.D format• <i>peer_ipv6</i>—Peer IPv6 address in A::B format• <i>vrfname</i>—(Optional) VRF instance name• <i>local_ipv4</i>—(Optional) Local IPv4 address in A.B.C.D format• <i>local_ipv6</i>—(Optional) Local IPv6 address in A::B format• <i>interfacename</i>—Interface name (ranges)
Modes	EXEC
Usage	<p>Use this command to display general BFD peer information.</p>

Examples

```
sonic# show bfd peer 192.168.2.1 interface Ethernet0
BFD Peers:

    peer 192.168.2.1 vrf default interface Ethernet0
        ID: 106764218
        Remote ID: 3876686491
        Status: up
        Uptime: 0 day(s), 0 hour(s), 51 min(s), 49 sec(s)
        Diagnostics: ok
        Remote diagnostics: ok
        Peer Type: configured
        Local timers:
            Detect-multiplier: 3
            Receive interval: 300ms
            Transmission interval: 300ms
            Echo transmission interval: 0ms
        Remote timers:
            Detect-multiplier: 3
            Receive interval: 300ms
            Transmission interval: 300ms
            Echo transmission interval: 50ms
```

```
sonic# show bfd peer 192.168.2.1 multihop local-address 192.168.2.2
BFD Peers:

    peer 192.168.2.1 multihop local-address 192.168.2.2 vrf default
        ID: 2900535060
        Remote ID: 0
        Status: down
        Downtime: 0 day(s), 0 hour(s), 0 min(s), 30 sec(s)
        Diagnostics: ok
        Remote diagnostics: ok
        Peer Type: configured
        Local timers:
            Detect-multiplier: 3
            Receive interval: 300ms
            Transmission interval: 300ms
            Echo transmission interval: 60ms
        Remote timers:
            Detect-multiplier: 3
            Receive interval: 1000ms
            Transmission interval: 1000ms
            Echo transmission interval: 0ms
```

Releases

3.2 or later

show bfd peer counters

Displays single-hop and multihop BFD peer counter information.

Command `show bfd peer counters {peer_ipv4 | peer_ipv6} [vrf] vrfname [multihop] [local-address] {local_ipv4 | local_ipv6} [interface] interfacename`

Options

- `peer_ipv4`—Peer IPv4 address in A.B.C.D format
- `peer_ipv6`—Peer IPv6 address in A::B format
- `vrfname`—(Optional) VRF instance name
- `local_ipv4`—(Optional) Local IPv4 address in A.B.C.D format
- `local_ipv6`—(Optional) Local IPv6 address in A::B format
- `interfacename`—(Optional) Interface name (ranges)

Modes EXEC

Usage

Use this command to display the packet and event counters.

Examples

```
sonic# show bfd peer counters 192.168.2.1 interface Ethernet0
peer 192.168.2.1 vrf default interface Ethernet0
```

```

Control packet input: 25 packets
Control packet output: 25 packets
Echo packet input: 0 packets
Echo packet output: 0 packets
Session up events: 1
Session down events: 0
Zebra notifications: 0

```

```

sonic# show bfd peer counters 192.168.2.1 multihop local-address 192.168.2.2
peer 192.168.2.1 multihop local-address 192.168.2.2 vrf default
    Control packet input: 25 packets
    Control packet output: 25 packets
    Echo packet input: 0 packets
    Echo packet output: 0 packets
    Session up events: 1
    Session down events: 0
    Zebra notifications: 0

```

Releases

3.2 or later

show bfd peers

Displays all BFD peer information.

Command

`show bfd peers [vrf vrfname] {[brief] | [counters]}`

Options

- *vrfname*—(Optional) VRF name prefixed by Vrf (up to 15 characters)
- *brief*—(Optional) Display brief information on BFD peers
- *counters*—(Optional) Display information on BFD counters

Modes

EXEC

Usage

Use this command to display general information about BFD peers.

Examples

```

sonic# show bfd peers brief
Session Count: 6
SessionId LocalAddress                               PeerAddress
          Status      Vrf
=====
1842336549 fe80::3e2c:30ff:fe55:2f82             fe80::1a5a:58ff:fea2:d965
          UP        default
459038002  fe80::3e2c:30ff:fe55:2f82             fe80::1a5a:58ff:fea2:d965
          UP        default
3595626914 fe80::3e2c:30ff:fe55:2f82             fe80::1a5a:58ff:fea2:d965
          UP        default
485839230  fe80::3e2c:30ff:fe55:2f82             fe80::eab5:d0ff:fe99:65ec
          UP        default
1853247457 fe80::3e2c:30ff:fe55:2f82             fe80::eab5:d0ff:fe99:65ec
          UP        default
111352211  fe80::3e2c:30ff:fe55:2f82             fe80::eab5:d0ff:fe99:65ec
          UP        default
sonic#

```

```

sonic# show bfd peers
BFD Peers:

    peer 192.168.2.2 vrf default interface Ethernet0
        ID: 1861362724
        Remote ID: 3644437776
        Status: up
        Uptime: 0 day(s), 0 hour(s), 0 min(s), 6 sec(s)
        Diagnostics: ok
        Remote diagnostics: ok
        Peer Type: configured
        Local timers:
            Detect-multiplier: 3
            Receive interval: 300ms
            Transmission interval: 300ms

```

```
        Echo transmission interval: 0ms
Remote timers:
    Detect-multiplier: 3
    Receive interval: 300ms
    Transmission interval: 300ms
    Echo transmission interval: 50ms
```

```
sonic# show bfd peers vrf Vrf7
BFD Peers:

peer 192.168.2.2 vrf Vrf7 interface Ethernet0
    ID: 1861362724
    Remote ID: 3644437776
    Status: up
    Uptime: 0 day(s), 0 hour(s), 0 min(s), 6 sec(s)
    Diagnostics: ok
    Remote diagnostics: ok
    Peer Type: configured
    Local timers:
        Detect-multiplier: 3
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo transmission interval: 0ms
    Remote timers:
        Detect-multiplier: 3
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo transmission interval: 50ms
```

```
sonic# show bfd peers counters
BFD Peers:

peer 192.168.2.2 vrf default interface Ethernet0
    Control packet input: 239 packets
    Control packet output: 292 packets
    Echo packet input: 0 packets
    Echo packet output: 0 packets
    Session up events: 1
    Session down events: 0
    Zebra notifications: 0
```

```
sonic# show bfd peers vrf Vrf7 counters
BFD Peers:

peer 192.168.2.2 vrf Vrf7 interface Ethernet0
    Control packet input: 239 packets
    Control packet output: 292 packets
    Echo packet input: 0 packets
    Echo packet output: 0 packets
    Session up events: 1
    Session down events: 0
    Zebra notifications: 0
```

Releases

3.0 or later

show bfd profile

Displays BFD profile information.

Command `show bfd profile [profile-name]`

Options `profile-name`—Specific BFD profile

Modes EXEC

Usage Use the `show bfd profile` command to display general information about BFD peers.

Examples

Per-BFD profile:

```
sonic# show bfd profile active1
BFD Profile:
  Profile-name: active1
    Enabled: True
    Echo-mode: Enabled
    Passive-mode: Enabled
    Minimum-Ttl: 254
    Detect-multiplier: 3
    Receive interval: 300ms
    Transmission interval: 300ms
    Echo transmission interval: 300ms
```

All BFD profiles:

```
sonic# show bfd profile
BFD Profile:
  Profile-name: active1
    Enabled: True
    Echo-mode: Enabled
    Passive-mode: Enabled
    Minimum-Ttl: 254
    Detect-multiplier: 3
    Receive interval: 300ms
    Transmission interval: 300ms
    Echo transmission interval: 300ms
  Profile-name: fast
    Enabled: True
    Echo-mode: Enabled
    Passive-mode: Disabled
    Minimum-Ttl: 254
    Detect-multiplier: 3
    Receive interval: 400ms
    Transmission interval: 400ms
    Echo transmission interval: 400ms
```

Releases

4.0 or later

show bgp all

Displays BGP information for all address families.

Command

```
show bgp all [vrf vrf-name] {{peer-group [peer-group-name]} | {neighbors [neighbor-ip]}}
```

Options

- *vrf-name*—(Optional) VRF name prefixed by Vrf
- *peer-group-name*—(Optional) Peer group name
- *neighbor-ip*—(Optional) Neighbor IP address

Modes

EXEC

Usage

Use this command to display BGP information for all address families.

Examples

```
sonic# show bgp all neighbors

BGP neighbor is Ethernet50, remote AS 65500, local AS 65502, external link
BGP version 4, remote router ID 10.10.10.10 , local router ID 2.2.2.2
BGP state = Established, up for 1d00h30m
Last read 00:00:42, Last write 00:00:43
Hold time is 180 seconds, keepalive interval is 60 seconds
Minimum time between advertisement runs is 0 seconds
Neighbor capabilities:
  4 Byte AS: advertised and received
  AddPath: advertised and received
  Route refresh: advertised and received
  Multiprotocol Extension: advertised and received
  Graceful restart: advertised and received
Message statistics:
  InQ depth is 0
```

```

        OutQ depth is 0          Sent      Rcvd
        Opens:                  1          1
        Notifications:         0          0
        Updates:                2975     3413
        Keepalive:              1471     1471
        Route Refresh:          0          0
        Capability:             0          0
        Total:                 4447     4885
--more--

```

```

sonic# show bgp all peer-group

BGP peer-group spines
  Peer-group type is external
  Configured address-families:
  Peer-group members:
    Ethernet50 Established
    Ethernet54 Established
    PortChannel121 Established
    PortChannel122 Established
    Vlan21 Established
    Vlan22 Established

```

Releases 3.1 or later

show bgp as-path-access-list

Displays BGP AS path lists configured on the device.

Command	show bgp as-path-access-list [<i>list-name</i>]
Options	<i>as-path-access-list list-name</i> — (Optional) Access-list name
Modes	EXEC
Usage	Use this command to view the AS path access lists configured on this device. If an access-list name is not specified, all AS Path access lists display. A BGP AS path access-list is used in route-maps and with BGP neighbors to design routing policies.

Example

```

sonic(config)# show bgp as-path-access-list
AS path list asp_private:
  action: permit
  members: ^65000.*6510565109$
AS path list asp_private2:
  seq: 121
    action: permit
    members: ^62.*65121$
  seq: 7371
    action: deny
    members: ^67.*657371$

```

Releases 3.0 or later

show bgp community-list

Displays BGP community-list configuration information.

Command	show bgp community-list [<i>list-name</i>]
Options	<i>community-list list-name</i> — (Optional) Community-list name
Modes	EXEC
Usage	Use this command to view the community lists configured on this device. If a community-list name is not specified, all community lists display. Community-lists are used in route-maps to design BGP routing policies.

Example

```
sonic# show bgp community-list
Expanded community list CommList_Exp:    match: ANY
  300:500
  800:900
  no-export
Standard community list CommList_RT:   match: ANY
  100:200
  no-export
  no-peer
  65100:3456
```

Releases

3.0 or later

show bgp ext-community-list

Displays BGP extended community-list configuration information.

Command show bgp ext-community-list [*list-name*]**Options** ext-community list *list-name* — (Optional) Extended community-list name**Modes** EXEC**Usage** Use this command to view the extended community lists configured on this device. If extended community-list name is not specified, all extended community lists display.**Example**

```
sonic# show bgp ext-community-list
Standard extended community list ExtComm_AllowInt:  match: ALL
  rt:19.32.56.167:65011,rt:31.67.182.214:3001,soo:01:65010,soo:.13.175.21:65101
Standard extended community list ExtComm_BlockExt:  match: ANY
  rt:4020:65104
  soo:9.54.32.165:65200
```

Releases

3.0 or later

show bgp ipv4

Displays BGP IPv4 configuration.

Command show bgp ipv4 unicast [vrf {*vrf-name* | all}] [{*ip-address* | *ip-address/prefix*} [bestpath | multipath]] | community {AA:NN | local-as | no-advertise | no-export | no-peer} [exact-match] | dampening {dampened-paths | flap-statistics | parameters} | neighbors [*ipv4-address* | *IPv6-address*] | interface {Eth | PortChannel | Vlan}] [advertised-routes | filtered-routes | received-routes | routes] | route-map *route-map-name* | statistics | summary]**Options**

- *vrf-name*—VRF name prefixed by vrf (up to 15 characters)
- *ip-address*—IP address in A.B.C.D format
- *ip-address/prefix*—IP address with the prefix in A.B.C.D/mask format
- AA:NN—Community number in AA:NN format.
- *IPv4-address*—IPv4 address of a neighbor.
- *IPv6-address*—IPv6 address of a neighbor.
- *route-map-name*—Route-map name.
- *neighbor-ip*—Neighbor IP address in A.B.C.D or AA::NN format .
- *advertised-routes*—Routes that are received from a neighbor and advertised.
- *filtered-routes*—Routes that are received from a neighbor and not advertised.
- *received-routes*—Routes that are received from a neighbor.

Modes

EXEC

Usage

Use the `show bgp ipv4 unicast` command to display the BGP IPv4 configuration, including neighbors, routes, and peer-groups.

Example

```
sonic# show bgp ipv4 unicast
BGP routing table information for VRF default
Router identifier 200.9.0.5, local AS number 100
Status codes: R - removed, S - stale, s - suppressed, * - valid, h -
history,
d - damped, > - best, = - multipath, q - queued, r -
RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop        Metric      LocPref  Path
*-> 4.4.4.44/32       14.14.14.1      0          400    ?
*-> 10.59.128.0/20    14.14.14.1      0          400    ?
*-> 13.1.1.0/24       14.14.14.1      0          400    ?
*-> 14.14.14.0/24     14.14.14.1      0          400    ?
*-> 29.2.2.2/32       14.14.14.1      0          400    ?
*-> 192.168.1.0/24    14.14.14.1      0          400    ?
*-> 200.0.0.0/24       14.14.14.1      0          400    ?
```

```
sonic# show bgp ipv4 unicast summary
BGP router identifier 200.9.0.5, local AS number 100
Neighbor          V   AS   MsgRcvd   MsgSent   InQ    OutQ   Up/Down
State/PfxRcd
14.14.14.1        4   400    8         2         0       0      00:00:43 0
```

```
sonic# show bgp ipv4 unicast neighbors
```

```
BGP neighbor is 14.14.14.1, remote AS 400, local AS 100, external link
  Administratively shut down
  BGP version 4, remote router ID , local router ID
  BGP state = ESTABLISHED, up for 00:01:03
  Hold time is seconds, keepalive interval is 60 seconds, negotiated
  hold time is 180 seconds
  Minimum time between advertisement runs is seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                  Sent      Rcvd
  Opens:           1          1
  Notifications: 0          0
  Updates:         2          8
  Keepalive:       2          2
  Route Refresh:  0          0
  Capability:     0          0
  Total:          5         11

  Local host: 14.14.14.4, Local port: 46782
  Foreign host: 14.14.14.1, Foreign port: 179
```

The following example shows the IPv4 routes that are received from neighbors and not advertised:

```
Sonic# show bgp ipv4 unicast neighbors 8.1.1.2 filtered-routes
BGP routing table information for VRF default
Router identifier 8.1.1.1, local AS number 100
Status codes: R - removed, S - stale, s - suppressed, * - valid
              h - history, d - damped, > - best, = - multipath, q -
              queued, r - RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop        Metric      LocPref  Weight
Path
*-> 5.0.0.0/24       8.1.1.2        0          0
200 ?
*-> 172.50.50.0/24    8.1.1.2        0          0
200 ?
```

Releases

3.1 or later

show bgp ipv6

Displays BGP IPv6 configuration.

Command show bgp ipv6 unicast [vrf {vrf-name | all}] [{ip-address | ip-address/prefix} [bestpath | multipath]] | community {AA:NN | local-as | no-advertise | no-export | no-peer} [exact-match] | neighbors [{IPv4-address | IPv6-addresses} | interface {Eth | PortChannel | Vlan}] [advertised-routes | filtered-routes | received-routes | routes] | route-map route-map-name | statistics | summary]

- Options**
- *vrf-name*—VRF name prefixed by vrf (up to 15 characters)
 - *ip-address*—IP address in A.B.C.D format
 - *ip-address/prefix*—IP address with the prefix in A.B.C.D/mask format
 - *AA:NN*—Community number in AA:NN format.
 - *IPv4-address*—IPv4 address of a neighbor.
 - *IPv6-addresses*—IPv6 address of a neighbor.
 - *route-map-name*—Route-map name.
 - *neighbor-ip*—Neighbor IP address in A.B.C.D or AA::NN format .
 - *advertised-routes*—Routes that are received from a neighbor and advertised.
 - *filtered-routes*—Routes that are received from a neighbor and not advertised.
 - *received-routes*—Routes that are received from a neighbor.

Modes EXEC

Usage Use the `show bgp ipv6 unicast` command to display the BGP IPv6 configuration, including BGP neighbors, routes, and peer groups.

Examples

```
sonic# show bgp ipv6 unicast 5001:1111::22
BGP routing table entry for 5001:1111::/64
Paths: (2 available, best #2, table default)
  200
    1002:3333::2 from 1002:3333::2 (2.2.2.2)
      Origin IGP, metric 0, valid, external, multipath
      Community: 600:755 noExport noAdvertise localAs noPeer
      Last update: 2020-05-12 18:09:04
  200
    1001:2222::2 from 1001:2222::2 (2.2.2.2)
      Origin IGP, metric 0, valid, external, multipath, best
      (Older Path)
      Community: 600:755 noExport noAdvertise localAs noPeer
      Last update: 2020-05-12 18:09:04
```

```
sonic# show bgp ipv6 unicast 5001:1111::/64 bestpath
BGP routing table entry for 5001:1111::/64
Paths: (1 available, best #1, table default)
  200
    1001:2222::2 from 1001:2222::2 (2.2.2.2)
      Origin IGP, valid, best
      Community: 600:755 noExport noAdvertise localAs noPeer
      Last update: 2020-05-12 18:09:04
```

```
sonic# show bgp ipv6 unicast community 600:755
BGP routing table information for VRF default
Router identifier 1.1.1.1, local AS number 100
Status codes: R - removed, S - stale, s - suppressed, * - valid, h -
history,
              d - damped, > - best, = - multipath, q - queued, r -
RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop           Metric LocPref Weight Path
* 5001:1111::/64  fe80::92b1:1cff:fef4:ab9b 0      0        200      i
*>                  fe80::92b1:1cff:fef4:ab9b 0      0        200      i
```

```

* 5002:2222::/64 fe80::92b1:1cff:fef4:ab9b 0 0 200 i
*>           fe80::92b1:1cff:fef4:ab9b 0 0 200 i

sonic# show bgp ipv6 unicast community 600:755 exact-match
BGP routing table information for VRF default
Router identifier 1.1.1.1, local AS number 100
Status codes: R - removed, S - stale, s - suppressed, * - valid, h -
history,
d - damped, > - best, = - multipath, q - queued, r -
RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPref Weight Path
* 5002:2222::/64 fe80::92b1:1cff:fef4:ab9b 0 0 200 i
*>           fe80::92b1:1cff:fef4:ab9b 0 0 200 i

sonic# show bgp ipv6 unicast statistics
BGP IPv4 Unicast RIB statistics
Total Advertisements : 5
Total Prefixes : 3
Average prefix length : 64.00
Unaggregateable prefixes : 3
Maximum aggregateable prefixes: 0
BGP Aggregate advertisements : 0
Address space advertised : 5.53402e+19
    % announced :
    /8 equivalent :
    /24 equivalent :
Advertisements with paths : 5
Longest AS-Path (hops) : 1
Average AS-Path length (hops) : 0.80
Largest AS-Path (bytes) : 6
Average AS-Path size (bytes) : 4.80
Highest public ASN : 200

sonic# show bgp ipv6 unicast vrf all
BGP routing table information for VRF default
Router identifier 1.1.1.1, local AS number 100
Status codes: R - removed, S - stale, s - suppressed, * - valid, h -
history,
d - damped, > - best, = - multipath, q - queued, r -
RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPref Weight Path
*> 2211:2211::/64 :: 0 32768 i
* 5001:1111::/64 fe80::92b1:1cff:fef4:ab9b 0 200 i
*>           fe80::92b1:1cff:fef4:ab9b 0 200 i
* 5002:2222::/64 fe80::92b1:1cff:fef4:ab9b 0 200 i
*>           fe80::92b1:1cff:fef4:ab9b 0 200 i

BGP routing table information for VRF Vrf_blue
Router identifier 3.3.3.3, local AS number 300
Route status codes: * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPref Weight Path
*> 2112:3322::/64 :: 0 32768 i

```

The following example shows the IPv6 routes that are received from neighbors and not advertised:

```

Sonic# show bgp ipv6 unicast neighbors 1000::2 filtered-routes
BGP routing table information for VRF default
Router identifier 8.1.1.1, local AS number 100
Status codes: R - removed, S - stale, s - suppressed, * - valid
h - history, d - damped, > - best, = - multipath, q -
queued, r - RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPref Weight Path
*> 2000::2/128 1000::5 0 0 200
?
```

Releases	3.1 or later
-----------------	--------------

show bgp l2vpn evpn es

Displays information about the EVPN Ethernet segment configured on multihomed VTEPs.

Command	show bgp l2vpn evpn es {XX:XX:XX:XX:XX:XX:XX:XX:XX detail}
Options	<ul style="list-style-type: none">• XX:XX:XX:XX:XX:XX:XX:XX—Enter an ES-ID; for example, 00:00:00:00:00:00:00:01.• detail—Displays information for all EVPN Ethernet segments configured on a multihomed VTEP.
Command mode	EXEC
Usage	Use this command to display information about the EVPN Ethernet segment configured on multihomed VTEPs.

Example

```
sonic# show bgp l2vpn evpn es detail
ESI: 03:00:00:00:11:22:33:00:00:01
    Type: LR
    RD: 1.1.1.1:3
    Originator-IP: 1.1.1.1
    Local ES DF preference: 32767
    VNI Count: 2
    Remote VNI Count: 2
    VRF Count: 1
    MACIP EVI Path Count: 2
    MACIP Global Path Count: 5
    Inconsistent VNI VTEP Count: 0
    Inconsistencies: -
    VTEPs:
        4.4.4.4 flags: EA df_alg: preference df_pref: 32767

ESI: 03:00:00:00:11:22:33:00:00:02
    Type: LR
    RD: 1.1.1.1:3
    Originator-IP: 1.1.1.1
    Local ES DF preference: 32767
    VNI Count: 2
    Remote VNI Count: 2
    VRF Count: 1
    MACIP EVI Path Count: 2
    MACIP Global Path Count: 5
    Inconsistent VNI VTEP Count: 0
    Inconsistencies: -
    VTEPs:
        2.2.2.2 flags: EA df_alg: preference df_pref: 32767
        3.3.3.3 flags: EA df_alg: preference df_pref: 32767
        4.4.4.4 flags: EA df_alg: preference df_pref: 32767
```

```
sonic# show bgp l2vpn evpn es 03:00:00:00:11:22:33:00:00:01
ESI: 03:00:00:00:11:22:33:00:00:01
    Type: LR
    RD: 1.1.1.1:3
    Originator-IP: 1.1.1.1
    Local ES DF preference: 32767
    VNI Count: 2
    Remote VNI Count: 2
    VRF Count: 1
    MACIP EVI Path Count: 2
    MACIP Global Path Count: 5
    Inconsistent VNI VTEP Count: 0
    Inconsistencies: -
    VTEPs:
        2.2.2.2 flags: EA df_alg: preference df_pref: 32767
```

Releases	4.2.0 or later
-----------------	----------------

show bgp l2vpn evpn es-evi

Displays information about EVPN Ethernet segment and EVI configured on multihomed VTEPs.

Command	show bgp l2vpn evpn es-evi [vni detail]
Options	<ul style="list-style-type: none">• <i>vni</i>—Enter a VXLAN network identifier (VNI) for a tenant segment (1-16777215).• <i>detail</i>—Displays information for all EVPN Ethernet segments and the associated VXLAN IDs configured on a multihomed VTEP.
Command mode	EXEC
Usage	Use this command to display information about EVPN Ethernet segments and EVI configured on multihomed VTEPs.
Example	<pre>sonic# show bgp l2vpn evpn es-evi detail VNI: 100 ESI: 03:00:00:00:11:22:33:00:00:01 Type: LR Inconsistencies: - VTEPs: 2.2.2.2(EV) VNI: 200 ESI: 03:00:00:00:11:22:33:00:00:01 Type: LR Inconsistencies: - VTEPs: 2.2.2.2(EV) sonic# show bgp l2vpn evpn es-evi 100 VNI: 100 ESI: 03:00:00:00:11:22:33:00:00:01 Type: LR Inconsistencies: - VTEPs: 2.2.2.2(EV) sonic# show bgp l2vpn evpn es-evi Flags: L local, R remote, I inconsistent VTEP-Flags: E EAD-per-ES, V EAD-per-EVI VNI ESI Flags VTEPs 101007 00:00:00:11:22:33:00:00:00:01 LR 2.2.2.2(EV),3.3.3.3(EV),4.4.4.4(EV) 101007 00:00:00:55:00:66:00:00:00:01 R 5.5.5.5(V),6.6.6.6(V) 101007 01:54:bf:64:bd:d7:42:00:35:00 R 3.3.3.3(EV),4.4.4.4(EV),5.5.5.5(EV),6.6.6.6(EV) 101007 03:00:00:00:44:44:44:00:00:36 R 5.5.5.5(EV),6.6.6.6(EV) 101107 00:00:00:11:22:33:00:00:00:01 LR 2.2.2.2(EV),3.3.3.3(EV),4.4.4.4(EV) 101107 00:00:00:55:00:66:00:00:00:01 R 5.5.5.5(V),6.6.6.6(V) 101107 01:54:bf:64:bd:d7:42:00:35:00 R 3.3.3.3(EV),4.4.4.4(EV),5.5.5.5(EV),6.6.6.6(EV) 101107 03:00:00:00:44:44:44:00:00:36 R 5.5.5.5(EV),6.6.6.6(EV)</pre>
Releases	4.2.0 or later

show bgp l2vpn evpn es-vrf

Displays information about the Ethernet Segment against the VRF configured on multihomed VTEPs.

Command	show bgp l2vpn evpn es-vrf [XX:XX:XX:XX:XX:XX:XX:XX:XX:XX]
Options	XX:XX:XX:XX:XX:XX:XX:XX:XX—Enter a 10-byte ID with the type byte set to 0 for an ES-ID; for example, 00:00:00:00:00:00:00:0a:00:01.
Command mode	EXEC
Usage	Use this command to view information about the Ethernet Segment against the corresponding VRF.

Example

```
sonic# show bgp l2vpn evpn es-vrf 00:00:00:11:22:33:00:00:00:01
ES-VRF Flags: A Active
ESI VRF Flags: IPv4-NHG IPv6-NHG
Ref VRF Vrf042 A 70312501 70312502 16
00:00:00:11:22:33:00:00:00:01 VRF Vrf048 A 70312503 70312504 16
00:00:00:11:22:33:00:00:00:01 VRF Vrf063 A 70312505 70312506 16
00:00:00:11:22:33:00:00:00:01 VRF Vrf012 A 70312507 70312508 16
00:00:00:11:22:33:00:00:00:01 VRF Vrf027 A 70312509 70312510 16
00:00:00:11:22:33:00:00:00:01 VRF Vrf055 A 70312511 70312512 16
```

Releases

4.2.0 or later

show bgp l2vpn evpn next-hops

Displays information about the next hops in BGP EVPN routes.

Command show bgp l2vpn evpn next-hops

Options None

Modes EXEC

Usage The BGP EVPN next-hop IP address for base destination paths is displayed for each tenant VRF.

Example

```
sonic# show bgp l2vpn evpn next-hops
VRF IP RMAC #Paths Base Path
Vrf016 5.5.5.5 18:5a:58:b1:83:25 1120 172.16.250.23/32
Vrf016 6.6.6.6 18:5a:58:b1:a3:a5 1112 172.16.255.13/32
Vrf016 ::ffff:3.3.3.3 8c:04:ba:b5:e5:c2 128 2001:172:16:f6::2/128
Vrf016 ::ffff:4.4.4.4 8c:04:ba:b5:f0:42 128 2001:172:16:f0::2/128
Vrf016 3.3.3.3 8c:04:ba:b5:e5:c2 616 172.16.254.103/32
Vrf016 4.4.4.4 8c:04:ba:b5:f0:42 632 172.16.253.104/32
Vrf016 ::ffff:5.5.5.5 18:5a:58:b1:83:25 256 2001:172:16:fe::3/128
Vrf016 2.2.2.2 0c:29:ef:e3:bf:82 112 172.16.254.102/32
Vrf016 ::ffff:7.7.7.7 18:5a:58:a3:40:61 128 2001:172:16:f9::4/128
```

Releases

4.2.0 or later

show bgp l2vpn evpn route

Displays BGP EVPN route information.

Command show bgp l2vpn evpn route {[rd] {rdvalue {[mac] {macvalue {ip ipvalue}}}} | {[type] {ead | es | macip | multicast | prefix}}}}

Options

- *rdvalue*—(Optional) RD value in A.B.C.D:NN or ASN:NN format
- *macvalue*—MAC address value in nn:nn:nn:nn:nn:nn format
- *ipvalue*—IP address value in A.B.C.D or A::B format
- *ead*—Ethernet auto-discovery EVPN route type
- *es*—Ethernet segment EVPN route type
- *macip*—MAC + IP EVPN route type
- *multicast*—Multicast EVPN route type
- *prefix*—Prefix EVPN route type

Modes EXEC

Usage Use this command to display all the BGP EVPN routes.

Example

```
sonic# show bgp l2vpn evpn route
BGP table version is 33, local router ID is 2.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, q queued,
r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[EthTag]:[ESI]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
```

```

EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]
      Network          Next Hop          Metric LocPrf Weight Path
      Extended Community
Route Distinguisher: 61101:1
*>   [5]:[0]:[24]:[172.16.0.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.1.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.2.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.3.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.4.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.5.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.6.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.7.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.8.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.9.0]
      1.1.1.1           0             32768 ?
      ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
*>   [5]:[0]:[24]:[172.16.10.0]

```

Releases

3.0 or later

show bgp l2vpn evpn route detail type

Displays BGP EVPN routes of a specified type in detail.

Command show bgp l2vpn evpn route detail [type {ead | es | macip | multicast | prefix}]

Options

- ead—Ethernet auto-discovery EVPN route type
- es—Ethernet segment EVPN route type
- macip—MAC + IP EVPN route type
- multicast—Multicast EVPN route type
- prefix—Prefix EVPN route type

Modes

EXEC

Usage

Use this command to display the detail information of all BGP EVPN routes.

Example

```

sonic# show bgp l2vpn evpn route detail
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]
BGP routing table entry for 11:11:[5]:[0]:[0]:[0.0.0.0]
Paths: (1 available, best #1)
Zebra Add: 6d21h36m
Advertised to non peer-group peers:
 10.1.1.2
Route [5]:[0]:[0]:[0.0.0.0] VNI 0
Local
 0.0.0.0 from 0.0.0.0 (10.59.142.127)
Origin IGP, weight 32768, valid, sourced, local, best (First path received)
Extended Community: ET:8
Last update: Wed Feb 12 17:06:15 2020
BGP routing table entry for 11:11:[5]:[0]:[0]:[::]

```

```

Paths: (1 available, best #1)
Zebra Add: 6d21h36m
Advertised to non peer-group peers:
10.1.1.2
Route [5]:[0]:[0]:[::] VNI 0
Local
0.0.0.0 from 0.0.0.0 (10.59.142.127)
Origin IGP, weight 32768, valid, sourced, local, best (First path
received)
Extended Community: ET:8
Last update: Wed Feb 12 17:06:15 2020
Displayed 2 prefixes (2 paths) with this RD (of requested type)

```

```

sonic# show bgp l2vpn evpn route detail type prefix
BGP routing table entry for 3.3.3.3:5160:[5]:[0]:[0]:[::]
Paths: (0 available, no best path)
    Zebra Add: 1d00h37m
        Not advertised to any peer
BGP routing table entry for 3.3.3.3:5160:[5]:[0]:[24]:[153.0.0.0]
Paths: (0 available, no best path)
    Zebra Add: 1d00h37m
        Not advertised to any peer
BGP routing table entry for 3.3.3.3:5160:[5]:[0]:[24]:[153.0.0.0]
Paths: (0 available, no best path)
    Zebra Add: 1d00h37m
        Not advertised to any peer
Route Distinguisher: 3.3.3.3:5160
BGP routing table entry for 3.3.3.3:5160:[5]:[0]:[24]:[153.1.1.0]
Paths: (6 available, best #6)
    Zebra Add: 1d00h37m
        Advertised to non peer-group peers:
        Ethernet50 Ethernet54 PortChannel11 PortChannel12 Vlan11 Vlan12
        Route [5]:[0]:[24]:[153.1.1.0] VNI 102000
        65500 65502
            3.3.3.3 from PortChannel12 (20.20.20.20)
            Origin incomplete, valid, external
            Extended Community: RT:65502:102000 ET:8 Rmac:8c:04:ba:bb:ba:40
            Last update: Wed Dec 2 23:38:26 2020
--more--

```

Releases

3.0 or later

show bgp l2vpn evpn route rd

Displays BGP EVPN routes for a specific RD in detail.

Command show bgp l2vpn evpn route rd rdvalue

Options rdvalue—RD in A.B.C.D:NN or ASN:NN format

Command mode EXEC

Usage Use this command to display EVPN routes with specific RD.

Example

```

sonic# show bgp l2vpn evpn route rd 61101:1
EVPN type-1 prefix: [1]:[EthTag]:[ESI]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]
BGP routing table entry for 61101:1:[5]:[0]:[24]:[172.16.0.0]
Paths: (1 available, best #1)
    Advertised to non peer-group peers:
    Ethernet56 Ethernet64 PortChannel11 PortChannel12 Vlan4001 Vlan4002 Vlan4021 Vlan4022
    Route [5]:[0]:[24]:[172.16.0.0] VNI 1103001
    Local
        1.1.1.1 from 0.0.0.0 (2.0.0.1)
            Origin incomplete, metric 0, weight 32768, valid, sourced, local, best (First path
received)
            Extended Community: ET:8 RT:65501:1103001 Rmac:00:a0:c9:00:00:02
            SubType: 1 Last update: Wed Apr 3 10:19:03 2024

```

Releases

3.1 or later

show bgp l2vpn evpn route type

Displays BGP EVPN routes of a specified type.

Command show bgp l2vpn evpn route type {ead | es | macip | multicast | prefix}

Options

- ead—Ethernet auto-discovery EVPN route type
- es—Ethernet segment EVPN route type
- macip—MAC + IP EVPN route type
- multicast—Multicast EVPN route type
- prefix—Prefix EVPN route type

Modes

EXEC

Usage

Use this command to display all BGP EVPN routes.

Example

```
sonic# show bgp l2vpn evpn route type prefix
BGP table version is 10, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]
      Network          Next Hop           Metric LocPrf Weight Path
      Extended Community
Route Distinguisher: 3.3.3.3:5160
*   [5]:[0]:[24]:[153.1.1.0]
      3.3.3.3
      RT:65502:102000 ET:8 Rmac:8c:04:ba:bb:ba:40          0 65500 65502 ?
*   [5]:[0]:[24]:[153.1.1.0]
      3.3.3.3
      RT:65502:102000 ET:8 Rmac:8c:04:ba:bb:ba:40          0 65500 65502 ?
*   [5]:[0]:[24]:[153.1.1.0]
      3.3.3.3
      RT:65502:102000 ET:8 Rmac:8c:04:ba:bb:ba:40          0 65500 65502 ?
*   [5]:[0]:[24]:[153.1.1.0]
      3.3.3.3
      RT:65502:102000 ET:8 Rmac:8c:04:ba:bb:ba:40          0 65500 65502 ?
*   [5]:[0]:[24]:[153.1.1.0]
      3.3.3.3
      RT:65502:102000 ET:8 Rmac:8c:04:ba:bb:ba:40          0 65500 65502 ?
*   [5]:[0]:[24]:[153.1.1.0]
      3.3.3.3
      RT:65502:102000 ET:8 Rmac:8c:04:ba:bb:ba:40          0 65500 65502 ?
--more--
```

Releases

3.0 or later

show bgp l2vpn evpn route vni

Displays BGP EVPN routes for a specified VNI.

Command show bgp l2vpn evpn route vni *vni number*

Options *vni number*—VNI number

Command mode EXEC

Usage Use this command to display BGP EVPN routes for a specific VNI.

Example

```
sonic# show bgp l2vpn evpn route vni 1001
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]
      Network          Next Hop           Metric LocPrf Weight Path
      Extended Community
*   [2]:[0]:[48]:[00:00:00:01:03]:[32]:[101.1.1.253]
      45.45.45.45
      RT:65502:1001 ET:8 Default Gateway          0 65500 65502 i
*   [2]:[0]:[48]:[00:00:00:01:03]:[32]:[101.1.1.253]
```

```

        45.45.45.45                               0 65500 65502 i
* [2]:[0]:[48]:[00:00:00:01:03]:[32]:[101.1.1.253]
        45.45.45.45                               0 65500 65502 i
* [2]:[0]:[48]:[00:00:00:01:03]:[32]:[101.1.1.253]
        45.45.45.45                               0 65500 65502 i
* [2]:[0]:[48]:[00:00:00:01:03]:[32]:[101.1.1.253]
        45.45.45.45                               0 65500 65502 i
--more--

```

Releases 3.1 or later

show bgp l2vpn evpn summary

Displays BGP summarized information for BGP L2VPN EVPN address-family including neighbors with EVPN address-family activated.

Command show bgp l2vpn evpn summary

Options None

Modes EXEC

Usage Use this command to display BGP summarized information for BGP L2VPN EVPN address-family including neighbors with EVPN address-family activated.

Example

```

sonic# show bgp l2vpn evpn summary
BGP router identifier 2.0.0.1, local AS number 65501 VRF default
Neighbor          V   AS      MsgRcvd  MsgSent  InQ   OutQ
Up/Down           State/PfxRcd
Ethernet56        4   65500   184869  208134  0     0
5d02h16m          166673
Ethernet64        4   65500   188137  208134  0     0
5d02h16m          166673
PortChannel11     4   65500   184869  208134  0     0
5d02h16m          166673
PortChannel121    4   65500   188137  208134  0     0
5d02h16m          166673
Vlan4001          4   65500   184869  208134  0     0
5d02h16m          166673
Vlan4002          4   65500   184869  208134  0     0
5d02h16m          166673
Vlan4021          4   65500   188137  208134  0     0
5d02h16m          166673
Vlan4022          4   65500   188137  208134  0     0
5d02h16m          166673
Total number of neighbors 8
Total number of neighbors established 8

```

Releases 3.0 or later

show bgp l2vpn evpn vni

Displays VNI information.

Command show bgp l2vpn evpn vni *vni num*

Options *vni num*—VNI number

Modes EXEC

Usage Use this command to display the BGP EVPN tributes for a specific VNI.

Example

```
sonic# show bgp 12vpn evpn vni 100001
VNI: 100001(known to the kernel)
  Type: L2
  RD: 2.0.0.1:1
  Originator IP: 1.1.1.1
  Originator External IP: 0.0.0.0
  Mcast group: 0.0.0.0
  Advertise-gw-macip: False
  Advertise-svi-macip: False
  Import Route Target:
    65501:100001
  Export Route Target:
    65501:100001
sonic#
```

Releases

3.0 or later

show buffer interface

Displays ingress priority group and egress queue mappings to buffer profiles.

Command `show buffer interface Ethernet {all | slot/port {priority-group | queue}}`

Options

- `all | slot/port`—Displays priority group or queue mapping on all interfaces or a specified interface.
- `priority-group`—Displays priority group-to-buffer profile configuration.
- `queue`—Displays queue-to-buffer profile configuration.

Modes

EXEC

Usage

Use this command to display ingress priority group and egress queue mappings to buffer profiles.

Examples

```
s$ sonic# show buffer interface Ethernet all priority-group
Interface  Priority-group      Profile
Ethernet0      0                ingress_lossy_profile
Ethernet4      3-4              ingress_lossless_profile
...
sonic# show buffer interface Ethernet0 priority-group
Interface  Priority-group      Profile
Ethernet0      0                ingress_lossy_profile

sonic# show buffer interface Ethernet all queue
Interface     Queue      Profile
Ethernet0      0          ingress_lossy_profile
Ethernet4      3-4      ingress_lossless_profile
...
sonic# show buffer interface Ethernet0 queue
Interface     Queue      Profile
Ethernet0      0          ingress_lossy_profile
```

Releases

4.0. or later

show buffer-pool

Displays persistent watermark counters recorded by the system.

Command `show buffer-pool {persistent-watermark | watermark} [percentage] [interface Ethernet port]`

Options

- `persistent-watermark`—Display persistent-watermark counters.

- `watermark`—Display user watermark counters.
- `interface`—Display watermark counters for an interface.
- `percentage`—Display watermark counters in percentage.
- `port`—Port information.

Modes

EXEC

Usage

Use this command to display user or persistent watermark counters recorded by the system. The `show buffer-pool` command is not supported on Z9432F-ON, Z9664F-ON, and Z9864F-ON switches.

Examples

```
sonic# show buffer-pool watermark
-----
Pool                      Bytes (Total)      Bytes (Multicast)
-----
egress_lossless_pool      23183104        3539712
egress_lossy_pool          0                  0
ingress_lossless_pool     23187712        0

sonic# show buffer-pool persistent-watermark percentage
-----
Pool                      Percent (Total)    Percent (Multicast)
-----
egress_lossless_pool      70                 10
egress_lossy_pool          0                  0
ingress_lossless_pool     100                0

sonic# show buffer-pool persistent-watermark percentage interface
Ethernet 47
-----
Pool                      Percent (Total)    Percent (Unicast)
-----
egress_lossy_pool          0                 0
ingress_lossless_pool      10                0
egress_lossless_pool       0                 0
```

Releases

4.0 or later

show buffer profile

Displays QoS buffer profile configurations.

Command `show buffer profile`

Options None

Modes EXEC

Usage Use this command to display the ingress and egress buffer profile settings for loss and lossless pools.

Examples

```
sonic# show buffer profile
Profile egress_lossless_profile:
  mode           : static
  pool          : egress_lossless_pool
  size          : 0
  static_threshold : 32575488 byte
```

Releases

4.1.0 or later

show ca-crypto cert

Displays information about CA certificates.

Command show crypto ca-cert {certificate-name | all}

Options • *certificate-name* — Display information about a specified CA certificate.

• *all* — Display information about all CA certificates.

Modes EXEC

Usage Use this command to display installed CA certificates. Use the [show crypto cert](#) command to display information about host certificates.

Example

```
sonic# show crypto ca-cert CA
Certificate Name: CA.crt
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      64:f2:8f:46:09:68:73:34:46:d4:53:94:2c:fc:1f:12:06:6c:ee:8c
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = US, ST = CA, L = Sacramento, O = Dell, OU =
Networking, CN = www.dell.com
    Validity
      Not Before: Jul 7 20:24:34 2022 GMT
      Not After : Jul 4 20:24:34 2032 GMT
    Subject: C = US, ST = CA, L = Sacramento, O = Dell, OU =
Networking, CN = www.dell.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:ea:27:4f:1e:9f:03:97:3f:77:f1:48:6a:29:46:
        86:ef:d9:d1:ec:e1:d0:93:28:88:f6:36:47:66:21:
        00:92:d9:d3:65:8d:3c:bc:80:ac:8f:22:ee:cd:20:
        5e:ec:47:13:e1:a8:85:20:01:73:30:94:8c:6a:0a:
        73:93:3c:0a:e5:f6:b1:0a:f5:ad:c1:0b:e2:84:3c:
        a6:5b:5f:7d:b8:71:da:ab:46:88:03:e8:42:63:52:
        76:8f:1d:3e:1a:c1:d4:dc:55:75:b8:8f:af:03:19:
        95:d3:84:62:e9:f9:1b:6c:9d:ff:a7:f6:8e:32:2f:
        32:7f:5d:05:79:84:e3:f4:cd:78:59:49:80:18:a8:
        d6:c5:6d:54:2d:07:1a:16:e0:ce:15:f4:c6:2c:ae:
        f5:8f:a1:89:aa:37:79:ea:1a:75:dd:11:df:ee:8a:
        87:ed:4e:3c:3a:54:96:d4:13:75:a0:af:57:94:b0:
        d5:13:80:3d:de:54:9b:e2:56:6b:1e:a1:d2:fd:93:
        d2:3b:77:7c:b7:c8:e9:7d:d0:5d:a1:dc:89:0e:a6:
        c4:82:e6:fc:15:4c:6a:df:45:8c:ab:0b:07:cf:49:
        b7:53:ee:2a:84:5a:ac:29:09:7c:ee:5a:ff:94:19:
        e2:7b:3f:11:7b:f7:dd:5b:2a:da:99:98:59:b8:07:
        23:e9
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:TRUE
    X509v3 Key Usage:
      Digital Signature, Non Repudiation, Key Encipherment,
  Certificate Sign
    Signature Algorithm: sha256WithRSAEncryption
      63:9a:e3:b4:b7:10:d7:fa:92:cd:04:7b:f4:6a:c3:5e:7c:11:
      c6:e6:9e:eb:61:60:97:cf:ad:60:03:ab:89:0f:e2:f1:5b:94:
      7f:dd:6e:21:e9:21:60:0a:8d:81:ec:7e:35:84:b6:97:5e:65:
      07:c4:e2:44:7c:8e:8c:7e:20:94:29:6d:32:e7:dc:6c:70:5d:
      64:ed:cc:3a:d8:83:11:84:26:ab:87:f2:ce:05:8f:29:d2:0f:
      62:de:a2:d9:86:cb:d4:7f:1c:60:f8:38:e3:41:9b:13:6d:24:
      b4:eb:0d:ac:8b:5f:96:d4:0a:5c:26:aa:20:d3:c0:f8:06:24:
      84:3d:d0:1b:e0:33:99:49:5e:3c:f9:77:68:94:d7:f2:11:be:
      39:41:2a:44:5d:9e:a6:b6:a7:02:14:f4:02:6f:f1:f8:71:a5:
      c2:ac:94:39:5d:b6:68:7d:00:5a:e5:92:74:5c:f7:52:5e:2d:
      6a:4f:a6:0c:a6:1b:c1:ff:a9:46:1f:3c:5e:a1:16:fa:72:55:
```

```
1b:84:d2:a8:25:b1:c8:f2:35:97:e0:02:2c:08:9c:e3:69:0e:
2e:0d:9c:f1:98:25:28:06:dc:57:59:9d:bb:48:97:02:63:16:
80:80:b9:1e:5d:13:10:a7:8a:1c:84:2d:aa:7d:ec:3e:67:a0:
14:b5:d9:6a
```

Releases

4.1.0 or later

show cable-diagnostics

Displays cable diagnostic information.

Command show cable-diagnostics { cable-length | report } [Ethernet [port-port]]

Options

- **cable-length** — Show cable-length information
- **report** — Show the test report
- **Ethernet [port-port]** — Ethernet details

Modes

None

Usage

Use this command to display the test reports of one particular port or the ports in a specific range, or all the ports when port information is not specified.

Examples

Test report:

Interface	Type	Length	Result	Status	Timestamp
Ethernet0 08:11:39	SFP	3m	N/A	COMPLETED	29-Apr-2021
Ethernet1 08:11:39	SFP	3m	N/A	COMPLETED	29-Apr-2021
Ethernet2 08:11:40	SFP	3m	N/A	COMPLETED	29-Apr-2021
Ethernet3 08:11:40	SFP	3m	N/A	COMPLETED	29-Apr-2021
Ethernet4 08:11:40	SFP	10000m	N/A	COMPLETED	29-Apr-2021
Ethernet5 08:11:40	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021
Ethernet6 08:11:41	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021
Ethernet7 08:11:41	SFP	300m	Lo RxPwr	COMPLETED	29-Apr-2021
Ethernet8 08:11:41	SFP	10000m	N/A	COMPLETED	29-Apr-2021
Ethernet9 08:11:41	SFP	10000m	N/A	COMPLETED	29-Apr-2021
Ethernet10 08:11:41	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021
Ethernet11 08:11:42	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021
Ethernet12 08:11:42	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021

Report specific for interface range:

Interface	Type	Length	Result	Status	Timestamp	
Ethernet5	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021	08:11:40
Ethernet6	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021	08:11:41
Ethernet7	SFP	300m	Lo RxPwr	COMPLETED	29-Apr-2021	08:11:41
Ethernet8	SFP	10000m	N/A	COMPLETED	29-Apr-2021	08:11:41
Ethernet9	SFP	10000m	N/A	COMPLETED	29-Apr-2021	08:11:41
Ethernet10	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021	08:11:41
Ethernet11	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021	08:11:42
Ethernet12	SFP	80m	Lo RxPwr	COMPLETED	29-Apr-2021	08:11:42

Cable length information:

```
sonic# show cable-diagnostics cable-length
Interface      Type      Length
-----  -----
Ethernet0       SFP       3m
Ethernet1       SFP       3m
Ethernet2       SFP       3m
Ethernet3       SFP       3m
Ethernet4       SFP      10000m
Ethernet5       SFP      80m
Ethernet6       SFP      80m
Ethernet7       SFP      300m
Ethernet8       SFP      10000m
Ethernet9       SFP      10000m
Ethernet10      SFP      80m
Ethernet11      SFP      80m
Ethernet12      SFP      80m
```

Cable length information specific to interface range:

```
sonic# show cable-diagnostics cable-length Ethernet0-9
Interface      Type      Length
-----  -----
Ethernet0        9m
Ethernet1        9m
Ethernet2        9m
Ethernet3        9m
Ethernet4
Ethernet5
Ethernet6        10m
Ethernet7        10m
Ethernet8        9m
Ethernet9        7m
```

Releases

4.0 or later

show class-map

Displays class-map information.

Command `show class-map { [show-fbs-class-name] | [match-type]}] {acl | fields | copp}`

Options `show-fbs-class-name`—(Optional) Display FBS class name

Modes EXEC

Usage Use this command to view the configured class-maps on the switch.

Example

```
sonic# show class-map class_permit_ip
Class-map class_permit_ip match-type fields
  Description:
  Match:
  Referenced in flows:
    policy policy_qos at priority 10
    policy policy_vrf at priority 10
```

Releases

3.1 or later

show clock

Displays system date and time.

Command `show clock`

Options	None
Modes	EXEC
Usage	Use this command to view the system date and time.
Example	<pre>sonic# show clock Thu, 07 Jan 2021 21:58:31 UTC</pre>
Releases	3.1 or later

show config-key password-encrypt

Displays primary encryption key information.

Command	show config-key password-encrypt
Options	None
Modes	EXEC
Usage	Use this command to display if the primary encryption key is configured or not.
Examples	<pre>sonic# show config-key password-encrypt Primary encryption key configured : True</pre>
Releases	4.0 or later

show configuration

Displays the configuration in the current mode.

Command	show configuration
Options	None
Modes	CONFIGURATION
Usage	Use this command to verify the configurations in the current mode.
Examples	<pre>sonic(config)# router bgp 50 vrf VrfYellow sonic(config-router-bgp)# show configuration ! router bgp 50 vrf VrfYellow timers 500 3000 ! address-family ipv4 unicast ! neighbor interface Ethernet8 description bgp-neighbor capability dynamic passive sonic(config-router-bgp)# neighbor interface Ethernet 8 sonic(config-router-bgp-neighbor)# show configuration ! neighbor interface Ethernet8 description bgp-neighbor capability dynamic passive sonic(config)# bfd sonic(config-bfd)# show configuration ! bfd</pre>

```

peer 192.168.2.1 interface Ethernet0
  detect-multiplier 5
  echo-interval 200
  echo-mode
  receive-interval 200
  transmit-interval 200
!
peer 192.168.2.1 multihop local-address 192.168.2.2
  detect-multiplier 4
  receive-interval 150
  transmit-interval 150
!
```

```

sonic# interface Ethernet 0
sonic(config-if-Ethernet0)# show configuration
!
interface Ethernet8
  mtu 9100
  speed 100000
  switchport access Vlan 51
  switchport trunk allowed Vlan 52-56,58,60,62-64
```

```

sonic(conf)# interface PortChannel 5
sonic(config-if-po5)# show configuration
!
interface PortChannel 5
  mtu 5000
  ip vrf forwarding VrfYellow
  ip address 6.6.6.1/24
```

Releases

3.1 or later

show consistency-check status

Displays the status of the consistency checker.

Command `show consistency-check status [access-list [brief | detail] | route]`

Options

- `access-list`—(Optional) Shows the status of access-list consistency-checker
- `brief`—(Optional) Shows the final status of all ACL entries verified
- `detail`—(Optional) Shows the detail of matches and actions of all ACL entries verified
- `route`—(Optional) Shows the status of route consistency-checker

Modes

EXEC

Usage

After running the consistency-check for routes or ACL, use this command to check the status of consistency check and information of inconsistent routes or ACL.

Examples

Status:

```

sonic# show consistency-check status
-----
Feature           Consistency-status
-----
Access-list       Please run the check to get the status
Route            Consistent
```

Route status:

```

sonic# show consistency-check status route
Last Route consistency check ran at 01/19/2022, 23:31:39(UTC) took 3.01
seconds
Final Route consistency check status: Consistent
  Route check for vrf default and address-family ipv4:
    rib_vs_appdb: Consistent
```

```

rib_vs_asicdb: Consistent
rib_vs_fib: Consistent
rib_vs_sai: Consistent
Route check for vrf default and address-family ipv6:
rib_vs_appdb: Consistent
rib_vs_asicdb: Consistent
rib_vs_fib: Consistent
rib_vs_sai: Consistent

```

```

sonic# show consistency-check status access-list
Final status: Consistent
MAC access-list consistency status: Consistent
    ACLs checked: 9
    ACL entries checked: 135
IPv4 access-list consistency status: Consistent
    ACLs checked: 11
    ACL entries checked: 1487
Last ran on Mar 18 2022 at 06:11:08 (UTC) and took 19.82 seconds

```

Releases

4.0 or later

show copp

Displays the CoPP configuration.

Command

`show copp {classifiers | protocols | actions | policy}`

Options

None

Modes

EXEC

Usage

Displays the CoPP action groups, CoPP classifiers, CoPP policy and supported CoPP protocols.

Example

```

sonic# show copp classifiers
Classifier match-type copp
    protocol arp_req
    protocol arp_resp
    protocol neigh_discovery
Classifier match-type copp
    protocol bgp

```

```

sonic# show copp protocols
Classifier match-type copp protocols
protocol stp
protocol lacp
protocol eapol
protocol lldp
protocol pvrst

```

```

sonic# show copp actions
CoPP action group copp-system-arp
    trap-action copy
    trap-priority 3
    trap-queue 3
    police cir 6000 cbs 6000
        meter-type packets
        mode sr_tcm
        red-action drop
CoPP action group copp-system-bgp
    police cir 7000 cbs 7000

```

```

sonic# show copp policy
Policy copp-system-policy Type copp
    Flow copp-system-arp
        trap-action copy

```

```
trap-priority 3
trap-queue 3
police cir 6000 cbs 6000
    meter-type packets
    mode sr_tcm
    red-action drop
```

Releases

3.1 or later

show core config

Displays if the COREDUMP feature is administratively enabled or disabled.

Command show core config**Options** None**Modes** EXEC**Usage** Use this command to view if the COREDUMP feature is enabled or disabled. If the feature is enabled, COREDUMP is generated and stored during software exceptions.**Examples**

```
sonic# show core config
Coredump : Enabled
```

```
sonic# show core config
Coredump : Disabled
```

Releases

3.1 or later

show core info

Displays detailed information about core problems for troubleshooting crashes.

Command show core info key**Options** key—Process ID or executable name to match against**Modes** EXEC**Usage** If multiple core dump files are found that match the specified condition, all core file information displays.**Table 6. Core information for troubleshooting**

Field	Description
Time	Time of the crash as reported by the kernel in UTC.
Executable	Full path to the application executable that has been unresponsive.
Core File	File name of the application core dump of the executable that has been unresponsive.
PID	Identifier of the process that is unresponsive.
User ID	User identifier of the process that is unresponsive.
Group ID	Group identifier of the process that is unresponsive.
Signal	Signal that caused the process to crash.

Table 6. Core information for troubleshooting (continued)

Field	Description
Command Line	Command-line argument of the process that is unresponsive.
Boot ID	Unique identifier of the local system that is generated and set on each system boot-up event.
Machine ID	Unique machine identifier of the local system that is set during installation.
Core File Found	Indicates if the capture core file exists on the local disk or has been removed.
Crash Message	Copy of the application stack trace information of the process that is unresponsive.

Example

```
sonic# show core info clish
Time          : 2020-05-16 11:54:33
Executable    : /usr/sbin/cli/clish
Core File     : /var/lib/systemd/coredump/
core.clish.1000.8f1cad11c59840318a6df3aa6ed3633e.26480.1589630073000000000000.1z4
PID           : 26480
User ID       : 1000
Group ID      : 1000
Signal         : 11
Command Line   : /usr/sbin/cli/clish
Boot ID        : 8f1cad11c59840318a6df3aa6ed3633e
Machine ID     : fc0a437952314ee5a585a94ceaa480af
Core File Found: present
Crash Message  :
Process 26480 (clish) of user 1000 dumped core.
Stack trace of thread 152:
#0 0x00007f30f516357a PyEval_EvalFrameEx (libpython2.7.so.1.0)
#1 0x00007f30f52cc29c PyEval_EvalCodeEx (libpython2.7.so.1.0)
#2 0x00007f30f5220670 n/a (libpython2.7.so.1.0)
#3 0x00007f30f51b85c3 PyObject_Call (libpython2.7.so.1.0)
#4 0x00007f30f52cb6c7 PyEval_CallObjectWithKeywords (libpython2.7.so.1.0)
#5 0x00007f30ebb2f43a n/a (/usr/sbin/cli/.libs/clish_plugin_clish.so)
```

Releases

3.1 or later

show core list

Displays a summary of the core files generated by the kernel.

Command show core list**Options** None**Modes** EXEC

- Usage**
- TIME — Time of the crash as reported by the kernel in UTC
 - PID — Identifier of the process that crashed
 - SIG — Signal that caused the process to crash
 - COREFILE — Indicates if the capture core file exists on the local disk or has been removed
 - EXEC — Applicable executable that has crashed

Example

```
sonic# show core list
      TIME          PID  SIG  COREFILE  EXE
2020-05-16 11:54:33      26480  11  present  clish
2020-05-15 01:25:16      6195   11  present  crashme
2020-05-15 00:45:28     13604   11  present  crashme
2020-05-14 02:11:11     3197   11  present  crashme
2020-05-13 01:10:56     17844   11  missing  crashme
2020-05-13 01:10:55     17728   11  present  crashme
```

Releases	3.1 or later
-----------------	--------------

show crm

Displays summary information about critical resource monitoring (CRM).

Command	show crm [summary]
Options	summary—Displays a summary of CRM settings.
Modes	EXEC
Usage	Use this command to check the hardware resources usage and availability.
Examples	<pre>sonic# show crm summary ----- Attribute Value/State ----- Polling Interval 10 second(s)</pre>

Releases	4.2.1 or later
-----------------	----------------

show crm resources

Displays information about monitored critical resources.

Command	show crm resources {acl {group table} all dnat fdb ipmc ipv4 {neighbor nexthop route} ipv6 {neighbor nexthop route} nexthop group {member object} snat}
Options	Enter a CRM resource. Valid values are: <ul style="list-style-type: none">• acl group — ACL counter resources and group entries.• acl table — ACL table resources• all — Use the all value to view information about all CRM resources.• dnat — Destination Network Address Translation (NAT) entries• fdb — MAC forwarding database (FDB) entries• ipmc — IP multicast entries• ipv4 neighbor — IPv4 neighbor entries• ipv4 nexthop — IPv4 next-hop entries• ipv4 route — IPv4 route entries• ipv6 neighbor — IPv6 neighbor entries• ipv6 nexthop — IPv6 next-hop entries• ipv6 route — IPv6 route entries• nexthop group member — Next-hop group member resources• nexthop group object — Next-hop group object resources• snat — Source Network Address Translation entries
Modes	EXEC
Usage	Use the show crm resources command to check the number of used and available ASIC resources.
Examples	<pre>sonic# show crm resources snat Resource Name Used Count Available Count ----- snat_entry 2 1021 sonic# show crm resources dnat Resource Name Used Count Available Count</pre>

dnat_entry	2	1021
------------	---	------

```
sonic# show crm resources ipv4 neighbor
Resource Name          Used Count   Available Count
----- ----- -----
ipv4_neighbor           60          31616
```

```
sonic# show crm resources ipv4 nexthop
Resource Name          Used Count   Available Count
----- ----- -----
ipv4_nexthop            60          64380
```

```
sonic# show crm resources ipv4 route
Resource Name          Used Count   Available Count
----- ----- -----
ipv4_route              27452       63266
```

```
sonic# show crm resources nexthop group member
Resource Name          Used Count   Available Count
----- ----- -----
nexthop_group_member    340         15703
```

```
sonic# show crm resources nexthop group object
Resource Name          Used Count   Available Count
----- ----- -----
nexthop_group            127         0
```

```
sonic# show crm resources acl group
```

Stage Count	Bind Point	Resource Name	Used Count	Available
INGRESS	PORT	acl_group	0	256
INGRESS	PORT	acl_table	0	3
INGRESS	LAG	acl_group	0	256
INGRESS	LAG	acl_table	0	3
INGRESS	VLAN	acl_group	0	256
INGRESS	VLAN	acl_table	0	9
INGRESS	RIF	acl_group	0	256
INGRESS	RIF	acl_table	0	9
INGRESS	SWITCH	acl_group	0	256
INGRESS	SWITCH	acl_table	0	9
EGRESS	PORT	acl_group	0	256
EGRESS	PORT	acl_table	0	2
EGRESS	LAG	acl_group	0	256
EGRESS	LAG	acl_table	0	2
EGRESS	VLAN	acl_group	0	256
EGRESS	VLAN	acl_table	0	2
EGRESS	RIF	acl_group	0	256
EGRESS	RIF	acl_table	0	2
EGRESS	SWITCH	acl_group	0	256
EGRESS	SWITCH	acl_table	0	2

```
sonic# show crm resources acl table
```

Table ID	Resource Name	Used Count	Available Count
0x700000000007f9	acl_counter	2	57850
0x700000000007f9	acl_entry	2	2302

```
sonic# show crm resources all
```

Resource Name	Used Count	Available Count
ipv4_route	1	32751
ipv6_route	2	10238
ipv4_nexthop	0	65534
ipv6_nexthop	0	65534
ipv4_neighbor	0	24576

ipv6_neighbor	0	12288
nexthop_group_member	0	32768
nexthop_group	0	256
fdb_entry	0	65535
ipmc_entry	0	24576
snat_entry	0	1024
dnat_entry	0	1024
Stage Count	Bind Point	Resource Name
INGRESS	PORT	acl_group
INGRESS	PORT	acl_table
INGRESS	LAG	acl_group
INGRESS	LAG	acl_table
INGRESS	VLAN	acl_group
INGRESS	VLAN	acl_table
INGRESS	RIF	acl_group
INGRESS	RIF	acl_table
INGRESS	SWITCH	acl_group
INGRESS	SWITCH	acl_table
EGRESS	PORT	acl_group
EGRESS	PORT	acl_table
EGRESS	LAG	acl_group
EGRESS	LAG	acl_table
EGRESS	VLAN	acl_group
EGRESS	VLAN	acl_table
EGRESS	RIF	acl_group
EGRESS	RIF	acl_table
EGRESS	SWITCH	acl_group
EGRESS	SWITCH	acl_table
Table ID	Resource Name	Used Count
...		Available Count

Releases

4.2.1 or later

show crm thresholds

Displays information about the high and low thresholds used for critical resource monitoring.

Command	show crm thresholds {acl {group table} all dnat fdb ipmc ipv4 {neighbor nexthop route} ipv6 {neighbor nexthop route} nexthop group {member object} snat}
Options	Enter a CRM resource. Valid values are: <ul style="list-style-type: none"> • acl group — ACL counter resources and group entries. • acl table — ACL table resources • all — Use the all value to view information about all CRM resources. • dnat — Destination Network Address Translation (NAT) entries • fdb — MAC forwarding database (FDB) entries • ipmc — IP multicast entries • ipv4 neighbor — IPv4 neighbor entries • ipv4 nexthop — IPv4 next-hop entries • ipv4 route — IPv4 route entries • ipv6 neighbor — IPv6 neighbor entries • ipv6 nexthop — IPv6 next-hop entries • ipv6 route — IPv6 route entries • nexthop group member — Next-hop group member resources • nexthop group object — Next-hop group object resources • snat — Source Network Address Translation entries
Modes	EXEC

Usage

To set the high and low thresholds for CRM resources, use the `crm threshold` command. To configure the format in which CRM thresholds are monitored (that is, percentage or the number of used or available entries), use the `crm threshold type` command.

Examples

Resource Name	Threshold Type	Low Threshold	High Threshold
acl_group	percentage	70	90
acl_counter	percentage	70	90
acl_entry	percentage	70	90
acl_table	percentage	70	90
dnat_entry	percentage	70	90
fdb_entry	free	53000	60000
ipmc_entry	used	7000	8000
ipv4_neighbor	used	12000	16000
ipv4_nexthop	used	12000	16000
ipv4_route	free	60000	75000
ipv6_neighbor	used	6000	8000
ipv6_nexthop	used	6000	8000
ipv6_route	free	20000	28000
nexthop_group	percentage	70	90
nexthop_group_member	percentage	70	90
snat_entry	percentage	70	90

Releases

4.2.1 or later

show crypto ca-cert file

Displays the PEM (Base64 ASCII) format of an installed CA certificate.

Command

`show crypto ca-cert file certificate-name`

Options

`certificate-name` — Enter the name of a CA certificate.

Modes

EXEC

Usage

To display the raw ASCII format of host certificates, use the [show crypto cert file](#) command. To verify the validity of an installed CA certificate, use the [crypto ca-cert verify expiry](#) command.

Example

```
sonic# show crypto ca-cert CA
Certificate Name: CA
-----BEGIN CERTIFICATE-----
MIIDfzCCAmegAwIBAgIUZPKPRgloczRG1FOULPwfEgZs7owwDQYJKoZIhvvcNAQEL
BQAjELMAkGA1UEBhMCVVMxGzAJBgNVBAgMAMNBMRmWEQYDVQQHApTYWNyYW11
bnRvMQ0wCwYDVQQKDAREZWxsMRMwEQYDVQQLDApOZXRs3bJraW5nMRUwEwYDVQD
DAx3d3cuZGVsbC5jb20wHhcNMjIwNzA3MjAyNDM0WhcNmzIwNzA0MjAyNDM0WjBq
MQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExEzARBgNVBAcMC1NhY3JhbWVudG8x
DTALBgNVBAoMBER1bGwxEzARBgNVBAsMCk51dHdvcmtpbmcxFTATBjNvBAMMDh3
dy5kZWxsLmNvbTCCASIwDQYJKoZIhvvcNAQEBQADggEPADCCAQoCggEBAOonTx6f
A5c/d/FIailGhu/Z0ezh0JMoIPY2R2YhAJLZ02WNPLyArI8i7s0gXuxHE+GohSAB
czCUjGoKc5M8CuX2sQr1rcEL4oQ8pltfbhx2qtGiAPoQmNSdo8dPhrB1NxVdbiP
rwMZldOEYun5G2yd/6f2jjIvMn9dBxM4/TNeF1JgBio1sVtVC0HGhbghX0xiyu
9Y+hiao3eeoadd0R3+6Kh+1OPDpUltQTdaCvV5Sw1ROAPd5Um+jWax6h0v2T0jt3
fLfY6X3QXaHciQ6mxILm/BVmAt9FjKsLB89Jt1PuKoRarCkJfO5a/5QZ4ns/EXv3
3Vsq2pmYWbgHI+kCAwEAAaMdMBswDAYDVR0TBAnAwEB/zALBjNVHQ8EBAMCAuQw
DQYJKoZIhvvcNAQELBQADggEBAGOa47S3ENf6ks0Ee/Rqw158EcblmnuthYjfPrWAD
q4kP4vfblH/dbiHpIWAKjYHsfjWEtpdeZQfE4kR8jox+iJQpbTLn3GxwXTtzDrY
gxGEJquH8s4FjynSD2LeotmGy9R/HGD4OONBmxNtJLTrDayLX5bUClwmqiDTwPgG
JIQ90BvgM51JXjz5d2iU1/IRvj1BKkRdnqa2pwIU9Ajv8fhxpcKs1Dldtmh9AFrl
knRc91JeLWpPpgymG8H/quYfPF6hFvpyVRuE0qglscjyNZfgAiwInONpDi4NnPgy
JSgG3FdZnbtIlwJjFoCAur5dExCniyhELap97D5noBS12Wo=
-----END CERTIFICATE-----
```

Releases

4.1.0 or later

show crypto cert

Displays information about host certificates.

Command	<code>show crypto cert {certificate-name all}</code>
Options	<ul style="list-style-type: none">• <i>certificate-name</i> — Display information about a specified host certificate.• <i>all</i> — Display information about all certificates.
Modes	EXEC
Usage	Use this command to display installed host certificates. Use the show ca-crypto cert command to display information about CA certificates.
Example	

```
sonic# show crypto cert server.crt
Certificate Name: server.crt
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = US, ST = CA, L = Sacramento, O = Dell, OU =
Networking, CN = www.dell.com
    Validity
      Not Before: Aug 13 08:00:00 2015 GMT
      Not After : Aug 13 09:00:00 2025 GMT
    Subject: C = US, ST = CA, O = Dell, OU = Networking, CN = server
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
        Modulus:
          00:c1:cd:48:73:ad:62:5d:fb:70:f0:7d:eb:20:97:
          e5:5a:5c:a7:89:ef:0e:12:c4:36:52:1c:fa:d1:a1:
          91:1d:f3:95:2a:f8:c6:ed:41:da:bf:e8:a2:d2:14:
          f8:6d:7f:3d:c0:ae:58:08:91:75:82:8e:3e:3e:6f:
          4c:04:e2:86:75:45:a0:e8:37:5f:b2:92:81:b0:23:
          34:eb:15:c4:d6:69:f1:c6:93:9e:a7:32:b9:52:f8:
          c1:53:35:57:ec:70:fb:85:dd:24:8c:47:6b:2d:34:
          9c:03:60:ad:a6:de:f3:88:1b:17:16:97:b0:e0:09:
          17:67:ed:4d:c3:a6:41:70:e9:86:be:f1:2c:b5:14:
          0a:c3:45:58:96:7f:73:43:30:35:3a:7a:42:8c:53:
          df:bb:de:fe:58:50:2b:83:df:71:65:41:ff:ae:30:
          e7:ce:f6:99:15:5f:ad:d5:e8:86:e0:18:80:a0:d0:
          e9:01:45:7b:4e:51:7d:38:bb:e3:25:9c:5c:9c:b7:
          20:ea:ff:4e:aa:65:e2:51:4a:c3:4b:82:b8:4f:85:
--more--
          e4:af:e1:b6:5c:7f:7e:90:a9:29:1a:b9:e0:5b:d6:
          b1:cd:2f:7a:89:38:ad:6f:97:66:de:cf:89:b1:c8:
          46:05:5d:47:7d:33:a2:c9:77:22:a4:65:82:9a:2d:
          c5:ed
        Exponent: 65537 (0x10001)
  X509v3 extensions:
    Authority Information Access:
--more--
    OCSP - URI:http://127.0.0.1:8181
    X509v3 Subject Alternative Name:
      DNS:server
    Signature Algorithm: sha256WithRSAEncryption
      66:84:b0:d5:18:32:2b:7b:22:c4:8f:e4:b1:c1:c8:bd:ce:ca:
      33:5b:4b:4a:79:ea:d3:9c:8b:20:d9:46:2f:7e:6f:91:1c:89:
      a2:2e:14:bc:25:71:1a:05:a6:1a:7d:f9:3a:ef:93:55:29:bc:
      4a:87:f3:96:96:93:27:c3:7a:43:9c:f8:a2:1a:c4:0a:e5:95:
      a7:00:b8:04:1c:70:25:c5:3c:9c:ed:da:8e:fd:d3:b1:8e:76:
      97:84:df:59:c3:8e:11:22:10:23:97:71:ff:14:31:1c:b8:a0:
--more--
      ed:1f:e1:31:c7:c1:de:89:f6:3e:0b:d5:95:84:ee:4b:64:ed:
      ab:0a:f7:36:44:12:52:d1:36:10:96:7b:ef:4c:44:b6:46:b2:
--more--
      41:20:0b:f5:70:b9:68:f1:34:5a:78:71:73:77:d2:8b:f9:5d:
      2f:ea:dd:14:b0:71:0f:9d:73:e0:72:06:b7:a2:0c:60:87:83:
```

```
--more--
91:8a:4a:2d:cc:7a:3b:40:22:b9:3d:7a:d8:26:03:7e:2b:a3:
8a:59:34:07:30:90:9c:17:55:11:ce:f7:b4:6b:44:2d:f2:bb:
9a:e4:7c:fe:09:fb:db:22:d1:1f:b2:e7:7a:e4:e1:98:a4:d2:
ef:27:a3:37:30:94:5c:09:c2:71:5e:bf:5b:ac:a9:af:ee:ae:
--more--
ac:63:83:d3
```

Releases

4.1.0 or later

show crypto cert file

Displays the PEM (Base64 ASCII) format of a host certificate.

Command show crypto cert file *certificate-name*

Options *certificate-name* — Enter the name of a host certificate.

Modes EXEC

Usage To display the raw ASCII format of CA certificates, use the [show ca-crypto cert](#) command.

Example

```
sonic# show crypto cert server.crt
Certificate Name: server.crt
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIBAjANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExEzARBgNVBACMC1NhY3JhbWVudG8xDTALBgNVBAoMBERlbGwx
EzARBgNVBAsMCK5ldHdvcmtpbmcxFTATBgNVBAMMDHd3dy5kZWxsLmNvbTAeFw0x
NTA4MTMwODAwMDBaFw0yNTA4MTMwOTAwMDBaME8xCzAJBgNVBAYTA1VTMswCQYD
VQQIDAJDQTENMASGA1UECgwERGVsbDETMBEA1UECwwKTmV0d29ya2luZZEPMA0G
A1UEAwGc2VydmyMIIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMIIBCgKCAQEAc1I
c61ixftw8H3rIJflWlynies80EsQ2Uhz60aGRHfOVKvjG7UHav+ii0hT4bX89wK5Y
CJF1go4+Pm9MBOKGdUWg6DdfspKBsCM06xxE1mnxxpOepzK5UvjBUzVX7HD7hd0k
jEdrLTScA2Cpt7ziBsXFpew4AkXZ+1Nw6ZBcOmGvvEstRQKw0VYln9zQzA1OnpC
jFPfu97+WFArg99xZUH/rjDnzvaZFv+tlei4G4BiAoNDpAUv7T1F9OLvjJZxcnLcg
6v9OqmXiUUrDS4K4T4Xkr+G2XH9+kKkpGrngW9axzS96iTib5dm3s+JschGBV1H
fTOiyXcipGWCmi3F7QIDAQABo0gwRjAxBggxBgEFBQcbAQqlMCMwiQYIKwyBBQUH
MAGGFWh0dHA6Ly8xMjcuMC4wLjE6ODE4MTARBgNVHREcjaIggZzZXJ2ZXiwDQYJ
KoZIhvcNAQELBQADggEBAGaEsNUYMit7IsSP5LHByL3OyjNbS0p56tOciyDZRi9+
b5EciaIuFLwlRoFphp9+Trvk1UpvEqH85aWkyfDekOc+KIaxArllacAuAQccCXF
PJzt2o7907G0dpeE31nDjhEiECOxcf8UMRy4oO0f4THwd6J9j4L1ZWE7ktk7asK
9zzEE1LRNhCWe+9MRLZGskEgC/VwuWjxNFp4cXN30ov5XS/q3RSwcQ+dc+ByBrei
DGCHg5GKSi3MejtAIrk9etgmA34ro4pZNAcwkJwXVRHO97RrRC3yu5rkfP4J+9si
0R+y53rk4Zik0u8nozcw1FwJwnFevlusqa/urqxjg9M=
-----END CERTIFICATE-----
```

Releases

4.1.0 or later

show crypto security-profile

Displays information about security profiles.

Command show crypto security-profile {*profile-name* | all}

Options

- *profile-name* — Enter the name of a security profile.
- all — Display all security profiles.

Modes EXEC

Usage To configure a security profile, use the [crypto security-profile](#) command.

Example

```
sonic# show crypto security-profile myserver
-----
Security Profile : myserver
```

```
-----  
Key Usage Check : False  
Peer Name Check: False  
Revocation Check: False  
Certificate Name: server  
Trust Store: myts  
CDP Identifiers: None  
OCSP Responders: None
```

Releases 4.1.0 or later

show crypto ssh-key

Displays the SSH key that is generated for SSH client connections .

Command show crypto ssh-key {ecdsa | rsa}

Options

- **ecdsa** — View the generated ECDSA key.
- **rsa** — View the generated RSA key.

Mode EXEC

Usage SSH key generation supports various cryptographic algorithms, such as RSA and ECDSA, and key-length customization based on security requirements. To generate SSH host keys, use the [crypto ssh-keygen](#) command.

Examples

```
sonic# show crypto ssh-key ecdsa  
ecdsa-sha2-nistp256  
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBEKwpGyEQN9JEnpzdws5Ug9GGC5YEX  
root@sonic  
  
sonic# show crypto ssh-key rsa  
ssh-rsa  
AAAAB3NzaC1yc2EAAAQABAAQCy1P611KgeiDKfBdFLYhxavW3ZiCL9RRGJKsL42k/grhctSyjTlC  
root@sonic
```

Releases 4.4.1 or later

show crypto trust-store

Displays information about the trust stores on the switch.

Command show crypto trust-store *trust-store-name*

Options *trust-store-name* — Enter the name of a trust store.

Modes EXEC

Usage To configure a trust store, use the [crypto trust-store](#) command.

Example

```
sonic# show crypto trust-store  
-----  
Trust Store : myts  
-----  
CA Certificates Name: CA
```

Releases 4.1.0 or later

show current

Displays the MST activated configuration.

Command show current

Options None

Modes SPANNING TREE

Usage Use this command to view the activated MST instance to VLAN mapping.

Examples

```
sonic-clt(config-mst) # show current
Current MST Configuration
Name test
Revision 10 Instances configured 4
Instance Vlans mapped
-----
0      1-9,11-19,21-4093
1      10
2      20
4094   4094
-----
```

Releases 4.0 or later

show database map

Displays a summary of databases currently in use.

Command show database map

Options None

Modes EXEC

- Usage**
- ID — Numeric database identifier
 - Name — Database name string used to refer to the database in the sonic-db-cli command and database connector APIs
 - Instance — Redis instance that the database is part of
 - TCP Port — TCP port used to connect to the Redis instance
 - Unix Socket Path — Socket path to connect to the Redis instance

Example

```
sonic# show database map
-----
 ID      Name     Instance   TCP Port  Unix Socket Path
-----
 0      APPL_DB  redis2    26379   /var/run/redis/redis2.sock
 1      ASIC_DB  redis3    36379   /var/run/redis/redis3.sock
 2      COUNTERS_DB  redis    6379    /var/run/redis/redis.sock
 3      LOGLEVEL_DB  redis    6379    /var/run/redis/redis.sock
 4      CONFIG_DB  redis    6379    /var/run/redis/redis.sock
 5      PFC_WD_DB  redis    6379    /var/run/redis/redis.sock
 6      STATE_DB  redis    6379    /var/run/redis/redis.sock
 7      SNMP_OVERLAY_DB  redis    6379    /var/run/redis/redis.sock
 8      ERROR_DB  redis    6379    /var/run/redis/redis.sock
```

Releases 3.1 or later

show device

Displays device level watermark commands.

Command

```
show device { persistent-watermark | watermark }
```

Options

- *persistent-watermark*—Display persistent-watermark counters
- *watermark*—Display user watermark counters

Modes

EXEC

Usage

Use this command to view the buffer watermark counters.

Examples

```
sonic# show device watermark
Utilization (Bytes)    : 23187712
Utilization (Percent) : 69
```

Releases

4.0 or later

show dot1x

Displays a summary of the global dot1x configuration.

Command

```
show dot1x
```

Options

None

Modes

EXEC

Usage

Use this command to display a summary of the global dot1x configuration.

Examples

```
sonic# show dot1x
Administrative Mode..... Enabled
```

Table 7. Global dot1x configuration

Field	Description
Administrative Mode	Indicates whether 802.1x is enabled or disabled.

Releases

4.0 or later

show dot1x detail

Displays the details of the configuration for the specified port.

Command

```
show dot1x detail {all | Ethernet port}
```

Options

- *all*—All ports
- *port*—Physical interface ID

Modes

EXEC

Usage

Use this command to view the details of dot1x configuration on an interface or all interfaces.

Examples

```
sonic# show dot1x detail all
Interface ..... Ethernet0
PAE Capabilities ..... none
Server Timeout(secs) ..... 30
Quiet Period(secs) ..... 30
```

Interface	Ethernet1
PAE Capabilities	none
Server Timeout(secs)	30
Quite Period(secs)	30

Table 8. dot1x Configuration

Field	Description
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are <code>Authenticator</code> or <code>None</code> .
Server Timeout	Server timeout value in seconds.
Quite Period	Quite period value in seconds.

Releases

4.0 or later

show dropcounters capabilities

Displays drop counters capabilities.

Command show dropcounters capabilities

Options None

Modes EXEC

Usage Use this command to display drop counters capabilities available on the switch.

Examples

```
sonic# show dropcounters capabilities
Counter Type          Total
-----
PORT_INGRESS_DROPS      10
SWITCH_EGRESS_DROPS     2
PORT_MIRROR_SUPPORTED_INGRESS_DROPS  5

PORT_INGRESS_DROPS:
    L2_ANY
    SMAC_MULTICAST
    SMAC_EQUALS_DMPC
    INGRESS_VLAN_FILTER
    EXCEEDS_L2_MTU
    SIP_CLASS_E
    SIP_LINK_LOCAL
    DIP_LINK_LOCAL
    UNRESOLVED_NEXT_HOP
    DECAP_ERROR

SWITCH_EGRESS_DROPS:
    L2_ANY
    L3_ANY
    A_CUSTOM_REASON

PORT_MIRROR_SUPPORTED_INGRESS_DROPS:
    L2_ANY
    SMAC_MULTICAST
    SMAC_EQUALS_DMPC
    INGRESS_VLAN_FILTER
    EXCEEDS_L2_MTU
```

Releases

4.0 or later

show dropcounters configuration

Displays drop counters configuration.

Command show dropcounters configuration

Options None

Modes EXEC

Usage Use this command to view the drop counters configured on the switch.

Examples

```
sonic# show dropcounters configuration
Counter      Alias      Group      Type          Mirror      Reasons
-----      -----      -----      -----      -----
DEBUG_0      RX_LEGIT   LEGIT      PORT_INGRESS_DROPS  Session1  SMAC_EQUALS_DM
DEBUG_1      TX_LEGIT   None       SWITCH_EGRESS_DROPS NA
EGRESS_VLAN_FILTER
```

Releases 4.0 or later

show dropcounters configuration detail

Displays detailed drop counters configuration.

Command show dropcounters configuration detail

Options None

Modes EXEC

Usage Use this command to view the detailed information about the drop counters configured on the switch.

Examples

```
sonic# show dropcounters configuration detail
-----
Counter      :          DEBUG_0
Description  :          Debug_0
Alias        :          RX_LEGIT
Group        :          LEGIT
Type         :          PORT_INGRESS_DROPS
Mirror       :          Session1
Reasons     :          SMAC_EQUALS_DM
Status       :          Enabled
-----
Counter      :          DEBUG_1
Description  :          Debug_1
Alias        :          DEBUG_1
Group        :          TX_LEGIT
Type         :          None
Mirror       :          SWITCH_EGRESS_DROPS
Reasons     :          EGRESS_VLAN_FILTER
Status       :          Enabled
```

Releases 4.0 or later

show errdisable link-flap

Displays the Error Disable Recovery information in case of excessive link flaps.

Command show errdisable link-flap

Options None

Modes EXEC

Usage	Use this command to check the status of Error Disable Recovery for excessive link flaps.					
Examples	<pre>sonic# show errdisable link-flap Interface Flap-threshold Sampling-interval Recovery-interval Time-left Status ----- Ethernet0 3 10 300 N/A On Ethernet4 4 40 200 143 Err-disabled Ethernet12 6 25 0 N/A On Ethernet20 4 30 240 N/A Off</pre>					
Releases	4.0 or later					

show errdisable recovery

Displays error disable recovery information.

Command	show errdisable recovery
Options	None
Modes	EXEC
Usage	Use this command to check the status of error disable recovery for all supported features.
Example	<pre>sonic# show errdisable recovery Errdisable Cause Status ----- ----- udld disabled bpduguard disabled link-flap enabled Timeout for Auto-recovery: 300 seconds</pre>

Releases	3.1 or later
-----------------	--------------

show error-database

Displays the error database entries.

Command	show error-database {ALL ERROR_ROUTE_TABLE ERROR_NEIGH_TABLE ERROR_IPMC_ROUTE_TABLE}
Options	<ul style="list-style-type: none"> • ALL—Displays all tables • ERROR_IPMC_ROUTE_TABLE—Displays IPMC route table • ERROR_NEIGH_TABLE—Displays neighbor table • ERROR_ROUTE_TABLE—Displays route table
Modes	EXEC
Usage	This output shows the errors and failures seen while programming the routes in different tables.
Examples	<pre>sonic# show error-database ERROR_ROUTE_TABLE ROUTE TABLE : Number of routes failed : 4 VRF Name Prefix Nexthop Interface Error Code Operation Default 700::/64 remove SWSS_RC_NOT_FOUND Default 600::/64 remove SWSS_RC_NOT_FOUND Default 13.13.13.0/24 remove SWSS_RC_NOT_FOUND</pre>

```
Default 12.12.12.0/24 SWSS_RC_NOT_FOUND
remove
```

```
sonic# show error-database ERROR_NEIGH_TABLE
NEIGHBOR TABLE :
Number of neighbor entries failed : 2

IP address MAC address Interface Error Code Operation
2001::4 Ethernet120 SWSS_RC_NOT_FOUND remove
10.1.1.4 Ethernet120 SWSS_RC_NOT_FOUND remove
```

Releases 4.1.0 or later

show event

Displays Event messages for system operation and alarms.

Command sonic# show event [details | summary | severity level | start timestamp end timestamp | recent {5min|60min|24hr} | id event-id | from event-id to event-id]

Options

- **details**—Displays detailed event information.
- **summary**—Displays summary information of logged events, including a summary of severity levels.
- **severity level**—Displays information for events with the specified severity level: critical, major, minor, warning, or informational. The default is warning.
- **start timestamp end timestamp**—Displays the events that are logged between the specified times. Enter the *timestamp* in the format *yyyy-mm-hhTmm:ss:msZ*, where *yyyy* is a 4-digit year, *mm* is a 2-digit month, *hh* is a 2-digit hour, and *Tmm:ss:msZ* is the hour-second-millisecond in the timestamp.
- **recent {5min|60min|24hr}**—Displays the most recent events logged in the last 5 minutes, 60 minutes, or 24 hours.
- **id event-id**—Displays information for the specified event ID number in `show event` output.
- **from event-id to event-id**—Displays information for the events in the range of the specified event IDs in `show event` output.

Modes EXEC

Usage

Use the `show event` command to view the subset of Syslog messages that are tagged with the keyword EVENT or ALARM for system operation and alarm events. Events for system operation are logged only once. Events for alarms are raised for fault conditions that can be corrected and cleared. You can also use the `| grep` option to filter `show event` output.

Example

```
sonic# show event
-----
Id Action Severity Name Source Timestamp Description
-----
1 - INFORMATIONAL SYSTEM_REBOOT system_reboot 2024-03-09T00:13:12.402Z User issued 'Unknown
(First boot of...
2 RAISE WARNING PSU_POWER_STATUS PSU 2 2024-03-09T00:13:16.800Z PSU 2 is out of power.
3 - INFORMATIONAL SYSTEM_STATUS system_status 2024-03-09T00:13:26.948Z System is ready
4 - INFORMATIONAL INTERFACE_OPER_STATUS Loopback10 2024-03-09T00:13:42.729Z Interface Loopback10
oper state...
5 - INFORMATIONAL SYSTEM_STATUS system_status 2024-03-09T00:41:36.675Z System is not ready -
one or more...
6 - INFORMATIONAL SYSTEM_STATUS system_status 2024-03-09T00:43:12.168Z System is ready
7 - INFORMATIONAL INTERFACE_OPER_STATUS Loopback4 2024-03-09T02:34:08.250Z Interface Loopback4
oper state...
8 - INFORMATIONAL INTERFACE_OPER_STATUS Loopback4 2024-03-09T02:36:45.177Z Interface Loopback4
oper state...
9 - INFORMATIONAL INTERFACE_OPER_STATUS Loopback4 2024-03-09T02:36:46.812Z Interface Loopback4
oper state...
```

```
sonic# show event details
-----
Event Details - 1
-----
Id: 1
Action: RAISE
Severity: WARNING
Type: PSU_REMOVED
Timestamp: 2023-10-20T09:17:54.479Z
Description: PSU 2
```

```

Source:          PSU 2
-----
Event Details - 2
-----
Id:            2
Action:        RAISE
Severity:     WARNING
Type:          PSU_REMOVED
Timestamp:    2023-10-20T09:17:54.488Z
Description:   PSU 3
Source:        PSU 3

-----
Event Details - 3
-----
Id:            3
Action:        RAISE
Severity:     WARNING
Type:          FAN_REMOVED
Timestamp:    2023-10-20T09:17:56.985Z
Description:   PSU 2 FAN 1
Source:        PSU 2 FAN 1

-----
Event Details - 4
-----
Id:            4
Action:        -
Severity:     INFORMATIONAL
Type:          SYSTEM_STATUS
Timestamp:    2023-10-20T09:19:59.868Z
Description:   System is ready
Source:        system_status

-----
Event Details - 5
-----
Id:            5
Action:        -
Severity:     INFORMATIONAL
Type:          SYSTEM_STATUS
Timestamp:    2023-10-20T09:19:59.925Z
Description:   System is not ready - one or more services are not up
Source:        system_status

-----
Event Details - 6
-----
Id:            6
Action:        -
Severity:     INFORMATIONAL
Type:          SYSTEM_STATUS
Timestamp:    2023-10-20T09:23:02.802Z
Description:   System is ready
Source:        system_status

-----
Event Details - 7
-----
Id:            7
Action:        ACKNOWLEDGE
Severity:     WARNING
Type:          PSU_REMOVED
Timestamp:    2023-10-20T09:53:47.425Z
Description:   Alarm id 1 ACKNOWLEDGE.
Source:        1

```

```

sonic# show event summary
Event summary
-----
Total:          6
Raised:         3
Acknowledged:   0
Cleared:        0
-----
```

```
sonic# show event severity warning
```

Event Log Examples																																																																							
sonic# show event recent 24hr																																																																							
<table border="1"> <thead> <tr> <th colspan="6">Event Log Examples</th> </tr><tr> <th colspan="6">sonic# show event recent 24hr</th> </tr><tr> <th colspan="6">sonic# show event from 2 to 5</th> </tr> </thead> <tbody> <tr> <td>Id</td><td>Action</td><td>Severity</td><td>Name</td><td>Source</td><td>Timestamp</td></tr> <tr> <td>1</td><td>RAISE</td><td>WARNING</td><td>PSU_REMOVED</td><td>PSU 2</td><td>2023-10-20T09:17:54.479Z</td></tr> <tr> <td>2</td><td>RAISE</td><td>WARNING</td><td>PSU_REMOVED</td><td>PSU 3</td><td>2023-10-20T09:17:54.488Z</td></tr> <tr> <td>3</td><td>RAISE</td><td>WARNING</td><td>FAN_REMOVED</td><td>PSU 2 FAN 1</td><td>2023-10-20T09:17:56.985Z</td></tr> <tr> <td>7</td><td>ACKNOWLEDGE</td><td>WARNING</td><td>PSU_REMOVED</td><td>1</td><td>2023-10-20T09:53:47.425Z</td></tr> <tr> <td colspan="6">Alarm id 1 ACKNOWLEDGE.</td></tr> </tbody> </table>						Event Log Examples						sonic# show event recent 24hr						sonic# show event from 2 to 5						Id	Action	Severity	Name	Source	Timestamp	1	RAISE	WARNING	PSU_REMOVED	PSU 2	2023-10-20T09:17:54.479Z	2	RAISE	WARNING	PSU_REMOVED	PSU 3	2023-10-20T09:17:54.488Z	3	RAISE	WARNING	FAN_REMOVED	PSU 2 FAN 1	2023-10-20T09:17:56.985Z	7	ACKNOWLEDGE	WARNING	PSU_REMOVED	1	2023-10-20T09:53:47.425Z	Alarm id 1 ACKNOWLEDGE.																	
Event Log Examples																																																																							
sonic# show event recent 24hr																																																																							
sonic# show event from 2 to 5																																																																							
Id	Action	Severity	Name	Source	Timestamp																																																																		
1	RAISE	WARNING	PSU_REMOVED	PSU 2	2023-10-20T09:17:54.479Z																																																																		
2	RAISE	WARNING	PSU_REMOVED	PSU 3	2023-10-20T09:17:54.488Z																																																																		
3	RAISE	WARNING	FAN_REMOVED	PSU 2 FAN 1	2023-10-20T09:17:56.985Z																																																																		
7	ACKNOWLEDGE	WARNING	PSU_REMOVED	1	2023-10-20T09:53:47.425Z																																																																		
Alarm id 1 ACKNOWLEDGE.																																																																							
<table border="1"> <thead> <tr> <th colspan="6">Event Log Examples</th> </tr><tr> <th colspan="6">sonic# show event from 2 to 5</th> </tr><tr> <th colspan="6">sonic# show event start 2023-10-20T09:17:55.000Z end 2023-10-20T09:19:59.900Z</th> </tr> </thead> <tbody> <tr> <td>Id</td><td>Action</td><td>Severity</td><td>Name</td><td>Source</td><td>Timestamp</td></tr> <tr> <td>2</td><td>RAISE</td><td>WARNING</td><td>PSU_REMOVED</td><td>PSU 3</td><td>2023-10-20T09:17:54.488Z</td></tr> <tr> <td>3</td><td>RAISE</td><td>WARNING</td><td>FAN_REMOVED</td><td>PSU 2 FAN 1</td><td>2023-10-20T09:17:56.985Z</td></tr> <tr> <td>4</td><td>-</td><td>INFORMATIONAL</td><td>SYSTEM_STATUS</td><td>system_status</td><td>2023-10-20T09:19:59.868Z</td></tr> <tr> <td>5</td><td>-</td><td>INFORMATIONAL</td><td>SYSTEM_STATUS</td><td>system_status</td><td>2023-10-20T09:19:59.925Z</td></tr> <tr> <td colspan="6">System is ready - one or more services are not up</td></tr> <tr> <td colspan="6">6 - INFORMATIONAL SYSTEM_STATUS system_status 2023-10-20T09:23:02.802Z System is ready</td></tr> <tr> <td colspan="6">7 ACKNOWLEDGE WARNING PSU_REMOVED 1 2023-10-20T09:53:47.425Z Alarm id 1 ACKNOWLEDGE.</td></tr> </tbody> </table>						Event Log Examples						sonic# show event from 2 to 5						sonic# show event start 2023-10-20T09:17:55.000Z end 2023-10-20T09:19:59.900Z						Id	Action	Severity	Name	Source	Timestamp	2	RAISE	WARNING	PSU_REMOVED	PSU 3	2023-10-20T09:17:54.488Z	3	RAISE	WARNING	FAN_REMOVED	PSU 2 FAN 1	2023-10-20T09:17:56.985Z	4	-	INFORMATIONAL	SYSTEM_STATUS	system_status	2023-10-20T09:19:59.868Z	5	-	INFORMATIONAL	SYSTEM_STATUS	system_status	2023-10-20T09:19:59.925Z	System is ready - one or more services are not up						6 - INFORMATIONAL SYSTEM_STATUS system_status 2023-10-20T09:23:02.802Z System is ready						7 ACKNOWLEDGE WARNING PSU_REMOVED 1 2023-10-20T09:53:47.425Z Alarm id 1 ACKNOWLEDGE.					
Event Log Examples																																																																							
sonic# show event from 2 to 5																																																																							
sonic# show event start 2023-10-20T09:17:55.000Z end 2023-10-20T09:19:59.900Z																																																																							
Id	Action	Severity	Name	Source	Timestamp																																																																		
2	RAISE	WARNING	PSU_REMOVED	PSU 3	2023-10-20T09:17:54.488Z																																																																		
3	RAISE	WARNING	FAN_REMOVED	PSU 2 FAN 1	2023-10-20T09:17:56.985Z																																																																		
4	-	INFORMATIONAL	SYSTEM_STATUS	system_status	2023-10-20T09:19:59.868Z																																																																		
5	-	INFORMATIONAL	SYSTEM_STATUS	system_status	2023-10-20T09:19:59.925Z																																																																		
System is ready - one or more services are not up																																																																							
6 - INFORMATIONAL SYSTEM_STATUS system_status 2023-10-20T09:23:02.802Z System is ready																																																																							
7 ACKNOWLEDGE WARNING PSU_REMOVED 1 2023-10-20T09:53:47.425Z Alarm id 1 ACKNOWLEDGE.																																																																							
<table border="1"> <thead> <tr> <th colspan="6">Event Log Examples</th> </tr><tr> <th colspan="6">sonic# show event start 2023-10-20T09:17:55.000Z end 2023-10-20T09:19:59.900Z</th> </tr> </thead> <tbody> <tr> <td>Id</td><td>Action</td><td>Severity</td><td>Name</td><td>Source</td><td>Timestamp</td></tr> <tr> <td>3</td><td>RAISE</td><td>WARNING</td><td>FAN_REMOVED</td><td>PSU 2 FAN 1</td><td>2023-10-20T09:17:56.985Z</td></tr> <tr> <td>4</td><td>-</td><td>INFORMATIONAL</td><td>SYSTEM_STATUS</td><td>system_status</td><td>2023-10-20T09:19:59.868Z</td></tr> <tr> <td colspan="6">System is ready</td></tr> </tbody> </table>						Event Log Examples						sonic# show event start 2023-10-20T09:17:55.000Z end 2023-10-20T09:19:59.900Z						Id	Action	Severity	Name	Source	Timestamp	3	RAISE	WARNING	FAN_REMOVED	PSU 2 FAN 1	2023-10-20T09:17:56.985Z	4	-	INFORMATIONAL	SYSTEM_STATUS	system_status	2023-10-20T09:19:59.868Z	System is ready																																			
Event Log Examples																																																																							
sonic# show event start 2023-10-20T09:17:55.000Z end 2023-10-20T09:19:59.900Z																																																																							
Id	Action	Severity	Name	Source	Timestamp																																																																		
3	RAISE	WARNING	FAN_REMOVED	PSU 2 FAN 1	2023-10-20T09:17:56.985Z																																																																		
4	-	INFORMATIONAL	SYSTEM_STATUS	system_status	2023-10-20T09:19:59.868Z																																																																		
System is ready																																																																							

Releases

4.2.0 or later

show evpn

Displays information about EVPN configuration, including EVPN multihoming.

Command

show evpn

Options

None

Command mode

EXEC

Usage

Use this command to check the EVPN configuration including EVPN multihoming.

Example

```
sonic# show evpn
L2 VNIs: 6
L3 VNIs: 1
Advertise gateway mac-ip: No
Advertise svi mac-ip: No
Advertise svi mac: No
Duplicate address detection: Enable
    Detection max-moves 5, time 180
EVPN MH:
    mac-holdtime: 1080s, neigh-holdtime: 1080s
    uplink-cfg-cnt: 0, uplink-active-cnt: 0
IPv4 Neigh Kernel threshold: 48000
IPv6 Neigh Kernel threshold: 48000
Total IPv4 neighbors: 2
Total IPv6 neighbors: 3
```

Releases

3.1 or later

show evpn arp-cache vni

Displays the EVPN ARP cache.

Command show evpn arp-cache vni *vni number* {[[ip *ipvalue*] | [duplicate] | {[vtep *vtepvalue*] }] }

Options

- *vni number*—VNI number
- *ipvalue*—(Optional) IP address in A.B.C.D or A::B format
- *vtepvalue*—(Optional) VTEP in A.B.C.D format

Command mode EXEC

Usage Use this command to view the EVPN ARP cache.

Example

```
sonic# show evpn arp-cache vni 1001
Number of ARPs (local and remote) known for this VNI: 109
          IP           Type   State    MAC           Remote VTEP      Seq #'s
101.101.0.108  remote  active  a0:01:01:00:12:01  172.16.28.10  0/0
101.101.0.111  remote  active  a0:01:01:00:15:01  172.16.31.10  0/0
101.1.1.202    remote  active  a0:30:01:00:02:01  172.16.52.10  0/0
101.101.0.107  remote  active  a0:01:01:00:11:01  172.16.27.10  0/0
fe80::200:ff:fe00:103 remote  active  00:00:00:00:01:03  45.45.45.45  0/0
101.101.0.98   remote  active  a0:01:01:00:08:01  172.16.18.10  0/0
101:1:1:1:71   local   inactive 00:31:01:00:00:01
101.1.1.213    remote  active  a0:30:01:00:0d:01  172.16.63.10  0/0
101.1.1.44     local   active  00:28:01:00:00:04
101.101.0.101  remote  active  a0:01:01:00:0b:01  172.16.21.10  0/0
101.1.1.23     local   active  00:2e:01:00:00:03
fe80::200:ff:fe00:102 local   active  00:00:00:00:01:02
101.1.1.21     local   active  00:2e:01:00:00:01
101.1.1.13     local   active  00:2c:01:00:00:03
101.101.0.112  remote  active  a0:01:01:00:16:01  172.16.32.10  0/0
101.101.0.91   remote  active  a0:01:01:00:01:01  172.16.11.10  0/0
101:1:1:1:131  remote  active  00:3e:01:00:00:01  45.45.45.45  0/0
101.1.1.204    remote  active  a0:30:01:00:04:01  172.16.54.10  0/0
101.101.0.113  remote  active  a0:01:01:00:17:01  172.16.33.10  0/0
101.1.1.223    remote  active  a0:30:01:00:17:01  172.16.73.10  0/0
101.101.0.93   remote  active  a0:01:01:00:03:01  172.16.13.10  0/0
101.1.1.12     local   active  00:2c:01:00:00:02
--more--
```

Releases 3.1 or later

show evpn arp-cache vni all

Displays information about all VNIs.

Command show evpn arp-cache vni all {[detail] | [duplicate]}]

Options

- *detail*—Displays detailed information about neighbor entries in EVPN.
- *duplicate*—Displays the duplicate neighbor entries detected in EVPN.

Command mode EXEC

Usage Use this command to display the EVPN ARP cache for all VNIs.

Example

```
sonic# show evpn arp-cache vni all
VNI 1305 #ARP (IPv4 and IPv6, local and remote) 43
          IP           Type   State    MAC           Remote VTEP      Seq #'s
102.50.1.43   local   inactive 00:28:01:00:04:c3
102.50.1.22   local   active  00:2e:01:00:04:c2
fe80::23b:1ff:fe00:131 local   active  00:3b:01:00:01:31
fe80::200:ff:fe00:102 local   active  00:00:00:00:01:02
101:131:1:1:71 remote  active  00:31:01:00:01:31  3.3.3.3
101:131:1:1:51 local   active  00:3c:01:00:01:31
102.50.1.11   local   active  00:2c:01:00:04:c1
fe80::23a:1ff:fe00:131 local   active  00:3a:01:00:01:31
102.50.1.24   local   active  00:2e:01:00:04:c4
102.50.1.63   local   inactive 00:2f:01:00:04:c3
102.50.1.32   local   active  00:37:01:00:04:c2
fe80::23c:1ff:fe00:131 local   active  00:3c:01:00:01:31
102.50.1.83   remote  active  00:32:01:00:04:c3  3.3.3.3
102.50.1.73   remote  active  00:3d:01:00:04:c3  3.3.3.3
102.50.1.52   local   inactive 00:2d:01:00:04:c2
```

```

102.50.1.71      remote active   00:3d:01:00:04:c1 3.3.3.3      0/0
102.50.1.12     local  active   00:2c:01:00:04:c2          0/0
102.50.1.81      remote active   00:32:01:00:04:c1 3.3.3.3      0/0
101:131:1:1::31  local  active   00:3b:01:00:01:31          0/0
102.50.1.42      local  active   00:28:01:00:04:c2          0/0
102.50.1.41      local  active   00:28:01:00:04:c1          0/0
102.50.1.33      local  inactive 00:37:01:00:04:c3          0/0
--more--

```

Releases 3.1 or later

show evpn es

Displays information about the EVPN Ethernet segment configured on multihomed VTEPs.

Command show evpn es {XX:XX:XX:XX:XX:XX:XX:XX:XX:XX | detail | startup-delay}

Options

- XX:XX:XX:XX:XX:XX:XX:XX:XX:XX—Enter an ES-ID; for example, 00:00:00:00:00:00:00:a:00:01.
- detail—Displays information for all EVPN Ethernet segments configured on a multihomed VTEP.

Command mode EXEC

Usage Use this command to view the information about the EVPN Ethernet segment configured on multihomed VTEPs.

Example

```

sonic# show evpn es detail
ESI: 03:00:00:00:11:22:33:00:00:01
Type: Local,Remote
Interface: PortChannel1
State: up
Bridge port: yes
Ready for BGP: yes
VNI Count: 2
MAC Count: 1
DF status: df
DF preference: 32767
Nexthop group: 536870913
VTEPs:
    4.4.4.4 df_alg: preference df_pref: 32767 nh: 268435458

ESI: 03:00:00:00:11:22:33:00:00:02
Type: Local,Remote
Interface: PortChannel2
State: up
Bridge port: yes
Ready for BGP: yes
VNI Count: 2
MAC Count: 1
DF status: df
DF preference: 32767
Nexthop group: 536870914
VTEPs:
    2.2.2.2 df_alg: preference df_pref: 32767 nh: 268435459
    3.3.3.3 df_alg: preference df_pref: 32767 nh: 268435460
    4.4.4.4 df_alg: preference df_pref: 32767 nh: 268435461

```

```

sonic# show evpn es 03:00:00:00:11:22:33:00:00:02
ESI: 03:00:00:00:11:22:33:00:00:02
Type: Local,Remote
Interface: PortChannel2
State: up
Bridge port: yes
Ready for BGP: yes
VNI Count: 2
MAC Count: 1
DF status: df
DF preference: 32767
Nexthop group: 536870914

```

```
VTEPs:
  2.2.2.2 df_alg: preference df_pref: 32767 nh: 268435459
  3.3.3.3 df_alg: preference df_pref: 32767 nh: 268435460
  4.4.4.4 df_alg: preference df_pref: 32767 nh: 268435461
```

```
sonic# show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                                         Type ES-IF
00:00:00:11:22:33:00:00:00:01   R   -
00:00:00:55:00:66:00:00:00:01   LN  PortChannel155
01:54:bf:64:bd:d7:42:00:35:00  LRN PortChannel153
3.3.3.3,4.4.4.4,6.6.6.6
03:00:00:00:44:44:44:00:00:36   LR  PortChannel154
                                         VTEPs
                                         3.3.3.3,4.4.4.4
                                         6.6.6.6
```

Releases 4.2.0 or later

show evpn es startup-delay

Displays the startup delay configured on a multihomed VTEP.

Command show evpn es startup-delay

Options None

Command mode EXEC

Usage During VTEP bootup, the EVPN multihoming interfaces are kept in an administrative-down state until the startup-delay timer expires. As a result, traffic from a multihomed tenant device is not load-balanced to the VTEP until the VTEP starts up and is ready. Traffic loss is avoided.

Example

```
sonic# show evpn es startup-delay
Startup Delay      : 600 secs
Time left         : 0 secs
```

Releases 4.2.0 or later

show evpn es-evi

Displays information about the EVPN Ethernet segment configured on multihomed VTEPs.

Command show evpn es-evi {vni | detail}

Options

- **vni**—Enter a VXLAN network identifier (VNI) for a tenant segment (1-16777215).
- **detail**—Displays information for all EVPN Ethernet segments and the associated VXLAN IDs configured on a multihomed VTEP.

Command mode EXEC

Usage Use this command to display information about EVPN Ethernet segments and EVI configured on multihomed VTEPs.

Example

```
sonic# show evpn es-evi detail
VNI 200 ESI: 03:00:00:00:11:22:33:00:00:01
  Type: L
  Ready for BGP: yes

VNI 100 ESI: 03:00:00:00:11:22:33:00:00:01
  Type: L
  Ready for BGP: yes

VNI 200 ESI: 03:00:00:00:11:22:33:00:00:02
  Type: L
  Ready for BGP: yes
```

```
VNI 100 ESI: 03:00:00:00:11:22:33:00:00:02
Type: L
Ready for BGP: yes
```

```
sonic# show evpn es-evi 100

VNI 100 ESI: 03:00:00:00:11:22:33:00:00:01
Type: L
Ready for BGP: yes

VNI 100 ESI: 03:00:00:00:11:22:33:00:00:02
Type: L
Ready for BGP: yes
```

```
sonic# show evpn es-evi
Type: L local, R remote
VNI          ESI                                         Type
101007      00:00:00:55:00:66:00:00:00:01      L
101007      01:54:bf:64:bd:d7:42:00:35:00      L
101007      03:00:00:00:44:44:44:00:00:36      L
101362      00:00:00:55:00:66:00:00:00:01      L
101362      01:54:bf:64:bd:d7:42:00:35:00      L
101362      03:00:00:00:44:44:44:00:00:36      L
101107      00:00:00:55:00:66:00:00:00:01      L
```

Releases

4.2.0 or later

show evpn l2-nh

Displays information about a Layer 2 next-hop neighbor for a multihomed VTEP.

Command

show evpn l2-nh

Options

None

Command mode

EXEC

Usage

In the show output, information about a multihomed peer VTEP's source IP address, Ethernet segment number, and next-hop ID are displayed.

Example

```
sonic# show evpn l2-nh
VTEP      NH id      #ES
1.1.1.1    268435462    1
2.2.2.2    268435461    1
3.3.3.3    268435463    3
```

Releases

4.2.0 or later

show evpn mac vni

Displays the VXLAN network identifier.

Commandshow evpn mac vni *vnid* {{ [mac *macvalue*] } | [duplicate] | {[vtep *vtepvalue*] } }**Options**

- *vnid*—VNI number
- *macvalue*—(Optional) MAC address in nn:nn:nn:nn:nn:nn format
- *vtepvalue*—(Optional) VTEP in A.B.C.D format
- *duplicate*—Displays the duplicate MAC entries detected in EVPN

Command mode

EXEC

Usage

Use this command to view the information about MAC addresses in EVPN for a specified VNI.

Example

```
sonic# show evpn mac vni 1001
Number of MACs (local and remote) known for this VNI: 100
MAC          Type   Intf/Remote VTEP      VLAN Seq #'s
a0:01:01:00:16:01 remote 172.16.32.10      0/0
a0:01:01:00:13:01 remote 172.16.29.10      0/0
00:28:01:00:00:04 local   PortChannel200    1001  0/0
a0:01:01:00:12:01 remote 172.16.28.10      0/0
00:3d:01:00:00:04 remote 3.3.3.3           1/0
a0:30:01:00:15:01 remote 172.16.71.10      0/0
00:2f:01:00:00:01 local   Ethernet21        1001  0/0
00:35:01:00:00:02 remote 45.45.45.45       0/0
a0:30:01:00:10:01 remote 172.16.66.10       0/0
a0:01:01:00:17:01 remote 172.16.33.10       0/0
00:32:01:00:00:01 remote 3.3.3.3           0/0
a0:01:01:00:02:01 remote 172.16.12.10       0/0
a0:30:01:00:0f:01 remote 172.16.65.10       0/0
a0:01:01:00:06:01 remote 172.16.16.10       0/0
00:28:01:00:00:02 local   PortChannel200    1001  0/0
a0:01:01:00:0d:01 remote 172.16.23.10       0/0
a0:01:01:00:07:01 remote 172.16.17.10       0/0
00:3d:01:00:00:01 remote 3.3.3.3           1/0
00:47:01:00:00:01 local   PortChannel200    1001  0/0
a0:30:01:00:01:01 remote 172.16.51.10       0/0
a0:01:01:00:0a:01 remote 172.16.20.10       0/0
00:37:01:00:00:03 local   PortChannel200    1001  0/0
--more--
```

Releases

3.1 or later

show evpn mac vni all

Displays information about all VNIs.

Command `show evpn mac vni all {[detail] | [duplicate] | {[vtep vtepvale]}}}`

Options

- `vtepvale`—VTEP in A.B.C.D format
- `detail`—Displays detailed information about mac neighbor entries in EVPN.
- `duplicate`—Displays the duplicate MAC entries detected in EVPN.

Command mode EXEC

Usage

Use this command to view the information about MAC addresses in EVPN for all VNI.

Example

```
sonic# show evpn mac vni all
VNI 1305 #MACs (local and remote) 37
MAC          Type   Intf/Remote VTEP      VLAN Seq #'s
00:2d:01:00:04:c1 local   PortChannel100    1305  0/0
00:32:01:00:04:c2 remote 3.3.3.3           0/0
00:2f:01:00:04:c4 local   PortChannel100    1305  0/0
00:2d:01:00:04:c4 local   PortChannel100    1305  0/0
00:32:01:00:04:c4 remote 3.3.3.3           0/0
00:32:01:00:04:c3 remote 3.3.3.3           0/0
00:37:01:00:04:c4 local   PortChannel200    1305  0/0
00:3d:01:00:04:c2 remote 3.3.3.3           0/0
00:2d:01:00:04:c2 local   PortChannel100    1305  0/0
00:28:01:00:04:c2 local   PortChannel200    1305  0/0
00:28:01:00:04:c4 local   PortChannel200    1305  0/0
00:37:01:00:04:c2 local   PortChannel200    1305  0/0
00:2d:01:00:04:c3 local   PortChannel100    1305  0/0
00:2f:01:00:04:c2 local   PortChannel100    1305  0/0
00:2e:01:00:04:c4 local   Ethernet21        1305  0/0
00:00:00:00:01:02 local   Vlan1305          1305  0/0
00:2e:01:00:04:c1 local   Ethernet21        1305  0/0
00:37:01:00:04:c1 local   PortChannel200    1305  0/0
00:3c:01:00:01:31 local   PortChannel100    1305  0/0
```

```
00:2c:01:00:04:c4 local Ethernet20          1305 0/0
00:2c:01:00:04:c2 local Ethernet20          1305 0/0
00:2c:01:00:04:c3 local Ethernet20          1305 0/0
--more--
```

Releases 3.1 or later

show evpn next-hops vni

Displays the remote VTEP next-hop information for the specified L3 VNI.

Command show evpn next-hops vni *vni number* {[ip *ip value*]}

Options • *vni number*—VNI number

• *ip value*—IP address in A.B.C.D or A::B format

Command mode EXEC

Usage Use this command to view the remote VTEP next-hop information for the specified L3 VNI.

Example

```
sonic# show evpn next-hops vni 102000
Number of NH Neighbors known for this VNI: 4
IP           RMAC
::ffff:3.3.3.3 8c:04:ba:bb:ba:40
3.3.3.3      8c:04:ba:bb:ba:40
45.45.45.45   3c:2c:30:24:95:80
::ffff:45.45.45.45 3c:2c:30:24:95:80
```

Releases 3.1 or later

show evpn next-hops vni all

Displays information about all VNIs.

Command show evpn next-hops vni all

Options None

Command mode EXEC

Usage Use this command to view the remote VTEP next-hop information for all L3 VNIs.

Example

```
sonic# show evpn next-hops vni all
VNI 102000 #Next-Hops 4
IP           RMAC
::ffff:3.3.3.3 8c:04:ba:bb:ba:40
3.3.3.3      8c:04:ba:bb:ba:40
45.45.45.45   3c:2c:30:24:95:80
::ffff:45.45.45.45 3c:2c:30:24:95:80
```

Releases 3.1 or later

show evpn rmac vni

Displays router MAC of a remote VTEP for a specified L3 VNI.

Command show evpn rmac vni *vni number* {[mac *mac value*]}

Options

• *vni number*—VNI number

• *mac value*—(Optional) MAC address in nn:nn:nn:nn:nn:nn format

Command mode EXEC

Usage Use this command to display the router MAC of a remote VTEP for a specified L3 VNI.

Example

```
sonic# show evpn rmac vni 102000
Number of Remote RMACs known for this VNI: 2
MAC           Remote VTEP
3c:2c:30:24:95:80 45.45.45.45
8c:04:ba:bb:ba:40 3.3.3.3
```

Releases 3.1 or later

show evpn rmac vni all

Displays information about all VNIs.

Command show evpn rmac vni all

Options None

Command mode EXEC

Usage Use this command to display the router MAC of a remote VTEP for all L3 VNIs.

Example

```
sonic# show evpn rmac vni all
VNI 102000 #RMACs 2
RMAC           Remote VTEP
3c:2c:30:24:95:80 45.45.45.45
8c:04:ba:bb:ba:40 3.3.3.3
```

Releases 3.1 or later

show evpn vni

Displays detailed information for a specified VNI.

Command show evpn vni *vni number*

Options *vni number*—VNI number

Command mode EXEC

Usage Use this command to view the detailed information for a specified VNI.

Example

```
sonic# show evpn vni 1103010
VNI: 1103010
    Type: L3
    Tenant VRF: Vrf010
    Local Vtep Ip: 5.5.5.5
    Local External Vtep Ip: 0.0.0.0
    Vxlan-Intf: vtep-leaf-3010
    SVI-If: Vlan3010
    State: Up
    Client State: Up
    VNI Filter: none
    System MAC: 18:5a:58:b1:83:25
    Router MAC: 18:5a:58:b1:83:25
    L2 VNIs: 100145 100146 100147 100148 100149 100150 100151 100152
              100153
              100154 100155 100156 100157 100158 100159 100160
```

Releases 3.1 or later

show evpn vni detail

Displays detailed information about each VNI.

Command show evpn vni detail

Options None

Command mode EXEC

Usage Use this command to view detailed information for all VNIs.

Example

```
sonic# show evpn vni detail
VNI: 1305
  Type: L2
  Tenant VRF: Vrf-102
  Client State: Up
  VxLAN interface: vtep-leaf-1305
  VxLAN ifIndex: 994
  Local VTEP IP: 12.12.12.12
  Mcast group: 0.0.0.0
  Remote VTEPs for this VNI:
    3.3.3.3 flood: HER
    Kernel Add: Success, Add ReAttempt:0
  Number of MACs (local and remote) known for this VNI: 39
  Number of ARPs (IPv4 and IPv6, local and remote) known for this VNI: 44
  Advertise-gw-macip: No
VNI: 1252
  Type: L2
  Tenant VRF: Vrf-84
  Client State: Up
  VxLAN interface: vtep-leaf-1252
  VxLAN ifIndex: 940
  Local VTEP IP: 12.12.12.12
  Mcast group: 0.0.0.0
  Remote VTEPs for this VNI:
    3.3.3.3 flood: HER
--more--
```

Releases 3.1 or later

show fips status

Displays FIPS mode status and other FIPS information.

Command show fips status

Options None

Modes EXEC

Usage To enable FIPS mode, use the [crypto fips enable](#) command.

Examples

```
sonic# show fips status
FIPS Mode          : Enabled
Crypto Library     : OpenSSL 1.1.1n-fips 15 Mar 2022
FIPS Object Module: DELL OpenSSL FIPS Crypto Module v2.6 July 2021
```

Releases 4.2.1 or later

show hardware tcam allocation

Displays the TCAM allocation.

Command show hardware tcam allocation {forwarding-fbs | ip-acl | ipv6-acl | mac-acl | monitoring-fbs | qos-fbs} {[ingress | egress] }

- Options**
- **forwarding-fbs**—Forwarding FBS feature
 - **ip-acl**—IP ACL feature
 - **ipv6-acl**—IPv6 ACL feature
 - **mac-acl**—MAC ACL feature
 - **monitoring-fbs**—Monitoring FBS feature
 - **qos-fbs**—QoS FBS feature
 - **ingress**—Ingress direction
 - **egress**—Egress direction

Modes EXEC

Usage Use this command to view the configured key-profiles for different flow-based services.

Examples

```
sonic# show hardware tcam allocation
Ingress:
-----
Feature          Configured      Key-Profile      Current
-----           -----
forwarding-fbs   ip             ip
ip-acl          pac            pac
monitoring-fbs  ip             ip
-----
Egress:
-----
Feature          Configured      Key-Profile      Current
-----           -----
ip-acl          pac            pac
-----
* Indicates configured and current/enforced key-profile are different.
  Please save the config and reboot to enforce the configured key-profile,
  if current
```

Releases 4.0 or later

show hardware tcam key-profile

Displays the qualifiers supported by each key profile in detail.

Command show hardware tcam key-profile { fbs | ip-acl | ipv6-acl | mac-acl | profile-name }

- Options**
- **fbs**—FBS feature
 - **ip-acl**—IP ACL feature
 - **ipv6-acl**—IPv6 ACL feature
 - **mac-acl**—MAC ACL feature
 - **profile-name**—Name of the key profile (up to 63)

Modes EXEC

Usage Use this command to display the qualifiers supported by each key profile in detail.

Examples

```
sonic# show hardware tcam key-profile ip-acl default
-----
Qualifiers          Ingress    Egress
-----           -----
ICMP Type          Yes       Yes
```

ICMP Code	Yes	Yes
L4 source port	Yes	Yes
L4 destination port	Yes	Yes
L4 source port range	Yes	No
L4 destination port range	Yes	No
IP Protocol	Yes	Yes
DSCP	Yes	Yes
Source IPv4 address	Yes	Yes
Destination IPv4 address	Yes	Yes
TCP Flags	Yes	Yes

Releases 4.0 or later

show histogram memory system

Displays histogram system memory details.

Command `show histogram memory {system [stime stime] [etime etime] [filter filter-name] [analyze analyze] }`

- Options**
- *stime*—Enter the start time in ISO format
 - *etime*—Enter the end time in ISO format
 - *filtername*—Enter the filter name (up to 63 characters)
 - *analyze*—Enter to analyze leak

Modes EXEC

Usage

This command displays the collected memory statistics of the system. As the data is collected, the difference in memory is calculated for each process, docker, and system and stored alongside the memory statistics. These differences are displayed using the analyze option and the leak keyword. If the difference column value for a process, docker, or system is high in the specified time slots, there is a possibility of a memory leak. When no settings are specified, a 30-day record is displayed for all processes, dockers, and systems.

Examples

```
sonic# show histogram memory system

Start Time : 2022-01-01 12:08:55
End Time : 2022-01-13 12:08:55
Current Time : 2022-01-13 12:08:55
-----
          Days     Days     Days     Days     Days   Current    High/Low     System
List      [01-04]  [04-07]  [07-10]  [10-13]  [13-13]
          Jan/1    Jan/4    Jan/7    Jan/10   Jan/13
-----
          -        -        -        -       15.1G  15.1G    15.1G/15.1G  total
          -        -        -        -       2.3G   2.4G    2.3G/2.3G   used
          -        -        -        -      11.2G  11.1G   11.2G/11.2G  free
          -        -        -        -     191.2M 198.9M  191.2M/191.2M buffers
          -        -        -        -      1.4G   1.4G    1.4G/1.4G   cached
          -        -        -        -      12.5G  12.4G   12.5G/12.5G available
```

Releases 4.0 or later

show hosts

Displays IP name server configuration.

Command `show hosts`

Options None

Mode

EXEC

Usage

Use this command to view the DNS configuration on the switch.

Example

```
sonic# show hosts
Source Interface: Loopback0
Name servers are: 1.2.3.4(vrf: mgmt), 2001:4860:4860::8888(vrf: mgmt), 8.8.8.8
Configuration mode: STATIC
```

Releases

3.1 or later

show image firmware

Displays a pending firmware upgrade and the result of an earlier firmware upgrade.

Command

show image firmware

Options

None

Command mode

EXEC

Usage

Use this command after a successful staging of a firmware package and before reboot.

Example

After a successful staging of a firmware package and before a reboot:

```
sonic# show image firmware
Pending Firmware Upgrade(s)
=====
Name
Version      Date
-----
onie-update-full-x86_64-dell EMC_z9400_c3758-r0.3.51.5.1-15.tar
3.51.5.1-15   2023-09-25 05:16:39

Past Firmware Upgrade(s)
=====
Name
Version      Result    Date
-----
-----
```

After you reboot the switch, and ONIE performs the firmware upgrade:

```
sonic# show image firmware
Pending Firmware Upgrade(s)
=====
Name
Version      Date
-----
onie-update-full-x86_64-dell EMC_z9400_c3758-r0.3.51.5.1-15.tar
3.51.5.1-15   Success  2023-09-25 06:02:15
```

Releases

4.2.0 or later

show image firmware status

Displays the firmware staging status.

Command	show image firmware status
Options	None
Modes	EXEC
Usage	The <code>show image firmware status</code> command displays information about the operational status of a firmware upgrade, including the following statuses: <ul style="list-style-type: none">• <code>GLOBAL_STATE_DOWNLOAD</code> during the firmware package downloading process• <code>GLOBAL_STATE_STAGE_PROGRESS</code> during the firmware package staging process• <code>GLOBAL_STATE_SUCCESS</code> after a successful staging of the firmware package• <code>GLOBAL_STATE_FAILED</code> if you incorrectly specified the image file or entered the wrong server IP address; for example:
Examples	<pre>sonic# show image firmware status %Info: System reboot is required to initiate the firmware upgrade operation. %Info: Reboot will take longer than normal and the upgrade process should not be interrupted. %Info: Device may auto-reboot during the upgrade process based on the components being upgraded. %Info: After successful upgrade, the device will boot into SONiC. ----- Global operation status : GLOBAL_STATE_SUCCESS ----- File operation status : TRANSFER_STATE_SUCCESS File size(bytes) : 79237120 File transfer bytes : 79237120 File download speed : 77380 KB/s File progress : 100% Transfer start time : 2023-09-25 05:16:38+0000 Transfer end time : 2023-09-25 05:16:39+0000 ----- Stage operation status : STAGE_STATE_SUCCESS Stage start time : 2023-09-25 05:16:39+0000 Stage end time : 2023-09-25 05:16:39+0000 -----</pre>
Releases	4.2.0 or later

show image list

Displays image list information.

Command	show image list
Options	None
Modes	EXEC
Usage	Use this command to view current, next, and available software image information.
Example	<pre>sonic# show image list Current: SONiC-OS-4.4.0-Cloud_Premium_Build102 Next: SONiC-OS-4.4.0-Cloud_Premium_Build106 Available: SONiC-OS-4.4.0-Cloud_Premium_Build102 SONiC-OS-4.4.0-Cloud_Premium_Build106</pre>
Releases	3.2 or later

show image patch history

Displays the patches that have been applied and removed (rolled back) for the current running image.

Command show image patch history

Options None

Modes EXEC

Usage Use this command to view the patches that have been applied and removed (rolled back) for the current running image.

Example

```
sonic# show image patch history
-----
Id Tag State Status Start End
-----
01 22.11.22-0001-patch-framework-verification-patch apply complete 2019.02.25-06:44:44 2019.02.25-06:47:01
01 22.11.22-0001-patch-framework-verification-patch rollback complete 2019.02.25-06:36:17 2019.02.25-06:37:50
01 22.11.22-0001-patch-framework-verification-patch apply complete 2019.02.25-06:29:44 2019.02.25-06:31:56
```

Releases 4.1.0 or later

show image patch list

Displays the list of patches that are already applied or installed on the switch.

Command show image patch list

Options None

Modes EXEC

Usage To install a patch, use the image patch install command. Use this command to view the list of patches that are already applied or installed on the switch.

Example

```
sonic# show image patch list
-----
Id Tag Date
-----
01 22.11.22-0001-patch-framework-verification-patch 2019.02.25-06:46:57
```

Releases 4.1.0 or later

show image patch status

Displays the progress of a patch installation or removal.

Command show image patch status

Options None

Modes EXEC

Usage To view the progress of a patch installation or removal, use the show image patch status command. During patch installation, if a patch fails to install properly, any part that was applied is removed and the image is restored to its previous state. To install a patch, use the image patch install command.

Example

```
sonic# show image patch status
-----
Global operation status : GLOBAL_STATE_SUCCESS
-----
File operation status   : TRANSFER_STATE_SUCCESS
File size(bytes)       : 2665197550
```

```

File transfer bytes      : 2665197550
File progress           : 100%
Transfer start time    : 2022-11-22 06:19:42+0000
Transfer end time       : 2022-11-22 06:20:07+0000
-----
Install operation status : INSTALL_STATE_SUCCESS
Install start time      : 2022-11-22 06:21:06+0000
Install end time         : 2022-11-22 06:24:00+0000

```

Releases 4.1.0 or later

show image status

Displays image installation status.

Command show image status

Options None

Modes EXEC

Usage The command output displays Global operation status. The following global operation statuses may be displayed:

- GLOBAL_STATE_DOWNLOAD during the image downloading process.
- GLOBAL_STATE_INSTALL during the image installation process.
- GLOBAL_STATE_SUCCESS after a successful image installation.
- GLOBAL_STATE_FAILED if the image installation process fails. For example, if you incorrectly specified the image file or entered the wrong server IP address.
- GLOBAL_STATE_IDLE when there is no image installation activity.

Examples

```

sonic# show image status
-----
Global operation status : GLOBAL_STATE_IDLE
-----
```

```

sonic# show image status
-----
Global operation status : GLOBAL_STATE_INSTALL
-----
File operation status   : TRANSFER_STATE_SUCCESS
File size(bytes)        : 1111533595
File transfer bytes     : 1111533595
File download speed     : 120609 KB/s
File progress           : 100%
Transfer start time    : 2024-07-09 20:20:41+0000
Transfer end time       : 2024-07-09 20:20:50+0000
-----
Install operation status : INSTALL_PROGRESS
Install start time      : 2024-07-09 20:20:54+0000
Install end time         : N/A
```

```

sonic# show image status
-----
Global operation status : GLOBAL_STATE_SUCCESS
-----
File operation status   : TRANSFER_STATE_SUCCESS
File size(bytes)        : 1111533595
File transfer bytes     : 1111533595
File download speed     : 120609 KB/s
File progress           : 100%
Transfer start time    : 2024-07-09 20:20:41+0000
Transfer end time       : 2024-07-09 20:20:50+0000
-----
Install operation status : INSTALL_STATE_SUCCESS
```

```
Install start time      : 2024-07-09 20:20:54+0000
Install end time       : 2024-07-09 20:21:24+0000
```

Releases 4.0 or later

show in-memory-logging

Displays in-memory logging information.

Command show in-memory-logging

Options None

Modes EXEC

Usage Debug logs from applications are logged into a RAM based in-memory logging store which is periodically saved to persistent storage. Use this command to display the in-memory logs.

Examples

```
sonic# show in-memory-logging
May 02 10:42:42.992558+00:00 2024 leaf1 DEBUG system#monitor:
    Main process- received event:rsyslog.service from source:sysbus
time:2024-05-02 10:42:42
May 02 10:42:43.009942+00:00 2024 leaf1 DEBUG system#monitor:
    Get unit status for rsyslog.service
May 02 10:42:43.065702+00:00 2024 leaf1 DEBUG system#monitor:
    Main process- received event:caclmgrd.service from source:sysbus
time:2024-05-02 10:42:43
May 02 10:42:43.092583+00:00 2024 leaf1 DEBUG system#monitor:
    Get unit status for caclmgrd.service
May 02 10:42:44.450128+00:00 2024 leaf1 DEBUG mgmt-
framework#rest_server[31]:
    [platform_config.go:510] Default DPB mode for Ethernet56 is 1x100G
May 02 10:42:44.450192+00:00 2024 leaf1 DEBUG mgmt-
framework#rest_server[31]:
    [platform_config.go:530] [1/51/Ethernet56] BW 100000 for 1x100G
May 02 10:42:44.450226+00:00 2024 leaf1 DEBUG mgmt-
framework#rest_server[31]:
    [platform_config.go:592] Lane count 4 total_bandwidth 100000
    port_count 1 lane_speed 25000
```

Releases 3.2 or later

show in-memory-logging count

Displays the total number of messages in in-memory logging.

Command show in-memory-logging count

Options None

Modes EXEC

Usage None

Examples

```
sonic# show in-memory-logging count
57039
```

Releases 3.2 or later

show in-memory-logging lines

Displays the in-memory logging output for the last specified number of lines.

Command	show in-memory-logging lines [lines]
Options	lines—Enter the number of lines (1 to 65535)
Modes	EXEC
Usage	If you do not specify the number of lines, the command displays all in-memory logging output.
Examples	<pre>sonic# show in-memory-logging lines 10 May 03 06:59:08.446433+00:00 2024 leaf1 DEBUG mgmt- framework#rest_server[31]: [common_app.go:360] translateAction:path =/openconfig-infra- logging:show-sys-in-memory-log [123 34 111 112 101 110 99 111 110 102 105 103 45 105 110 102 114 97 45 108 111 103 103 105 110 103 58 105 110 112 117 116 34 58 32 123 34 110 117 109 45 108 105 110 101 115 34 58 32 49 48 125 125] May 03 06:59:08.446433+00:00 2024 leaf1 DEBUG mgmt- framework#rest_server[31]: [common_app.go:591] Before calling transformer.CallRpcMethod() for path /openconfig-infra-logging:show-sys-in-memory-log May 03 06:59:08.446433+00:00 2024 leaf1 DEBUG mgmt- framework#rest_server[31]: [cs_getdb.go:32] GetConfigDB: { DBNo: CONFIG_DB, InitIndicator: , TableNameSeparator: , KeySeparator: , IsWriteDisabled: false, IsCacheEnabled: false, IsEnableOnChange: false, SDB: <nil>, DisableCVLCheck: false, IsSession: false, ConfigDBLazyLock: true, TxCmdsLim: 0 }</pre>
Releases	3.2 or later

show interface

Displays all configured interface information.

Command	show interface {{counters {[rate] [phy-if-name] [po-name]}}} {Eth [iface_num] {Ethernet [iface_num]} iface_range_num {PortChannel [po-id]} {Management [mgmt-if-id]} vlan_range_num {Loopback lo-id} status {transceiver [phy-if-name] [summary] {[diagnostics {capability status}] transceiver dom [Ethslot/port] [rif] }}}}
Options	<ul style="list-style-type: none">• <i>phy-if-name</i> — (Optional) Physical interface name• <i>po-name</i> — (Optional) PortChannel name• <i>po-id</i> — (Optional) PortChannel ID (1 to 128)• <i>iface_num</i> — (Optional) Ethernet ID (1 to 65535)• <i>iface_range_num</i> — (Optional) Ethernet range numbers• <i>mgmt-if-id</i> — (Optional) Management interface ID (0)• <i>vlan-id</i> — (Optional) VLAN ID (1 to 4094)• <i>vlan_range_num</i> — (Optional) VLAN range numbers• <i>lo-id</i> — (Optional) Loopback interface ID (0 to 16383)• <i>transceiver dom</i> — (Optional) Monitor real-time Ethernet port transceiver operations with digital optical monitoring (DOM).• <i>rif</i> — (Optional) Packet counts and rates in TX and RX direction.
Modes	EXEC
Usage	Use this command to view interface configuration information about counters, interfaces, and status. Use the do show interface command to view interface information from other command modes.

Examples

```
sonic# show interface Ethernet

Ethernet0 is up, line protocol is up
Hardware is Eth
IPV4 address is 192.168.1.1/31
Mode of IPV4 address assignment: MANUAL
IPV6 address is 2001:1::1/64,fe80::1e72:1dff:fec3:c2e0/64
Mode of IPV6 address assignment: MANUAL
IP MTU 9100 bytes
LineSpeed 100GB, Auto-negotiation off
FEC: DISABLED
Last clearing of "show interface" counters: never
10 seconds input rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
10 seconds output rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
Input statistics:
    11 packets, 2994 octets
    11 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded, 0 Oversize
    0 Packets (128 to 255 Octects)
Output statistics:
    17 packets, 4086 octets
    17 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded, 0 Oversize
Ethernet4 is up, line protocol is down
Hardware is Eth
IPV4 address is 192.168.2.1/24
Mode of IPV4 address assignment: MANUAL
IPV6 address is 2001:2::1/64,fe80::1e72:1dff:fec3:c2e0/64
Mode of IPV6 address assignment: MANUAL
IP MTU 9100 bytes
LineSpeed 100GB, Auto-negotiation off
FEC: DISABLED
Last clearing of "show interface" counters: never
10 seconds input rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
10 seconds output rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
Input statistics:
    0 packets, 0 octets
    0 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded, 0 Oversize
    0 Packets (128 to 255 Octects)
Output statistics:
    0 packets, 0 octets
    0 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded, 0 Oversize
Ethernet8 is up, line protocol is down
Hardware is Eth
IPV4 address is 192.168.3.1/24
Mode of IPV4 address assignment: MANUAL
IPV6 address is 2001:3::1/64,fe80::1e72:1dff:fec3:c2e0/64
Mode of IPV6 address assignment: MANUAL
IP MTU 9100 bytes
LineSpeed 100GB, Auto-negotiation off
FEC: DISABLED
Last clearing of "show interface" counters: never
10 seconds input rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
10 seconds output rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
Input statistics:
    0 packets, 0 octets
    0 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded, 0 Oversize
    0 Packets (128 to 255 Octects)
Output statistics:
    0 packets, 0 octets
    0 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded, 0 Oversize
```

```
sonic# show interface counters
-----
Interface State RX_OK     RX_ERR RX_DRP RX_OVERSIZE TX_OK      TX_ERR TX_DRP TX_OVERSIZE
-----
Ethernet28 U    201809144 0      0      0          201809148 0      0      0
```

```

Ethernet32 U      201803931 0      0      0      0      201803929 0      0      0      0
Ethernet36 D      0      0      0      0      0      0      0      0      0      0

```

```

sonic# show interface PortChannel 100
PortChannel100 is down, line protocol is down, mode LACP
Minimum number of links to bring PortChannel up is 1
Fallback: Enabled
MTU 9100
LACP mode ACTIVE interval SLOW priority 65535 address 90:b1:1c:f4:9c:9f
Members in this channel: Ethernet84(Selected), Ethernet80
LACP Actor port 85 address 90:b1:1c:f4:9c:9f key 100
LACP Partner port 0 address 00:00:00:00:00:00 key 0
Last clearing of "show interface" counters: 1970-01-01 00:00:00
Input statistics:
    2972 packets, 712962 octets
2972 Multicasts, 0 Broadcasts, 0 Unicasts
0 error, 2972 discarded
Output statistics:
    2969 packets, 712560 octets
2969 Multicasts, 0 Broadcasts, 0 Unicasts
0 error, 0 discarded

```

```

sonic# show interface Management 0
Management0 is up, line protocol is up
Hardware is Mgmt
IPV4 address is 44.2.3.4/24
Mode of IPV4 address assignment: MANUAL
IPV6 address is a::e/64
Mode of IPV6 address assignment: MANUAL
IP MTU 1500 bytes
LineSpeed 1000MB, Auto-negotiation on
Input statistics:
    0 packets, 0 octets
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 error, 0 discarded
Output statistics:
    0 packets, 0 octets
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 error, 0 discarded

```

```

sonic# show interface Vlan 2
Vlan2 is up
Mode of IPV4 address assignment: not-set
Mode of IPV6 address assignment: not-set
IP MTU 9100 bytes

```

```

sonic# show interface status
-----
Name      Description      Admin      Oper      Speed      MTU      Alternate Name
-----
Ethernet0   -            down      down     100000     9100      Eth1/1
Ethernet4   -            down      down     100000     9100      Eth1/2
Ethernet8   -            down      down     100000     9100      Eth1/3
Ethernet12  -            down      down     100000     9100      Eth1/4

```

```

sonic# show interface transceiver dom Eth1/32
-----
Eth1/32
-----
alarm-rx-power-hi 5.9999
alarm-rx-power-lo -7.9022
alarm-temp-hi 75.0000
alarm-temp-lo -10.0000
alarm-tx-bias-hi 75.0000
alarm-tx-bias-lo 10.0000
alarm-tx-power-hi N/A
alarm-tx-power-lo N/A
alarm-volt-hi 3.6300
alarm-volt-lo 2.9700
rx-power 3.5629,1.4019,2.0887,2.3142,-inf,-inf,-inf,-inf
temperature 27.6992
tx-bias 59.9560,59.9560,59.9560,59.9560,0.0000,0.0000,0.0000,0.0000
tx-power 2.2425,1.7768,1.3975,2.0080,-inf,-inf,-inf,-inf
type QSFP-DD
vendor DELL
vendor-part 6MGDY
voltage 3.2091
warning-rx-power-hi 4.4999

```

```

warning-rx-power-lo -6.4016
warning-temp-hi 70.0000
warning-temp-lo -5.0000
warning-tx-bias-hi 70.0000
warning-tx-bias-lo 15.0000
warning-tx-power-hi N/A
warning-tx-power-lo N/A
warning-volt-hi 3.4650
warning-volt-lo 3.1350

```

```

sonic# show interface counters rif
-----
----- Interface RX_OK RX_BPS RX_PPS RX_ERR TX_OK TX_BPS TX_PPS
----- TX_ERR -----
----- Ethernet46 561 100 32 N/A 34678 364 941 N/
A
Ethernet96 0 0 0 N/A 0 0 0 N/
A
Po33.101 258 50 4 N/A 698 100 20 N/
A
Vlan200 5432 58 123 N/A 0 0 0 N/
A
PortChannel001 0 0 0 N/A 4852 68 12 N/
A
----- -----
----- show interface counters rif Vlan 200

```

Releases 3.1 or later

show interface advertise

Displays Auto negotiation advertisement for physical interface information.

Command show interface advertise [Ethernet *if-name/if-range*]

Options *if-name/if-range*—(Optional) Interface name or range

Modes EXEC

Usage Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface.

Examples

```

sonic# show interface advertise

----- Interface Type Auto Neg Oper
----- Advertised Speed -----
----- Eth1/1 QSFP56-DD 400GBASE-CR8-DAC-1.0M off
Eth1/2 QSFP56-DD 400GBASE-CR8-DAC-1.0M off
Eth1/3 QSFP56-DD 400GBASE-CR8-DAC-2.0M off
Eth1/4 QSFP56-DD 400GBASE-CR8-DAC-2.0M off
Eth1/5/1 QSFP28 100GBASE-CR4-DAC-3.0M off
Eth1/6/1 QSFP28 100GBASE-CR4-DAC-3.0M off
Eth1/7 off
Eth1/8 off
Eth1/9/1 QSFP28 100GBASE-CR4-DAC-3.0M off
Eth1/10/1 QSFP28 100GBASE-CR4-DAC-3.0M off
Eth1/11/1 QSFP28 4x(25GBASE-CR-DAC)-3.0M off
Eth1/11/2 QSFP28 4x(25GBASE-CR-DAC)-3.0M off
Eth1/11/3 QSFP28 4x(25GBASE-CR-DAC)-3.0M on 25000
Eth1/11/4 QSFP28 4x(25GBASE-CR-DAC)-3.0M on 25000

```

Eth1/12/1	QSFP28	4x (25GBASE-CR-DAC) -3.0M	off	
Eth1/12/2	QSFP28	4x (25GBASE-CR-DAC) -3.0M	off	
Eth1/12/3	QSFP28	4x (25GBASE-CR-DAC) -3.0M	on	25000
Eth1/12/4	QSFP28	4x (25GBASE-CR-DAC) -3.0M	on	25000


```
sonic# show interface advertise Eth 1/11/3

Name: Eth1/11/3
Type: QSFP28 4x(25GBASE-CR-DAC)-3.0M
Admin State: UP
Link Status: UP
Auto Negotiation: ON
Operational FEC Mode: NONE
Operational Link Training: TRAINED
Standalone Link Training: OFF

          800G 400G 200G 100G 50G 40G 25G 10G 5G
2.5G 1G 100f 100h 10f 10h ----- -----
----- -----
Admin Local Advertisement no no no no no no yes yes no
no no no no no no no yes no no
Oper Local Advertisement no no no no no no yes no no
no no no no no no no yes no no
Oper Remote Advertisement no no no no no no yes yes no
no no no no no no no yes yes no
```

Releases 4.0 or later

show interface breakout

Displays information about breakout ports.

Command show interface breakout [dependencies {port slot/port} | modes | port slot/port | resources | detail]

Options • dependencies {port slot/port} — (Optional) Dependent interface configurations.

• modes — (Optional) Breakout modes supported on a port.

• port slot/port — (Optional) Breakout port configuration.

• resources — (Optional) Maximum number of breakout ports supported per pipeline on the switch and the current consumption.

Modes EXEC

Usage For the Z9432F-ON switch, 8x25 breakout interfaces are supported only on eight ports: Eth1/2 through Eth1/16. Use the show interface breakout command to verify the configured breakout interfaces.

Example (Z9432F-ON)

sonic# show interface breakout				
Port	Breakout Mode	Status	Interfaces	
1/2	8x25G	Completed	Ethernet8	Ethernet9
			Ethernet10	Ethernet11
			Ethernet12	Ethernet13
			Ethernet14	Ethernet15
1/4	8x25G	Completed	Ethernet24	Ethernet25
			Ethernet26	Ethernet27
			Ethernet28	Ethernet29
			Ethernet30	

1/6	8x25G	Completed	Ethernet31
			Ethernet40
			Ethernet41
			Ethernet42
			Ethernet43
			Ethernet44
			Ethernet45
			Ethernet46
			Ethernet47

```
sonic# show interface breakout modes
-----
Port Pipe Interface Supported Modes Default Mode
-----
1/1 4 Eth1/1 1x25G, 1x10G, 1x100G(4), 1x50G, 1x40G, 1x400G
1x200G, 1x400G, 2x40G, 2x200G, 2x100G(8),
4x25G, 4x10G, 4x100G
1/2 4 Eth1/2 1x25G, 1x10G, 1x100G(4), 1x50G, 1x40G, 1x400G
1x200G, 1x400G, 2x40G, 2x200G, 2x100G(8),
4x25G, 4x10G, 4x100G
1/3 1 Eth1/3 1x25G, 1x10G, 1x100G(4), 1x50G, 1x40G, 1x400G
1x200G, 1x400G, 2x40G, 2x200G, 2x100G(8),
4x25G, 4x10G, 4x100G
1/4 1 Eth1/4 1x25G, 1x10G, 1x100G(4), 1x50G, 1x40G, 1x400G
1x200G, 1x400G, 2x40G, 2x200G, 2x100G(8),
4x25G, 4x10G, 4x100G
1/5 1 Eth1/5 1x25G, 1x10G, 1x50G, 1x100G, 2x10G, 1x100G
2x25G, 2x50G
1/6 1 Eth1/6 1x25G, 1x10G, 1x50G, 1x100G, 2x10G, 1x100G
2x25G, 2x50G
...
```

```
sonic# show interface breakout dependencies port 1/1
-----
Dependent Configurations
-----
VLAN|Vlan100
VLAN_MEMBER|Vlan100|Ethernet2
```

```
sonic# show interface breakout port 1/1
-----
Port Breakout Mode Status Interfaces
-----
1/1 4x25G Completed Ethernet0
Ethernet1
Ethernet2
Ethernet3
```

```
sonic# show interface breakout resources
Maximum ports supported in the system: 144
Current ports in the system: 32
-----
Pipeline Ports Max-Ports Front-panel-ports
-----
1 16 18 1/1, 1/2, 1/3, 1/4
2 16 18 1/5, 1/6, 1/7, 1/8
3 16 18 1/9, 1/10, 1/11, 1/12
4 16 18 1/13, 1/14, 1/15, 1/16
5 16 18 1/17, 1/18, 1/19, 1/20
6 16 18 1/21, 1/22, 1/23, 1/24
7 16 18 1/25, 1/26, 1/27, 1/28
8 16 18 1/29, 1/30, 1/31, 1/32
```

```
sonic# show interface breakout detail
-----
Port Breakout Mode Status Interfaces Owner
-----
1/1 4x25G Completed Ethernet0 Auto
```

			Ethernet1	
			Ethernet2	
			Ethernet3	
1/2	1x40G	InProgress	Ethernet4	Manual
1/3	1x40G	Completed	Ethernet8	Auto
1/6	1x40G	InProgress	Ethernet20	Manual
1/14	1x100G	Completed	Ethernet52	Auto
1/15	1x100G	Completed	Ethernet56	Auto
1/16	1x100G	Completed	Ethernet60	Auto
1/18	1x100G	Completed	Ethernet68	Auto
1/19	1x10G	Completed	Ethernet72	Auto
1/20	1x25G	Completed	Ethernet76	Auto

Releases

3.1 or later

show interface counters

Displays transmitting and receiving packet statistics.

Command `show interface counters [Ethernet if-name | PortChannel portchannel-id | rate | rif [Ethernet if-name | PortChannel portchannel-id | vlan vlan-id]]`

Options

- Ethernet *if-name*—(Optional) Physical interface details
- PortChannel *portchannel-id*—(Optional) Port channel interface details
- rate—(Optional) Rate and utilization counters of interfaces details
- rif—(Optional) Routing interface details
- *if-name*—Ethernet ID
- *vlan-id*—VLAN ID (1 to 4094)

Modes

EXEC

Usage

Use this command to see the transmit and receive packet statistics.

Examples

```
sonic# show interface counters rif
Polling Rate      : 5 seconds
-----
Interface        RX_OK       RX_BPS    RX_PPS   RX_ERR   TX_OK       TX_BPS   TX_PPS   TX_ERR
-----
```

Interface	RX_OK	RX_BPS	RX_PPS	RX_ERR	TX_OK	TX_BPS	TX_PPS	TX_ERR
Ethernet64	13	0	0	N/A	33939813862	0	0	N/A
Ethernet68	43134851526	0	0	N/A	0	0	0	N/A
Ethernet72	9322684	0	0	N/A	34478831891	0	0	N/A
Ethernet76	39836873064	0	0	N/A	0	0	0	N/A
PortChannel156	0	0	0	N/A	0	0	0	N/A

Releases

4.0 or later

show interface description

Displays physical interfaces description.

Command `show interface description [Ethernet | Loopback | Management | PortChannel]`

Options

- Ethernet—Ethernet interface type
- Loopback—Loopback interface type
- Management—Management interface type
- PortChannel—Port channel interface type
- Vlan—VLAN interface type

Modes

EXEC

Usage

Use this command to display the descriptions configured on the interfaces.

Examples

```
sonic# show interface description
-----
Name          Admin   Oper    Description
-----
Management0   up      up      Management0
Eth1/1        up      down   to-spine1-vrf-default-400G
Eth1/2        up      up      to-spine1-vrf-default-400G
Eth1/3        up      up      to-spine1-vrf-Vrf-1-400G
Eth1/4        up      up      to-spine1-vrf-Vrf-1-400G
Eth1/5/1      up      up      -
Eth1/6/1      up      up      -
```

Releases

4.0 or later

show interface dropcounters

Displays drop counters for physical interfaces.

Command `show interface dropcounters Ethernet if-name`

Options Ethernet *if-name*—Physical interface details.

Modes EXEC

Usage Use this command to view the drop counters for all or specific interfaces.

Examples

```
sonic#show interface dropcounters
  IFACE   STATE    RX_ERR    RX_DROPS    TX_ERR    TX_DROPS    RX_LEGIT
  -----  -----  -----  -----  -----  -----  -----
Ethernet0    U       10       100        0         0         20
Ethernet4    U       0        1000        0         0        100
Ethernet8    U      100        10        0         0         0
```

```
sonic# show interface dropcounters Ethernet 1
-----
-----
```

Interface	STATE	RX_ERR	RX_DROPS	TX_ERR
Ethernet1	D	0	0	0

```
-----
```

Releases

4.0 or later

show interface Ethernet

Displays the information about a physical Ethernet interface or interface range.

Command `show interface Ethernet port-port`

Options Ethernet *port-port*—A physical interface or interface range details.

Modes EXEC

Usage Use this command to view the detailed information about a physical Ethernet interface and packet statistics on that interface.

Examples

```
sonic# show interface Ethernet 68
Ethernet68 is up, line protocol is up, reason oper-up
Hardware is Eth, address is 0c:29:ef:e1:f8:02
Description: Test Config
```

```

IPV4 address is 10.210.9.3/31
Mode of IPV4 address assignment: MANUAL
IPV6 address is 10:21:10:9::3/64,fe80::e29:efff:fee1:f802/64
Mode of IPV6 address assignment: MANUAL
IP MTU 9100 bytes
LineSpeed 10GB, Auto-negotiation off
FEC: DISABLED
Events:
    initialized at 2022-03-24T05:46:43.421001Z
    admin-up at 2022-03-24T05:46:53.361035Z
    xcvr-status-up at 2022-03-24T05:48:07.486835Z
    port-enabled at 2022-03-24T05:48:07.487593Z
    phy-link-up at 2022-03-24T05:48:07.729433Z
Last clearing of "show interface" counters: never
10 seconds input rate 70000 packets/sec, 769602688 bits/sec, 96200336
Bytes/sec
10 seconds output rate 19999 packets/sec, 242878752 bits/sec, 30359844
Bytes/sec
Input statistics:
    2606931547 packets, 3582259145792 octets
    20 Multicasts, 466699 Broadcasts, 2606464835 Unicasts
    0 error, 209297229 discarded, 0 Oversize
    6 Packets (128 to 255 Octects)
Output statistics:
    682419292 packets, 1035901416402 octets
    1877 Multicasts, 1 Broadcasts, 682417414 Unicasts
    0 error, 0 discarded, 0 Oversize
Time since last interface status change: 12:51:50

```

Releases

4.0 or later

show interface link-training

Displays the link-training status of all interfaces.

Command

`show interface link-training [Ethernet port-port]`

Options

`Ethernet port-port`—A physical interface or interface range details.

Modes

EXEC

Usage

Link training tunes the characteristics of the transmitted signal to be optimal over a copper cable. Use this command to display the link-training status for physical interfaces.

Examples

sonic# show interface link-training	Auto	Link-Training		
Interface	Type	Negotiation	Standalone	Operational
Ethernet0		on	off	on
Ethernet1		off	on	on
Ethernet2		off	off	off
Ethernet3		off	off	off
Ethernet4		off	off	off
Ethernet5		off	off	off
Ethernet6		off	off	off
Ethernet7		off	off	off
Ethernet8		off	off	off
Ethernet9		off	off	off
Ethernet10		off	off	off
Ethernet11		on	off	on
Ethernet12		on	off	on

sonic# show interface link-training Ethernet 0,9-12	Auto	Link-Training		
Interface	Type	Negotiation	Standalone	Operational
Ethernet0		off	off	off

Ethernet9	off	off	off
Ethernet10	off	off	off
Ethernet11	on	off	on
Ethernet12	on	off	on

Releases 4.0 or later

show interface loopback

Displays the Loopback interface details.

Command show interface loopback [*loopback-id*]

Options *loopback-id*—Loopback ID details

Modes EXEC

Usage Use this command to display the Loopback interface details.

Examples

```
sonic# show interface Loopback

Loopback0 is up, line protocol is up
Hardware is Loopback, address is 00:a0:c9:00:00:02
IPV4 address is 1.1.1.1/32
Mode of IPV4 address assignment: MANUAL
Mode of IPV6 address assignment: not-set
Interface IPv6 oper status: Disabled
Time since last interface status change: 3d03h28m

Loopback101 is up, line protocol is up
Hardware is Loopback, address is 00:a0:c9:00:00:02
IPV4 address is 101.1.1.1/32
Mode of IPV4 address assignment: MANUAL
Mode of IPV6 address assignment: not-set
Interface IPv6 oper status: Disabled
Time since last interface status change: 3d03h28m

Loopback102 is up, line protocol is up
Hardware is Loopback, address is 00:a0:c9:00:00:02
IPV4 address is 101.1.2.1/32
Mode of IPV4 address assignment: MANUAL
Mode of IPV6 address assignment: not-set
Interface IPv6 oper status: Disabled
Time since last interface status change: 3d03h28m
```

Releases 4.0 or later

show interface management

Displays the Management interface details.

Command show interface Management [*management-id*]

Options *management-id*—Enter the Management port ID.

Modes EXEC

Usage Use this command to display the Management interface details.

Examples

```
sonic# show interface Management 0
Management0 is up, line protocol is up
Hardware is MGMT, address is 0c:29:ef:e1:f8:00
Description: Management0
IPV4 address is 100.94.189.13/24
Mode of IPV4 address assignment: MANUAL
```

```

IPV6 address is 2000::13/64, fe80::e29:ffff:feel:f800/64
Mode of IPV6 address assignment: DHCP
IP MTU 1500 bytes
LineSpeed 1GB, Auto-negotiation True
Input statistics:
    75106 packets, 15083074 octets
    28980 Multicasts, 0 error, 1553 discarded
Output statistics:
    3291 packets, 765626 octets
    0 error, 0 discarded
Time since last interface status change: 12:56:27

```

Releases 4.0 or later

show interface-naming

Displays the interface naming configuration.

Command show interface-naming

Options None

Modes EXEC

Usage Use this command to view whether interface-naming is set to standard or native.

Example

```

sonic# show interface-naming
Interface naming is set to standard

```

Releases 3.1 or later

show interface phy counters

Displays the link-training status of all interfaces.

Command show interface phy { counters [Ethernet port-id] }

Options Ethernet *port*—(Optional) Enter the physical interface details.

Modes EXEC

Usage Use this command to view the Physical Coding Sublayer (PCS) error statistics.

Examples

```

sonic# show interface phy counters
-----
Eth1/39 :
-----
FEC_CORR      : 86          at 2024-05-10T06:40:58Z+00:00
FEC_NON_CORR  : 12          at 2024-05-09T12:56:58Z+00:00
FEC_SYM_ERR   : 86          at 2024-05-10T06:40:58Z+00:00
-----
Eth1/40/1 :
-----
FEC_CORR      : 313         at 2024-05-10T06:40:58Z+00:00
FEC_SYM_ERR   : 313         at 2024-05-10T06:40:58Z+00:00

```

Table 9. show interface phy counters output

Field	Description
FEC_CORR	FEC correctable errors
FEC_NON_CORR	FEC uncorrectable error

Table 9. show interface phy counters output

Field	Description
FEC_SYM_ERR	FEC symbol error

Releases 4.0 or later

show interface phy status

Displays the link-training status of all interfaces.

Command `show interface phy { status [Ethernet port-id] }`

Options Ethernet *port*—(Optional) A physical interface details

Modes EXEC

Usage Use this command to view the Physical Coding Sublayer (PCS) status and Physical Medium Dependent (PMD) status. This is used to monitor and debug serdes link quality and link down reason.

Examples

```
sonic# show interface phy status Ethernet0
-----
Ethernet0 :
-----
REMOTE_FAULT      : off since 2022-01-12 11:28:19.205152
AMPS_LOCK         : nok since 2022-01-12 11:28:19.205152
LINK              : nok since 2022-01-12 11:28:19.205152
LOCAL_FAULT       : off since 2022-01-12 11:28:19.205152
DESKEW             : nok since 2022-01-12 11:28:19.205152
HI_BER             : off since 2022-01-12 11:28:19.205152
BLOCK_LOCK        : nok since 2022-01-12 11:28:19.205152
SIGNAL_DETECT     : nok since 2022-01-12 11:28:19.205152
CDR               : nok since 2022-01-12 11:28:19.205152
AM_LOCK            : nok since 2022-01-12 11:28:19.205152
```

Table 10. show interface phy status output

Field	Description
AMPS_LOCK	PCS AMPS lock
AM_LOCK	PCS AM lock
CDR	PMD CDR Lock
DESKEW	PCS Deskew state
HI_BER	PCS HI_BER state
LINK	PCS Link state
LOCAL_FAULT	PCS Local fault
REMOTE_FAULT	PCS Remote fault
SIGNAL_DETECT	PMD Signal Detect

Releases 4.0 or later

show interface portchannel

Displays the information about a port channel interface or interface range.

Command `show interface PortChannel ID/range`

Options	<i>ID/range</i> —PortChannel ID or range (1 to 256)
Modes	EXEC
Usage	Use this command to view the information about a port channel interface or interface range.
Examples	

```
sonic# show interface PortChannel 1
PortChannel1 is up, line protocol is up, reason oper-up, mode LACP
Hardware is PortChannel, address is 90:3c:b3:c5:bd:95
Minimum number of links to bring PortChannel up is 1
Mode of IPV4 address assignment: not-set
Mode of IPV6 address assignment: not-set
Fallback: Enabled, Operational
Graceful shutdown: Disabled
MTU 9100
LineSpeed 20.0GB
Events:
    all-links-down at 2021-10-21.02:53:15.567432
    lacp-fail at 2021-10-21.02:53:15.614807
    portchannel-up at 2021-10-21.02:53:19.077914
LACP mode ACTIVE interval SLOW priority 65535 address 90:3c:b3:c5:bd:95
Members in this channel: Ethernet0(Selected)
LACP Actor port 1 address 90:3c:b3:c5:bd:95 key 1
LACP Partner port 1 address 90:3c:b3:c5:95:bd key 1
Members in this channel: Ethernet1(Selected)
LACP Actor port 2 address 90:3c:b3:c5:bd:95 key 1
LACP Partner port 2 address 90:3c:b3:c5:95:bd key 1
Last clearing of "show interface" counters: never
10 seconds input rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
10 seconds output rate 0 packets/sec, 0 bits/sec, 0 Bytes/sec
Input statistics:
    30 packets, 5594 octets
    16 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded
Output statistics:
    42 packets, 6563 octets
    28 Multicasts, 0 Broadcasts, 0 Unicasts
    0 error, 0 discarded
Time since last interface status change: 02:02:22
```

Releases	4.0 or later
-----------------	--------------

show interface port-locator

Displays port locator LED status.

Command	show interface port-locator [Ethernet <i>port-port</i>]
Options	Ethernet <i>port-port</i> —(Optional) Physical interface id or range
Modes	EXEC
Usage	Use this command to check the status of the port locator LED. The port locator LED allows you to identify ports that have cabling errors. LED blinks on the port locator-enabled ports so that you can identify the miswired ports.
Examples	

```
sonic# show interface port-locator Ethernet 1-4
      Interface      Locator Mode   Expiration Time
-----  -----
Ethernet1        Enabled
Ethernet2        Disabled
Ethernet3        Disabled
Ethernet4        Disabled
```

```
sonic# show interface port-locator
```

Interface	Locator Mode	Expiration Time
Eth1/1	Disabled	
Eth1/2	Disabled	
Eth1/3	Disabled	
Eth1/4	Enabled	
Eth1/5	Enabled	
Eth1/6	Enabled	
Eth1/7	Enabled	2021-08-13 02:52:46
Eth1/8	Disabled	

Releases 4.0 or later

show interface status

Displays the link and autonegotiation status of all interfaces.

Command `show interface status [admin-down | err-disabled | phy-link-down | oper-up | all-links-down | lacp-fail | min-links]`

Options

- `admin-down` — (Optional) Admin down interface details
- `err-disabled` — (Optional) Error disabled interface details
- `phy-link-down` —(Optional) Physical link down interface details
- `oper-up` — (Optional) Operation status up interface details
- `all-links-down` — (Optional) All links down interface details
- `lacp-fail` — (Optional) LACP failed interface details
- `min-links` — (Optional) Minimum links interface details

Modes EXEC

Usage

There is an option to list the interfaces with the specified reason. The output is displayed with more details like related events with timestamp of occurrence.

Examples

sonic# show interface status								
Name	Description	Oper	Reason	AutoNeg	Speed	MTU	Alternate Name	Name
Ethernet0	-	down	admin-down	off	25000	9100	Eth1/1	
Ethernet1	-	down	admin-down	off	25000	9100	Eth1/2	
Ethernet2	-	down	admin-down	off	25000	9100	Eth1/3	
Ethernet3	-	down	admin-down	off	25000	9100	Eth1/4	
Ethernet4	-	down	admin-down	off	25000	9100	Eth1/5	
PortChannel1	-	down	admin-down	-	20000	9100	-	
PortChannel3	-	down	min-links	-	30000	9100	-	
PortChannel5	-	down	err-disabled	-	30000	9100	-	
PortChannel7	-	down	all-links-down-		40000	9100	-	

Output for specific reason:

sonic# show interface status phy-link-down		
Interface	Event	Timestamp
Ethernet0	transceiver-not-present	2022-01-11T14:29:44.752701Z
Ethernet1	transceiver-not-present	2022-01-11T14:29:44.753316Z
Ethernet2	transceiver-not-present	2022-01-11T14:29:44.753676Z
Ethernet3	transceiver-not-present	2022-01-11T14:29:44.754002Z
Ethernet4	transceiver-not-present	2022-01-11T14:29:44.754316Z
Ethernet5	transceiver-not-present	2022-01-11T14:29:44.75463Z
Ethernet6	transceiver-not-present	2022-01-11T14:29:44.754972Z
Ethernet8	transceiver-incompatible	2022-01-11T14:29:42.827712Z
Ethernet9	transceiver-incompatible	2022-01-11T14:29:42.838054Z
Ethernet10	transceiver-not-present	2022-01-11T14:29:44.755749Z

Releases 4.0 or later

show interface transceiver

Displays the information of the transceivers that are installed in Ethernet ports.

Command show interface transceiver [Eth slot/port[/breakout-port | dom [summary] | summary]]

- Options**
- *slot/port[/breakout-port]*—Specify the port information.
 - *dom*—Displays transceiver DOM information.
 - *summary*—Displays the summary of transceiver information.

Modes EXEC

Usage

In the show interface transceiver output, N/A or NOT-PRESENT indicate that no transceiver is installed. To view the show output in one display without having to page through screen displays, enter show interface transceiver | no-more.

(i) NOTE: If the standard interface-naming mode is enabled, you must enter the Ethernet interface in the format show interface transceiver Eth slot/port[/breakout-port]; for example, show interface transceiver Eth 1/1/1.

(i) NOTE: In show interface transceiver Eth port command output, the is-high-power-media value displays as True only if the max-module-power (Watts) is equal to or greater than the max-port-power (Watts). The is-high-power-media value displays as False if the max-module-power (Watts) is less than the max-port-power (Watts).

Example

```
sonic# show interface transceiver

Eth1/1
-----
Attribute : Value/State
-----
present   : NOT-PRESENT

Eth1/4/1
-----
Attribute : Value/State
-----
cable-length(m)      : 2
connector-type       : NO-SEPARABLE
date-code            : 2022-08-26
display-name         : QSFP56-DD 400GBASE-CR8-DAC-2.0M
firmware-revision    : 0.0
form-factor          : QSFP56-DD-TYPE1
is-high-power-media  : False
max-module-power(Watts) : 1.5
max-port-power(Watts)  : 15
media-lockdown-state : False
present              : PRESENT
qualified             : True
revision-compliance   : 3.0
serial-no             : CN0LXD0028QJ0LB
vendor                : DELL EMC
vendor-oui             : 3C-18-A0
vendor-part            : XR11M
vendor-rev             : A0

Eth1/33
-----
Attribute : Value/State
-----
cable-length(m)      : 0
connector-type       : LC
date-code            : 2013-06-08
display-name         : SFP+ 10GBASE-SR
form-factor          : SFP+
is-high-power-media  : False
```

```

max-module-power(Watts)      : 2
max-port-power(Watts)        : 15
media-lockdown-state         : False
present                      : PRESENT
qualified                     : True
serial-no                     : APP26J3
vendor                        : FINISAR CORP.
vendor-oui                    : 00-90-65
vendor-part                   : FTLX8571D3BCL-FC
vendor-rev                    : A0

Eth1/34
-----
Attribute          : Value/State
-----
cable-length(m)    : 0
connector-type     : LC
date-code          : 2017-09-07
display-name       : SFP+ 10GBASE-SR
form-factor        : SFP+
is-high-power-media: False
max-module-power(Watts): 2
max-port-power(Watts)  : 15
media-lockdown-state: False
present            : PRESENT
qualified           : True
serial-no          : AD795A023J
vendor              : DELL
vendor-oui         : 00-17-6A
vendor-part         : WTRD1
vendor-rev          : A0

```

```
sonic# show interface transceiver Eth 1/4/1
```

```

Eth 1/4/1
-----
Attribute          : Value/State
-----
cable-length(m)    : 2
connector-type     : NO-SEPARABLE
date-code          : 2022-08-26
display-name       : QSFP56-DD 400GBASE-CR8-DAC-2.0M
firmware-revision : 0.0
form-factor        : QSFP56-DD-TYPE1
is-high-power-media: False
max-module-power(Watts): 1.5
max-port-power(Watts)  : 15
media-lockdown-state: False
present            : PRESENT
qualified           : True
revision-compliance: 3.0
serial-no          : CN0LXD0028QJ0LB
vendor              : DELL EMC
vendor-oui         : 3C-18-A0
vendor-part         : XR11M
vendor-rev          : A0

```

```
sonic# show interface transceiver Ethernet76 summary
```

Interface No.	Name	Vendor	Part
	Serial No.	QSA Adapter	Qualified
Ethernet76 616760003	QSFP+ 4x(10GBASE-CR-DAC)-3.0M CN027GG535R03VK	N/A	Amphenol True

Releases

4.1.0 or later

show interface transceiver wattage

Displays wattage information of the optics present in the switch.

Command show interface transceiver wattage

Options None

Modes EXEC

Usage Use the show interface transceiver wattage command to view information about each Z9332F-ON or Z9432F-ON port in which pluggable media is inserted:

- Maximum media power threshold above which an optic is disabled on the interface.
- Maximum port power threshold above which an optic is disabled on the interface.
- A field to indicate if the pluggable optic present in the port is a high-power optic or not.
- A field to indicate if the pluggable optic is enabled or disabled.

(i) NOTE: The High-Power-Media value displays as True only if the Media-Max-Power is equal to or greater than the Port-Max-Power. The High-Power-Media value displays as False if the Media-Max-Power is less than the Port-Max-Power.

Examples

Interface	Media	Media-Max-Power	Port-Max-Power	High-Power-Media	Media-Lockdown-state
Eth1/1	QSFP56-DD 400GBASE-ZR	18	15	True	True
Eth1/2	Not Present				
Eth1/3	QSFP56-DD 400GBASE-CR8-DAC-0.5M	1.5	15	False	False
Eth1/4	Not Present				
Eth1/5	QSFP56-DD 400GBASE-CR8-DAC-0.5M	1.5	15	False	False
Eth1/6	Not Present				
Eth1/7	QSFP+ 40GBASE-CR4-DAC-1.0M	1.5	15	False	False
Eth1/8	QSFP28 100GBASE-CR4-DAC-1.0M	1.5	15	False	False
Eth1/9	QSFP56-DD 400GBASE-ZR	19	20	True	False
Eth1/10	QSFP+ 40GBASE-SR4	1.5	15	False	False
Eth1/11	Not Present				
Eth1/12	Not Present				
Eth1/13	Not Present				
Eth1/14	Not Present				
Eth1/15	QSFP28 100GBASE-CR4-DAC-1.0M	1.5	15	False	False
Eth1/16	Not Present				
Eth1/17	Not Present				
Eth1/18	Not Present				
Eth1/19	Not Present				
Eth1/20	Not Present				
Eth1/21	Not Present				
Eth1/22	Not Present				
Eth1/23	QSFP+ 40GBASE-CR4-DAC-1.0M	1.5	20	False	False
Eth1/24	Not Present				
Eth1/25	Not Present				
Eth1/26	Not Present				
Eth1/27	Not Present				
Eth1/28	QSFP+ 40GBASE-CR4-DAC-2.0M	1.5	15	False	False
Eth1/29	Not Present				
Eth1/30	Not Present				
Eth1/31	Not Present				
Eth1/32	Not Present				
Eth1/33	Not Present				
Eth1/34	Not Present				

Releases 4.1.0 or later

show interface transceiver summary

Displays the summary of transceivers that are installed in Ethernet ports.

Command show interface transceiver summary

Options None

Modes EXEC

Usage Use this command to view the summary of the transceivers that are installed in Ethernet ports.

Example

Interface	Name	Vendor	Part No.	Serial No.

Ethernet0	QSFP+	4x(10GBASE-CR-DAC)-1.0M	DELL	L56QF023-SD-R	161140006
Ethernet4	QSFP+	4x(10GBASE-CR-DAC)-1.0M	Amphenol	616760001	CN0TCPM23
Ethernet8	QSFP+	4x(10GBASE-CR-DAC)-1.0M	Amphenol	616760001	CN0TCPM23
Ethernet12	QSFP+	4x(10GBASE-CR-DAC)-1.0M	Amphenol	616760001	CN0TCPM23
Ethernet16	QSFP+	40GBASE-SR4	AVAGO	AFBR-79E4Z-D-FT1	QC011115
Ethernet17	QSFP+	40GBASE-SR4	AVAGO	AFBR-79E4Z-D-FT1	QC011115
Ethernet18	QSFP+	40GBASE-SR4	AVAGO	AFBR-79E4Z-D-FT1	QC011115
Ethernet19	QSFP+	40GBASE-SR4	AVAGO	AFBR-79E4Z-D-FT1	QC011115
Ethernet20	QSFP+	40GBASE-CR4-DAC-1.0M	DELL	L56QF026-SD-R	171127736
Ethernet21	QSFP+	40GBASE-CR4-DAC-1.0M	DELL	L56QF026-SD-R	171127736
Ethernet22	QSFP+	40GBASE-CR4-DAC-1.0M	DELL	L56QF026-SD-R	171127736
Ethernet23	QSFP+	40GBASE-CR4-DAC-1.0M	DELL	L56QF026-SD-R	171127736
Ethernet24	N/A		N/A	N/A	N/A
Ethernet28	N/A		N/A	N/A	N/A
Ethernet32	QSFP+	40GBASE-CR4-DAC-1.0M	Amphenol	599690001	APF124200
Ethernet36	QSFP+	40GBASE-CR4-DAC-1.0M	Amphenol	599690001	APF123000
Ethernet40	QSFP+	40GBASE-SR4	DELL EMC	FTL410QE3C-FC	CN0F1C001
Ethernet41	QSFP+	40GBASE-SR4	DELL EMC	FTL410QE3C-FC	CN0F1C001
Ethernet42	QSFP+	40GBASE-SR4	DELL EMC	FTL410QE3C-FC	CN0F1C001
Ethernet43	QSFP+	40GBASE-SR4	DELL EMC	FTL410QE3C-FC	CN0F1C001
Ethernet44	QSFP28	100GBASE-CR4-DAC-1.0M	DELL	P7C7N	CN0772065
--more--					

Releases 4.1.0 or later

show interface unreliable-los status

Displays loss of signal (LOS) of an interface or interface range.

Command show interface unreliable-los status [Ethslot/port[/breakout-port] | port-range]

Options

- Ethslot/port[/breakout-port]—Enter an Ethernet interface by specifying its slot and port number.
- port-range—Enter an Ethernet port range. Separate each range or individual interface number with a comma.

Modes EXEC

Usage Use this command to display unreliable LOS of an interface or interface range.

Examples

```
sonic# show interface unreliable-los status Eth 1/42-1/44

Interface      Type          Oper    Admin   If-State
-----  -----
Eth1/42        QSFP+ 40GBASE-SR4  on     auto    oper-up
Eth1/43        QSFP+ 40GBASE-SR4  off    none    admin-down
Eth1/44        QSFP+ 40GBASE-SR4  off    auto    oper-up
```

Releases 4.1.0 or later

show interface vlan-mappings

Displays the C-VLAN to S-VLAN ID mappings for VLAN translation that are used to transmit customer VLAN traffic over a service provider network.

Command show interface {Ethslot/port | PortChannel portchannel-number} vlan-mappings

Options

- Ethslot/port — Enter an Ethernet interface.
- PortChannel portchannel-number — Enter a port-channel number.

Modes EXEC

Usage

The show output displays the customer VLAN IDs that are mapped to a service provider VLAN ID for VLAN translation in a provider network. In the Flags column, M indicates multi-tag CVLAN-to-SVLAN mapping, and is only displayed for Trident3 switches that support the multi-tag option.

Examples

```
sonic# show interface vlan-mappings
-----
Name      Outer   Inner   Mapped Vlan  Priority  Flags
-----
Eth1/1    100     -       1000      -         M
Eth1/1    200     20      2000      3         -
Eth1/7    100     -       1000      -         M
PortChannel10 400     40      3000      -         -

sonic# show interface Eth1/1 vlan-mappings
-----
Name      Outer   Inner   Mapped Vlan  Priority  Flags
-----
Eth1/1    100     -       1000      -         M
Eth1/1    200     20      2000      3         -
```

Releases

4.1.0 or later

show interface vlan-mappings dot1q-tunnel

Displays the Q-in-Q VLAN configurations that are used to transmit customer VLAN traffic over a service provider network.

Command

```
show interface {Ethslot/port | PortChannel portchannel-number} vlan-
mappings dot1q-tunnel
```

Options

- *Ethslot/port* — Enter an Ethernet interface.
- *PortChannel portchannel-number* — Enter a port-channel number.

Modes

EXEC

Usage

The show output displays the customer VLAN IDs that are mapped to a service provider VLAN ID for Q-in-Q VLAN tunneling.

Examples

```
sonic# show interface vlan-mappings dot1q-tunnel
-----
Name      Vlan          dot1q-tunnel Vlan  Priority
-----
Eth1/2    10            100          -      -
Eth1/2    11-20         200          7      -
Eth1/4    30,32,35-40   300          -      -

sonic# show interface Eth1/2 vlan-mappings dot1q-tunnel
-----
Name      Vlan          dot1q-tunnel Vlan  Priority
-----
Eth1/2    10            100          -      -
Eth1/2    11-20         200          7      -
```

Releases

4.1.0 or later

show ip access-group

Displays all IPv4 access-group information.

Command

```
show ip access-group
```

Options

None

Modes

EXEC

Usage

Use this command to view ingress and egress IPv4 access-group configuration information.

Example

```
sonic# show ip access-group
Ingress IP access-list ACL1 on Ethernet0
Egress IP access-list ACL3 on Ethernet4
```

Releases

3.0 or later

show ip access-lists

Displays IPv4 access-lists information.

Command

```
show ip access-lists [access-list-name {[interface {Ethernet | PortChannel | Vlan | eth-sub-if-id | po-sub-if-id}] | [Switch]}]
```

Options

- *access-list-name*—(Optional) Access-list name (up to 63 characters)
- *PortChannel*—(Optional) PortChannel number
- *Vlan*—(Optional) VLAN number
- *eth-sub-if-id*/*eth-sub-if-id*—(Optional) Ethernet subinterface ID
- *po-sub-if-id*—(Optional) PortChannel subinterface ID

Modes

EXEC

Usage

Use this command to view information about all IPv4 access-lists, or for a specific access-list name.

Example

```
sonic# show ip access-lists
ip access-list ipacl-example
    seq 10 permit ip host 10.1.1.1 host 20.1.1.1 (0 packets) [0 bytes]
    seq 20 permit ip host 10.1.1.2 host 20.1.1.2 (0 packets) [0 bytes]
    seq 30 permit ip host 10.1.1.3 host 20.1.1.3 (0 packets) [0 bytes]
    seq 40 permit ip host 10.1.1.4 host 20.1.1.4 (0 packets) [0 bytes]
```

Releases

3.2 or later

show ip arp

Displays all ARP entries.

Command

```
show ip arp [vrf {vrfname | mgmt | all}] {[ip-addr] | {[mac-address mac-addr]} | [summary]}
```

Options

- *vrfname* — VRF name prefixed by Vrf (up to 15 characters)
- *ip-addr* — (Optional) IP address in A.B.C.D format
- *mac-addr* — (Optional) MAC address in nn:nn:nn:nn:nn:nn format

Modes

EXEC

Usage

Use this command to view all ARP entry configuration information, or for a specific IP address.

Examples

```
sonic# show ip arp
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address      Hardware address      Interface      Egress Interface      Type      Action
-----
10.59.128.1  00:00:0c:9f:f4:68  Management0      -          Dynamic      Fwd
10.59.128.2  18:80:90:23:98:49  Management0      -          Dynamic      Fwd
10.59.128.3  18:80:90:23:9c:09  Management0      -          Dynamic      Fwd
```

```
sonic# show ip arp interface Vlan 100
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address      Hardware address      Interface      Egress Interface Type      Action
```

```

-----
192.168.3.6 00:01:02:03:04:05 Vlan100      Ethernet4        Dynamic Fwd
sonic# show ip arp interface Management 0
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address      Hardware address   Interface  Egress Interface Type     Action
-----
10.11.48.254 00:01:e8:8b:44:71 Management0 -          Dynamic Fwd
10.14.8.102  00:01:e8:8b:44:71 Management0 -          Dynamic Fwd

sonic# show ip arp 192.168.1.4
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address      Hardware address   Interface  Egress Interface Type     Action
-----
192.168.1.4  00:01:02:03:44:55 Ethernet8    -          Dynamic Fwd

sonic# show ip arp mac-address 00:01:02:03:ab:cd
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address      Hardware address   Interface  Egress Interface Type     Action
-----
192.168.2.4  00:01:02:03:ab:cd PortChannel1200 -          Dynamic Fwd

```

Releases 3.1 or later

show ip arp interface

Displays ARP entries for an interface.

Command `show ip arp interface {{phy-if-name [summary]} | {phy-subif-name [summary]} | {Loopback {lo-id [summary]}} | {Management {mgmt-if-id [summary]}} | {PortChannel {lag-id [summary]}} | {Vlan {vlan-id [summary]}} | {Vxlan {vxlan-if-name [summary]}}}}`

Options

- *phy-if-name*—Enter a physical interface name.
- *phy-subif-name*—Enter a physical subinterface name.
- *lo-id*—Enter a loopback interface ID (0 to 16383).
- *mgmt-if-id*—Enter the Management interface ID (0).
- *lag-id*—Enter a PortChannel ID (1 to 128).
- *vlan-id*—Enter a VLAN ID (1 to 4094).
- *vxlan-if-name*—Enter a VXLAN name (up to 63 characters).

Modes EXEC

Usage

Use this command to view a summary of ARP interface entries, or entries for a specific interface.

Example

```

sonic# show ip arp interface Vlan 1
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address      Hardware address   Interface  Egress Interface Type     Action
-----
193.0.1.11   08:c0:eb:c1:b1:5e  Vlan1     Eth1/3/3       Dynamic Fwd

```

Releases 3.2 or later

show ip dhcp snooping

Displays general information about IPv4 DHCP snooping.

Command `show ip dhcp snooping`

Options	None
Modes	EXEC
Usage	Use this command to see if DHCP snooping is enabled or disabled, what VLANs it is configured on, and which ports are tagged as Trusted. It also shows the dynamic VLANs on which DHCP snooping is automatically enabled when showing the VLANs.
Examples	<pre>sonic# show ip dhcp snooping DHCP snooping is Enabled DHCP snooping source MAC verification is Enabled DHCP snooping is enabled on the following VLANs: 100 DHCP snooping trusted interfaces: Ethernet10</pre>
Releases	4.0 or later

show ip dhcp snooping binding

Displays the IPv4 DHCP snooping binding database.

Command	show ip dhcp snooping binding
Options	None
Modes	EXEC
Usage	Use this command to view the IPv4 DHCP snooping binding database.
Examples	<pre>sonic# show ip dhcp snooping binding Total number of Dynamic bindings: 0 Total number of Static bindings: 1 Total number of Tentative bindings: 0 MAC address IP Address VLAN Interface Type Lease (Secs) ----- ----- 00:00:00:00:00:01 10.1.1.1 100 Ethernet15 Static NA</pre>
Releases	4.0 or later

show ip dhcp snooping statistics

Displays the IPv4 DHCP snooping statistics.

Command	show ip dhcp snooping statistics
Options	None
Modes	EXEC
Usage	Use this command to view the DHCP snooping packet validation statistics.
Examples	<pre>sonic# show ip dhcp snooping statistics Interface MAC Verify Client Ifc DHCP Server Failures Mismatch Msgs Recvd ----- ----- Ethernet0 0 0 0 Ethernet1 0 0 0 Ethernet2 0 0 0 Ethernet3 0 0 0 Ethernet4 0 0 0 Ethernet5 0 0 0 Ethernet6 0 0 0 Ethernet7 0 0 0 Ethernet8 0 0 0</pre>

Table 11. show ip dhcp snooping statistics output

Field	Description
MAC Verify Failures	DHCP packets whose source MAC does not match the client hardware address.
Client Interface Mismatch	DHCP packets whose packet details (MAC, Incoming interface) do not match details in the snooping entry.
DHCP Server Msgs Recvd	DHCP packets received on an untrusted port.

Releases 4.0 or later

show ip dhcp snooping statistics detail

Displays the IPv4 DHCP snooping detailed statistics.

Command show ip dhcp snooping statistics detail

Options None

Modes EXEC

Usage Use this command to view the DHCP snooping detailed statistics.

Examples

```
sonic# show ip dhcp snooping statistics detail
DHCPv4 Snooping Detailed Statistics
-----
Error receiving from DHCP snooping socket : 0
DHCP message too big : 0
Illegal source IP address in snooped packet : 0
Illegal source MAC in snooped packet : 0
Error sending from DHCP snooping socket : 0
Number of DHCP messages intercepted : 0
Number of DHCP messages processed : 0
Number of DHCP messages filtered : 0
Number of DHCP messages forwarded : 0
Rx RELEASE or DECLINE from client not in bindings db : 0
Number of bindings added to bindings table : 0
Number of bindings removed from bindings table : 0
MAC verification failures/server frames recv'd on untrusted ports : 0
Number of DHCP messages dropped as static binding exists : 0
Packets dropped due to no outgoing interface or interface down : 0
```

Releases 4.0 or later

show ip dhcp-relay

Displays IP DHCP relay configuration.

Command show ip dhcp-relay {[brief] | {[detailed {[intfName1] | [pchName1] | [vlanName1]}]} | {[statistics {[intfName] | [pchName] | [vlanName]}]}}}

Options

- *intfName1* — (Optional) Displays detailed information on all interfaces or for a specific interface
- *pchName1* — (Optional) Displays detailed information on all PortChannels or for a specific PortChannel
- *vlanName1* — (Optional) Displays detailed information on all VLANs or for a specific VLAN
- *intfName* — (Optional) Displays statistics for a specific interface
- *pchName* — (Optional) Displays statistics for a specific PortChannel

Modes EXEC

Usage

Use this command to display DHCPv4 statistics, relay configuration, or relay statistics for a given interface. If the interface name is not specified, this command displays information for all interfaces enabled for DHCP relay. If the given interface is not enabled for DHCP relay, this command returns an error message. If the source interface is not configured, the command output displays as *Not Configured*.

Examples

```
sonic# show ip dhcp-relay brief
-----
Interface          DHCP Helper Address
-----
Ethernet0          30.1.1.1
Ethernet0          40.1.1.1
```

```
sonic# show ip dhcp-relay detailed Vlan100
Relay Interface: Vlan100
Server Address: 112.0.0.2
Server VRF: VrfRed
Source Interface: Loopback1
Link Select: enable
VRF Select: enable
Max Hop Count: 10
Policy Action: Discard
```

```
sonic# show ip dhcp-relay statistics Vlan100
BOOTREQUEST messages received by the relay agent: 4
BOOTREQUEST messages forwarded by the relay agent: 2
BOOTREPLY messages forwarded by the relay agent: 0
DHCP DISCOVER messages received by the relay agent: 1
DHCP OFFER messages sent by the relay agent: 0
DHCP REQUEST messages received by the relay agent: 1
DHCP ACK messages sent by the relay agent: 0
DHCP RELEASE messages received by the relay agent: 0
DHCP DECLINE messages received by the relay agent: 0
DHCP INFORM messages received by the relay agent: 0
DHCP NACK messages sent by the relay agent: 0
Total number of DHCP packets dropped by the relay agent: 2
Number of DHCP packets dropped due to an invalid opcode: 0
Number of DHCP packets dropped due to an invalid option: 0
Errors relaying packets from clients: 0
Errors relaying packets from servers: 0
Packets dropped with bogus GIADDR: 0
Packets dropped due to bad relay info: 0
Packets dropped due to missing relay info: 0
Packets dropped due to invalid hdr length: 0
Packets dropped on interface with no IP: 0
Replies dropped on downstream interface: 0
Requests dropped on upstream interface: 2
DHCPv4 OFFER packets received from server: 0
DHCPv4 ACK packets received from server: 0
DHCPv4 NACK packets received from server: 0
Packets dropped on exceeding the max hop count: 0
DHCPv4 OFFER packets relayed to client on other downstream interface: 0
DHCPv4 ACK packets relayed to client on other downstream interface: 0
DHCPv4 NACK packets relayed to client on other downstream interface: 0
```

Releases

3.2 or later

show ip forward-protocol

Displays IP helper global information.

Command `show ip forward-protocol`

Options None

Modes EXEC

Usage Use this command to view IP helper global information.

Example

```
sonic# show ip forward-protocol
UDP forwarding : Enabled
UDP rate limit : 2000 pps
UDP forwarding enabled on the ports: TFTP, DNS, NTP, TACACS, 12200, 12202
UDP forwarding disabled on the ports: NetBios-Name-Server, NetBios-Datagram-Server
```

Releases

3.1 or later

show ip helper-address

Displays IP helper server addresses configured on an interface.

Command

```
show ip helper-address [iface]
```

Options

iface—(Optional) Interface range type

Modes

EXEC

Usage

Use this command to view IP helper server addresses configured on an interface or all interfaces.

Example

```
sonic# show ip helper-address
Interface      Vrf      Relay Address
-----  -----
Vlan200        4.4.4.4
Ethernet0       1.1.1.1
                  Vrf1    2.2.2.2
Vlan100        3.3.3.3
Ethernet4       5.5.5.5
                  7.7.7.7
```

```
sonic# show ip helper-address Ethernet0
Interface      Vrf      Relay Address
-----  -----
Ethernet0      Vrf1    2.2.2.2
                  1.1.1.1
```

Releases

3.1 or later

show ip helper-address statistics

Displays IP helper packet counters and statistics on an interface.

Command

```
show ip helper-address statistics [iface]
```

Options

iface—(Optional) Enter interface details.

Modes

EXEC

Usage

Use this command to view IP helper packet counters and statistics on an interface or all interfaces. Use `clear ip helper-address statistics` to clear the statistics.

Examples

```
sonic# show ip helper-address statistics
Ethernet0
-----
Packets received : 0
Packets relayed : 24
Packets dropped : 0
Invalid TTL packets : 0
All ones broadcast packets received : 0
Net directed broadcast packets received : 0
Vlan100
-----
Packets received : 45678
Packets relayed : 0
```

```

    Packets dropped : 0
    Invalid TTL packets : 0
    All ones broadcast packets received : 0
    Net directed broadcast packets received : 0
Ethernet4
-----
    Packets received : 0
    Packets relayed : 0
    Packets dropped : 24444
    Invalid TTL packets : 0
    All ones broadcast packets received : 0
    Net directed broadcast packets received : 0

sonic# show ip helper-address statistics Vlan100
    Packets received : 45678
    Packets relayed : 0
    Packets dropped : 0
    Invalid TTL packets : 0
    All ones broadcast packets received : 0
    Net directed broadcast packets received : 0

```

Releases

3.1 or later

show ip igmp snooping

Display IPv4 IGMP snooping membership details.

Command `show ip igmp snooping {{[vlan vlan-id]}} {[groups {[vlan vlan-id]}}} }`

Options *vlan-id*—(Optional) VLAN ID (1 to 4094)

Modes EXEC

Usage Use this command to view IGMP snooping configuration across all VLANs, a specified VLAN, or display IGMP snooping groups across all VLANs or a specified VLAN.

Examples

```

sonic# show ip igmp snooping
Vlan ID: 100
Querier: Disabled
IGMP Operation mode: IGMPv1
Is Fast-Leave Enabled: Disabled
Query interval: 125
Last Member Query Interval: 1000
Max Response time: 10

Vlan ID: 200
Querier: Enabled
IGMP Operation mode: IGMPv2
Is Fast-Leave Enabled: Disabled
Query interval: 125
Last Member Query Interval: 1000
Max Response time: 10

Vlan ID: 300
Querier: Enabled
IGMP Operation mode: IGMPv3
Is Fast-Leave Enabled: Disabled
Query interval: 20
Last Member Query Interval: 1000
Max Response time: 10

```

```

sonic# show ip igmp snooping vlan 200
Vlan ID: 200
Querier: Enabled
IGMP Operation mode: IGMPv2
Is Fast-Leave Enabled: Disabled
Query interval: 125

```

```
Last Member Query Interval: 1000
Max Response time: 10

sonic# show ip igmp snooping groups
Vlan ID: 100
-----
1 (*, 225.1.1.1)
    Outgoing Ports: Ethernet4, PortChannel13
2 (*, 225.1.1.2)
    Outgoing Ports: Ethernet8
Total number of entries: 2

Vlan ID : 300
-----
1 (100.10.2.3, 226.0.0.1 )
    Outgoing Ports: Ethernet8, Portchannel12
Total number of entries: 1
```

```
sonic# show ip igmp snooping groups vlan 100
Vlan ID: 100
-----
1 (*, 225.1.1.1)
    Outgoing Ports: Ethernet4, PortChannel13
2 (*, 225.1.1.2)
    Outgoing Ports: Ethernet8
Total number of entries: 2
```

Releases 3.2 or later

show ip igmp groups

Displays IGMP groups information.

Command show ip igmp groups

Options None

Modes EXEC

Usage Use this command to check the IGMP groups learned on all interfaces.

Example

```
sonic# show ip igmp groups

Interface      Address          Group          Mode   Timer     Srcs   V   Uptime
Vlan301        33.33.33.1      232.1.1.1      ----  00:00:03  1       2   00:00:02
```

Releases 3.2 or later

show ip igmp interface

Displays IGMP interface information.

Command show ip igmp interface *interfacename* [detail]

Options *interfacename*—Enter an interface name.

Modes EXEC

Usage Use this command to display the detailed IGMP information for a specific interface.

Example

```
sonic# show ip igmp interface Vlan301

Interface : Vlan301
State     : up
```

```

Address      : 33.33.33.1
Uptime       : 00:00:48
Version      : 2

Querier
-----
Querier      : local
Start Count  : 0
Query Timer  : 00:00:01
Other Timer   : --:--:--

Timers
-----
Group Membership Interval      : 5s
Last Member Query Count       : 2
Last Member Query Time        : 2s
Older Host Present Interval  : 5s
Other Querier Present Interval: 4s
Query Interval                : 2s
Query Response Interval       : 1s
Robustness Variable           : 2
Startup Query Interval         : 1s

Flags
-----
All Multicast    : no
Broadcast       : yes
Deleted         : no
Interface Index : 185
Multicast       : yes
Multicast Loop  : 0
Promiscuous     : no

```

Releases 3.2 or later

show ip igmp join

Displays IGMP static join information.

Command show ip igmp join

Options None

Modes EXEC

Usage Use this command to display IGMP static join information.

Examples

```

sonic# show ip igmp join
Interface  Address      Source      Group      Socket Uptime
Ethernet8  *            90.0.0.2   232.1.1.1  15 00:00:07
Ethernet8  *            91.0.0.2   232.1.1.1  16 00:00:07

```

Releases 3.2 or later

show ip igmp sources

Displays IGMP sources information.

Command show ip igmp sources

Options None

Modes EXEC

Usage Use this command to display IGMP sources. This command helps to verify whether the receivers have joined for specific sources.

Example

```
sonic# show ip igmp sources
Interface      Address          Group           Source   Timer     Fwd     Uptime
Vlan301        33.33.33.1      232.1.1.1      *        00:00:03  Y       00:00:02
```

Releases

3.2 or later

show ip igmp statistics

Displays IGMP receive packet statistics information.

Command

```
show ip igmp statistics [interface interfacename]
```

Options

- interfacename*—(Optional) Enter an interface name.

Modes

EXEC

Usage

Use this command to display IGMP receive packet statistics information for a specific interface or all interfaces.

Example

```
sonic# show ip igmp statistics
IGMP RX statistics
Interface      : global
V1 query       : 0
V2 query       : 0
V3 query       : 36
V2 leave       : 0
V1 report      : 0
V2 report      : 0
V3 report      : 74
mtrace response: 0
mtrace request : 0
unsupported     : 0
```

Releases

3.2 or later

show ip igmp vrf

Displays IGMP VRF information.

Command

```
show ip igmp vrf {vrf-name | all} {[interface [interfacename]]} | [statistics] | [groups] | [sources] | [join]]}
```

Options

- vrf-name*—Enter the name of the VRF prefixed by Vrf (up to 15 characters).
- all*—Display all information.
- interfacename*—(Optional) Enter the interface name.
- statistics*—(Optional) Display statistics information.
- groups*—(Optional) Display group information.
- sources*—(Optional) Display source information.
- join*—(Optional) Display join information.

Modes

EXEC

Usage

Use this command to display the IGMP information for a nondefault VRF.

Example

```
sonic# show ip igmp vrf Vrf-1 statistics
IGMP RX statistics
Interface      : Global
V1 query       : 0
V2 query       : 0
V3 query       : 0
V2 leave       : 0
V1 report      : 0
V2 report      : 0
```

```
V3 report      : 6
mtrace response : 0
mtrace request  : 0
unsupported     : 0
sonic#
```

Releases 3.2 or later

show ip interfaces

Displays IPv4 interface configuration information.

Command show ip interfaces

Options None

Modes EXEC

Usage Use this command to display all interfaces configured with IPV4 address.

Example

```
sonic# show ip interfaces
Flags: U-Unnumbered interface, A-Anycast IP
-----
Interface      IP address/mask      VRF      Admin/Oper      Flags
-----
Ethernet60    99.201.0.1/24          up/up
Vlan1001      100.1.1.1/24          up/up
Vlan1002      100.1.2.1/24          up/up
Vlan1003      100.1.3.1/24          up/up
Vlan1004      100.1.4.1/24          up/up
Vlan1005      100.1.5.1/24          up/up
Vlan1006      100.1.6.1/24          up/up
Vlan1007      100.1.7.1/24          up/up
Vlan1008      100.1.8.1/24          up/up
Vlan1009      100.1.9.1/24          up/up
Vlan1010      100.1.10.1/24         up/up
Vlan1011      100.1.11.1/24         up/up
Vlan1012      100.1.12.1/24         up/up
Vlan1013      100.1.13.1/24         up/up
Vlan1014      100.1.14.1/24         up/up
Vlan1015      100.1.15.1/24         up/up
Vlan1016      100.1.16.1/24         up/up
Vlan2001      100.2.1.1/24          up/up
Vlan2002      100.2.2.1/24          up/up
Vlan2003      100.2.3.1/24          up/up
--more--
```

Releases 3.0 or later

show ip load-share

Displays load share information of ECMP paths.

Command show ip load-share

Options None

Modes EXEC

Usage Use this command to view the load balance attributes or fields that are used for ECMP hashing.

Example

```
sonic# show ip load-share
IP Hash Mode: Default
IPv6 Hash Mode: Default
Packet Header Fields:
```

```

IP: ipv4-src-ip    ipv4-dst-ip    ipv4-14-src-port    ipv4-14-dst-port    ipv4-
ip-proto
IPv6: ipv6-src-ip    ipv6-dst-ip    ipv6-14-src-port    ipv6-14-dst-port    ipv6-
next-hdr
RoCE: qpn
Ingress-port: enabled
Hash seed: 100013
Hash offset: flow-based
Hash Algorithm: CRC_32HI

```

Releases

3.1 or later

show ip mroute

Displays IP multicast routes.

Command `show ip mroute [vrf {vrf-name | all}] {{[grp-addr [src-addr]]} | [summary]}`

- Options**
- *vrf-name* — VRF name prefixed by Vrf (up to 15 characters)
 - *all* — (Optional) Display all routes
 - *grp-addr* — (Optional) Group address in A.B.C.D format
 - *src-addr* — (Optional) Source address in A.B.C.D format
 - *summary* — Display summary information

Modes EXEC

Usage None

Examples

```

sonic# show ip mroute
IP Multicast Routing Table for VRF: default
  * -> indicates installed route

      Source        Group        Input        Output        Uptime
* 71.0.0.11    233.0.0.1    Vlan100    Vlan200    00:41:59
* 71.0.0.22    233.0.0.1    Vlan100    Vlan200    00:41:54
                                         Vlan201
* 71.0.0.11    234.0.0.1    Vlan100    Vlan200    00:41:59
* 71.0.0.33    234.0.0.1    Vlan100    Vlan200    00:41:31
                                         Vlan201
* 71.0.0.22    235.0.0.1    Vlan100    Vlan200    00:41:44
* 71.0.0.33    235.0.0.1    Vlan100    Vlan200    00:41:16
                                         Vlan200    00:41:14

```

```

sonic# show ip mroute 233.0.0.1
IP Multicast Routing Table for VRF: default
  * -> indicates installed route

      Source        Group        Input        Output        Uptime
* 71.0.0.11    233.0.0.1    Vlan100    Vlan200    00:41:59
* 71.0.0.22    233.0.0.1    Vlan100    Vlan200    00:41:54
                                         Vlan201    00:41:59

```

```

sonic# show ip mroute 233.0.0.1 71.0.0.22
IP Multicast Routing Table for VRF: default
  * -> indicates installed route

      Source        Group        Input        Output        Uptime
* 71.0.0.22    233.0.0.1    Vlan100    Vlan200    00:41:54
                                         Vlan201    00:41:59

```

```

sonic# show ip mroute vrf Vrf1
IP Multicast Routing Table for VRF: Vrf1
  * -> indicates installed route

```

```

      Source      Group      Input      Output      Uptime
* 51.0.0.11  233.0.0.1  Vlan300   Vlan301   00:41:59
* 51.0.0.22  233.0.0.1  Vlan300   Vlan301   00:41:54
                                         Vlan302   00:41:59

sonic# show ip mroute vrf all
IP Multicast Routing Table for VRF: default
  * -> indicates installed route

      Source      Group      Input      Output      Uptime
* 71.0.0.11  233.0.0.1  Vlan100   Vlan200   00:41:59
* 71.0.0.22  233.0.0.1  Vlan100   Vlan200   00:41:54
                                         Vlan201   00:41:59
* 71.0.0.11  234.0.0.1  Vlan100   Vlan200   00:41:34
* 71.0.0.33  234.0.0.1  Vlan100   Vlan200   00:41:31
                                         Vlan201   00:41:44
* 71.0.0.22  235.0.0.1  Vlan100   Vlan200   00:41:16
* 71.0.0.33  235.0.0.1  Vlan100   Vlan200   00:41:14

IP Multicast Routing Table for VRF: Vrf1
  * -> indicates installed route

      Source      Group      Input      Output      Uptime
* 51.0.0.11  233.0.0.1  Vlan300   Vlan301   00:41:59
* 51.0.0.22  233.0.0.1  Vlan300   Vlan301   00:41:54
                                         Vlan302   00:41:59

sonic# show ip mroute summary
IP Multicast Routing Table summary for VRF: default

Mroute Type      Installed/Total
(S, G)          6/6

```

Releases

3.2 or later

show ip ospf

Displays OSPF global configuration information.

Command

```
show ip ospf [vrf {vrf-name}] {[border-routers] | {[database {{[asbr-summary [lsid] {[adv-router advrouter]} | [self-originate]}]}]} | {[external [lsid] {[adv-router advrouter]} | [self-originate]}]} | [max-age] | {[network [lsid] {[adv-router advrouter]} | [self-originate]}]} | {[nssa-external [lsid] {[adv-router advrouter]} | [self-originate]}]} | {[opaque-area [lsid] {[adv-router advrouter]} | [self-originate]}]} | {[opaque-as [lsid] {[adv-router advrouter]} | [self-originate]}]} | {[opaque-link [lsid] {[adv-router advrouter]} | [self-originate]}]} | {[router [lsid] {[adv-router advrouter]} | [self-originate]}]} | {[self-originate] | {[summary [lsid] {[adv-router advrouter]} | [self-originate]}]}]} | {[interface [traffic] [interfacename]}]} | {[neighbor [neighip] | [all] | [interfacename]} [detail]}]}
```

Options

- *vrf-name* — (Optional) VRF name prefixed by Vrf (up to 15 characters)
- *lsid* — (Optional) LSID in A.B.C.D format
- *advrouter* — (Optional) Advertisement router in A.B.C.D format
- *interfacename* — (Optional) Interface name
- *neighip* — (Optional) Neighbor IP address in A.B.C.D format

Modes**Usage**

Use this command to display global, neighbors, and interface information related to an OSPFv2 router. You can optionally specify VRF on which the router have to be configured. If VRF name is not specified, the command is considered for VRF default.

Examples

```
sonic# show ip ospf
OSPF Routing Process, Router ID: 1.1.1.1
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is enabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 1
time is 92031756
SPF algorithm last executed 1065d4h22m ago
Last SPF duration 0.0s
SPF timer is inactive
LSA minimum interval 5000 msecs
LSA minimum arrival 1000 msecs
Write Multiplier set to 20
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of areas attached to this router: 2
Area ID: 0.0.0.0 (Backbone)
    Number of interfaces in this area: Total: 1 , Active: 1
    Number of fully adjacent neighbors in this area: 1
    Area has no authentication
    SPF algorithm executed 8 times
    Number of LSA 3
    Number of router LSA 2. Checksum Sum 0x40f64b4000000000
    Number of network LSA 1. Checksum Sum 0x40d5adc000000000
    Number of summary LSA 0. Checksum Sum 0x0
    Number of ASBR summary LSA 0. Checksum Sum 0x0
    Number of NSSA LSA 0. Checksum Sum 0x0
    Number of opaque link LSA . Checksum Sum 0x
    Number of opaque area LSA 0. Checksum Sum 0x0
Area ID: 0.0.0.1
    Number of interfaces in this area: Total: 1 , Active: 1
    Number of fully adjacent neighbors in this area: 0
    Area has no authentication
    SPF algorithm executed 1 times
    Number of LSA 2
    Number of router LSA 0. Checksum Sum 0x0
    Number of network LSA 0. Checksum Sum 0x0
    Number of summary LSA 2. Checksum Sum 0x40f1f61000000000
    Number of ASBR summary LSA 0. Checksum Sum 0x0
    Number of NSSA LSA 0. Checksum Sum 0x0
    Number of opaque link LSA . Checksum Sum 0x
    Number of opaque area LSA 0. Checksum Sum 0x0
```

```
sonic# show ip ospf neighbor | no-more
```

Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtL	RqstL	DBsmL
10.59.142.247	1	Full/Backup	37.343s	64.1.1.2	Ethernet64:64.1.1.1	0	0	0

```
sonic# show ip ospf neighbor Ethernet66 | no-more
```

Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtL	RqstL	DBsmL
2.2.2.2	1	Full/Backup	38.245s	64.1.1.2	Ethernet66:64.1.1.1	0	0	0

```
sonic# show ip ospf neighbor detail | no-more
```

```
Neighbor 10.59.142.247, interface address 64.1.1.2
In the area 0.0.0.0 via interface Ethernet64
Neighbor priority is 1, State is Full, 6 state changes
Most recent state change statistics:
    Progressive change 7h3m25s ago
    DR is 64.1.1.1, BDR is 64.1.1.2
    Options 2 *|-|-|-|-|E|-|
    Dead timer due in 30.687s
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission on
    Thread Link State Update Retransmission on
```

```
sonic# show ip ospf neighbor 2.2.2.2 | no-more
```

```
Neighbor 2.2.2.2, interface address 64.1.1.2
In the area 0.0.0.0 via interface Ethernet66
Neighbor priority is 1, State is Full, 5 state changes
Most recent state change statistics:
    Progressive change 0h1m11s ago
    DR is 64.1.1.1, BDR is 64.1.1.2
    Options 2 *|-|-|-|-|E|-|
    Dead timer due in 33.203s
    Database Summary List 0
```

```

Link State Request List 0
Link State Retransmission List 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
Thread Link State Request Retransmission on
Thread Link State Update Retransmission on

Neighbor 2.2.2.2, interface address 65.1.1.2
  In the area 0.0.0.1 via interface Ethernet67
  Neighbor priority is 1, State is Full, 5 state changes
  Most recent state change statistics:
    Progressive change 0h1m10s ago
    DR is 65.1.1.1, BDR is 65.1.1.2
    Options 2 *|-|-|-|-|E|-|
    Dead timer due in 34.590s
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission on
    Thread Link State Update Retransmission on

```

```

sonic# show ip ospf interface | no-more
VRF Name: default
Ethernet64 is up
  ifindex 128, MTU 9100 bytes, BW 25000 Mbit UP,BROADCAST,RUNNING,MULTICAST
  Internet Address 64.1.1.24, Broadcast 64.1.1.255, Area 0.0.0.0
  MTU mismatch detection: enabled
  Router ID 10.59.143.131, Network Type BROADCAST, Cost: 4
  Transmit Delay is 1 sec, State DR, Priority 1
  Backup Designated Router (ID) 10.59.142.247, Interface Address 64.1.1.2
  Saved Network-LSA sequence number 0x8000000f
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 9.023s
  Neighbor Count is 1, Adjacent neighbor count is 1

```

```

sonic# show ip ospf interface Ethernet67 | no-more
VRF Name: default
Ethernet67 is up
  ifindex 926, MTU 9100 bytes, BW 25000 Mbit UP,BROADCAST,RUNNING,MULTICAST
  Internet Address 65.1.1.24, Broadcast 65.1.1.255, Area 0.0.0.1
  MTU mismatch detection: enabled
  Router ID 1.1.1.1, Network Type BROADCAST, Cost: 4
  Transmit Delay is 1 sec, State DR, Priority 1
  Backup Designated Router (ID) 2.2.2.2, Interface Address 65.1.1.2
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 7.957s
  Neighbor Count is 1, Adjacent neighbor count is 1

```

```

sonic# show ip ospf interface traffic | no-more

```

Interface	HELLO Rx/Tx	DB-Desc Rx/Tx	LS-Req Rx/Tx	LS-Update Rx/Tx	LS-Ack Rx/Tx
Ethernet64	2563/2563	3/3	1/1	17/30	29/16

```

sonic# show ip ospf interface traffic Ethernet67 | no-more

```

Interface	HELLO Rx/Tx	DB-Desc Rx/Tx	LS-Req Rx/Tx	LS-Update Rx/Tx	LS-Ack Rx/Tx
Ethernet67	19/22	2/3	1/1	3/3	2/2

```

sonic# show ip ospf database | no-more
VRF Name: default

OSPF Router with ID (10.59.143.131)

  Router Link States (Area 0.0.0.0)

    Link ID      ADV Router      Age  Seq#      CkSum  Link count
    10.59.142.247  10.59.142      1682  0x80000011  0xb56b 1
    10.59.143.131  10.59.143      1498  0x80000011  0xdc2c 1

    Net Link States (Area 0.0.0.0)

```

```
Link ID          ADV Router      Age  Seg#      CkSum
64.1.1.1        10.59.143.131  1538 0x8000000f 0x1c70
```

```
sonic# show ip ospf database router | no-more
VRF Name: default

OSPF Router with ID (10.59.143.131)

Router Link States (Area 0.0.0.0)

LS age: 1709
Options: 0x2 : *|-|-|---|-|E|-
LS Flags: 0x6
Flags: 0x0 :
LS Type: router-LSA
Link State ID: 10.59.142.247
Advertising Router: 10.59.142
LS Seq Number: 80000011
Checksum: 0xb56b
Length: 36

Number of Links: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 64.1.1.1
(Link Data) Router Interface address: 64.1.1.2
Number of TOS metrics: 0
TOS 0 Metric: 4

LS age: 1525
Options: 0x2 : *|-|-|---|-|E|-
LS Flags: 0x3
Flags: 0x0 :
LS Type: router-LSA
Link State ID: 10.59.143.131
Advertising Router: 10.59.143
LS Seq Number: 80000011
Checksum: 0xdc2c
Length: 36

Number of Links: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 64.1.1.1
(Link Data) Router Interface address: 64.1.1.1
Number of TOS metrics: 0
TOS 0 Metric: 4
```

```
sonic# show ip ospf database network | no-more
VRF Name: default
```

```
OSPF Router with ID (10.59.143.131)

Net Link States (Area 0.0.0.0)

LS age: 1602
Options: 0x2 : *|-|-|---|-|E|-
LS Flags: 0x3
LS Type: network-LSA
Link State ID: 64.1.1.1 (address of Designated Router)
Advertising Router: 10.59.143.131
LS Seq Number: 8000000f
Checksum: 0x1c70
Length: 32

Network Mask: /24
Attached Router: 10.59.142.247
Attached Router: 10.59.143.131
```

```
sonic# show ip ospf database summary | no-more
VRF Name: default
```

```
OSPF Router with ID (1.1.1.1)

Summary Link States (Area 0.0.0.0)

LS age: 468
Options: 0x2 : *|-|-|---|-|E|-
LS Flags: 0x11
LS Type: summary-LSA
Link State ID: 65.1.1.0 (summary Network Number)
Advertising Router: 1.1.1.1
```

```

LS Seq Number: 80000001
Checksum: 0x0e04
Length: 28

Network Mask: /24
TOS: 0 Metric: 4

LS age: 429
Options: 0x2 : *|-|-|-|-|-|E|-
LS Flags: 0x6
LS Type: summary-LSA
Link State ID: 65.1.1.0 (summary Network Number)
Advertising Router: 2.2.2.2
LS Seq Number: 80000002
Checksum: 0xed1f
Length: 28

Network Mask: /24
TOS: 0 Metric: 4

Summary Link States (Area 0.0.0.1)

LS age: 468
Options: 0x2 : *|-|-|-|-|-|E|-
LS Flags: 0x11
LS Type: summary-LSA
Link State ID: 64.1.1.0 (summary Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x1bf7
Length: 28

Network Mask: /24
TOS: 0 Metric: 4

LS age: 429
Options: 0x2 : *|-|-|-|-|-|E|-
LS Flags: 0x6
LS Type: summary-LSA
Link State ID: 64.1.1.0 (summary Network Number)
Advertising Router: 2.2.2.2
LS Seq Number: 80000002
Checksum: 0xfa13
Length: 28

Network Mask: /24
TOS: 0 Metric: 4

```

```

sonic# show ip ospf database asbr-summary | no-more
VRF Name: default

        OSPF Router with ID (1.1.1.1)

ASBR-Summary Link States (Area 0.0.0.0)

LS age: 38
Options: 0x2 : *|-|-|-|-|-|E|-
LS Type: summary-LSA
Link State ID: 2.2.2.2 (AS Boundary Router address)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xb41
Length: 28

Network Mask: /0
TOS: 0 Metric: 4

```

```

sonic# show ip ospf database external | no-more
VRF Name: default

        OSPF Router with ID (1.1.1.1)

AS External Link States

LS age: 52
Options: 0x2 : *|-|-|-|-|-|E|-
LS Flags: 0x6
LS Type: AS-external-LSA
Link State ID: 25.1.1.1 (External Network Number)
Advertising Router: 2.2.2.2
LS Seq Number: 80000001
Checksum: 0x0892
Length: 36

```

```

Network Mask: /32
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0

```

```

sonic# show ip ospf database max-age
OSPF Router with ID (1.1.1.1)
    MaxAge Link States:

```

```

sonic# show ip ospf database self-originate | no-more
VRF Name: default

```

```
    OSPF Router with ID (1.1.1.1)
```

```
        Router Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	777	0x80000004	0x7b42	1

```
        Net Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum
64.1.1.1	1.1.1.1	777	0x80000001	0x8581

```
        Summary Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
65.1.1.0	1.1.1.1	816	0x80000001	0xe0e4	65.1.1.0/24

```
        ASBR-Summary Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum
2.2.2.2	1.1.1.1	360	0x80000001	0xb41

```
        Router Link States (Area 0.0.0.1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	776	0x80000004	0x8d2e	1

```
        Net Link States (Area 0.0.0.1)
```

Link ID	ADV Router	Age	Seq#	CkSum
65.1.1.1	1.1.1.1	776	0x80000001	0x788d

```
        Summary Link States (Area 0.0.0.1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
64.1.1.0	1.1.1.1	816	0x80000001	0x1bf7	64.1.1.0/24

```

sonic# show ip ospf database network adv-router 1.1.1.1 | no-more
VRF Name: default

```

```
    OSPF Router with ID (1.1.1.1)
```

```
        Net Link States (Area 0.0.0.0)
```

```

LS age: 886
Options: 0x2 : *|-|-|-|-|-|E|-|
LS Flags: 0x3
LS Type: network-LSA
Link State ID: 64.1.1.1 (address of Designated Router)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x8581
Length: 32

```

```
        Network Mask: /24
Attached Router: 1.1.1.1
```

```
Attached Router: 2.2.2.2
```

```
        Net Link States (Area 0.0.0.1)
```

```

LS age: 886
Options: 0x2 : *|-|-|-|-|-|E|-|
LS Flags: 0x3
LS Type: network-LSA
Link State ID: 65.1.1.1 (address of Designated Router)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x788d
Length: 32

```

```
Network Mask: /24
Attached Router: 1.1.1.1
Attached Router: 2.2.2.2
```

Releases	3.2 or later
-----------------	--------------

show ip ospf graceful-restart helper

Displays OSPF graceful restart helper information.

Command	show ip ospf graceful-restart helper [detail]
Options	detail—(Optional) View detailed OSPF graceful restart helper information.
Modes	EXEC
Usage	None
Examples	

```
sonic# show ip ospf graceful-restart helper
VRF Name: default
OSPF Router with ID (14.14.14.14)
Graceful restart helper support enabled.
Strict LSA check is enabled.
Helper supported for planned restarts only.
Supported Graceful restart interval: 1600(in seconds).
Enable Router List:
['13.13.13.13']

sonic# show ip ospf graceful-restart helper detail
VRF Name: default
OSPF Router with ID (14.14.14.14)
Graceful restart helper support enabled.
Strict LSA check is enabled.
Helper supported for planned restarts only.
Supported Graceful restart interval: 1600(in seconds).
Enable Router List:
['13.13.13.13']
Number of Active neighbours in graceful restart: 4
Neighbour 1:
Address: 192.168.10.1
Routerid: 13.13.13.13
Received Grace period: 250(in seconds).
Actual Grace period: 250(in seconds).
Remaining GraceTime: 245(in seconds).
Graceful Restart reason: Software restart.
Neighbour 2:
Address: 192.168.20.1
Routerid: 13.13.13.13
Received Grace period: 250(in seconds).
Actual Grace period: 250(in seconds).
Remaining GraceTime: 245(in seconds).
Graceful Restart reason: Software restart.
Neighbour 3:
Address: 192.168.30.1
Routerid: 13.13.13.13
Received Grace period: 250(in seconds).
Actual Grace period: 250(in seconds).
Remaining GraceTime: 245(in seconds).
Graceful Restart reason: Software restart.
Neighbour 4:
Address: 192.168.40.1
Routerid: 13.13.13.13
Received Grace period: 250(in seconds).
Actual Grace period: 250(in seconds).
Remaining GraceTime: 245(in seconds).
Graceful Restart reason: Software restart.

sonic# show ip ospf graceful-restart helper detail
```

```

VRF Name: default
OSPF Router with ID (1.1.1.2)
Graceful restart helper support enabled.
Strict LSA check is enabled.
Helper supported for Planned and Unplanned Restarts.
Supported Graceful restart interval: 1800(in seconds).
Last Helper exit Reason: Successful graceful restart

```

Releases 4.1.0 or later

show ip ospf neighbor detail

Displays the OSPF neighbor information.

Command show ip ospf neighbour detail

Options None

Modes EXEC

Usage Use this command to view the OSPF neighbor information and details about graceful restart helper.

Example

```

sonic# show ip ospf neighbor detail
Neighbor 13.13.13.13, interface address 192.168.10.1
    In the area 0.0.0 via interface Ethernet64
    Neighbor priority is 1, State is Full, 6 state changes
    Most recent state change statistics:
        Progressive change 17h32m19s ago
    DR is 192.168.10.1, BDR is 192.168.10.2
    Options 66 *|0|-|-|-|E|-|
    Dead timer due in 0.717s
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission on
    Thread Link State Update Retransmission on
    Graceful restart Helper info:
        Graceful Restart HELPER Status: Inprogress
        Graceful Restart grace period time: 250 (seconds).
        Graceful Restart reason: Software restart

```

Releases 4.1.0 or later

show ip ospf route

Displays OSPF routing table configuration information.

Command show ip ospf route

Options None

Modes EXEC

Usage Use this command to display OSPF routes in an OSPFv2 router. You can optionally specify the VRF on which the router needs to be configured. If the VRF name is not specified, the command is considered for the VRF default.

Example

```

sonic# show ip ospf vrf Vrf1 route | no-more
VRF Name: Vrf1
===== OSPF network routing table =====
N      101.1.1.0/24          [10] area: 0.0.0.0
                                         directly attached to Vlan101

```

```
===== OSPF router routing table =====
===== OSPF external routing table =====
```

Releases 3.1 or later

show ip pim

Displays PIM information.

Command show ip pim [vrf {vrf-name | all}] {[interface [ifName] [detail] [traffic]] | [multicast] [neighbor [nbr-addr]] | [rpf] | [ssm] | [topology [grp-addr] [src-addr]] }

Options

- *vrf-name*—(Optional) Enter the name of the VRF prefixed by Vrf (up to 15 characters)
- *ifName*—(Optional) Enter the interface name (ranges)
- *nbr-addr*—(Optional) Enter the neighbor address in A.B.C.D format.
- *grp-addr*—(Optional) Enter the group address in A.B.C.D format.
- *src-addr*—(Optional) Enter the source address in A.B.C.D format.
- *interface*—Display information about PIM interfaces.
- *neighbor*—Display information about PIM neighbor.
- *rpf*—Display information about current S,G and their RPF lookup information.
- *ssm*—Displays SSM group ranges.
- *topology*—Displays PIM interface topology information.
- *multicast*—Displays multicast information, route statistics, packet statistics, and timers used.

Modes EXEC

Usage Use this command to check PIM information.

Examples

```
sonic# show ip pim interface
PIM interface information for VRF: default
Interface      State       Address        PIM Nbrs      PIM DR      Hello-interval      PIM
DR-Priority
Vlan100        up         100.0.0.2     1           100.0.0.2    30          1
Vlan200        up         200.0.0.2     1           200.0.0.3    30          1

sonic # show ip pim interface vlan 100
PIM interface information for VRF: default
Interface      State       Address        PIM Nbrs      PIM DR      Hello-interval      PIM
DR-Priority
Vlan100        up         100.0.0.2     1           100.0.0.2    30          1

sonic# show ip pim neighbor
PIM neighbor information for VRF: default
Interface      Neighbor      Uptime      Expirytime      DR-Priority
Vlan100        100.0.0.1    01:38:52    00:01:22      1
Vlan200        200.0.0.3    01:22:33    00:01:13      1

sonic# show ip pim neighbor 100.0.0.1
PIM neighbor information for VRF: default
Interface      Neighbor      Uptime      Expirytime      DR-Priority
Vlan100        100.0.0.1    01:38:52    00:01:22      1

sonic# show ip pim ssm
PIM SSM information for VRF: default
SSM group range : PIM_PLIST1

sonic# show ip pim ssm
```

```

PIM SSM information for VRF: default
SSM group range : 232.0.0.0/8

sonic# show ip pim topology

PIM multicast routing table for VRF: default
(71.0.0.11, 233.0.0.1), uptime 13:08:24, expires 00:00:12
  Incoming interface: vlan100, RPF neighbor 100.0.0.1
  Outgoing interface list:
    vlan200  uptime/expiry-time: 13:07:50/00:01:39
    vlan122  uptime/expiry-time: 12:33:21/Never

(71.0.0.22, 233.0.0.1), uptime 13:08:45, expires 00:00:18
  Incoming interface: vlan100, RPF neighbor 100.0.0.1
  Outgoing interface list:
    vlan200  uptime/expiry-time: 13:22:52/00:01:45
    vlan124  uptime/expiry-time: 12:42:28/Never

(101.0.0.22, 225.1.1.1), uptime 13:07:51, expires 00:06:09
  Incoming interface: vlan105, RPF neighbor 105.0.0.1
  Outgoing interface list:
    vlan200  uptime/expiry-time: 13:03:50/00:01:39
    vlan123  uptime/expiry-time: 13:02:40/Never

```

```

sonic# show ip pim topology 233.0.0.1

PIM multicast routing table for VRF: default
(71.0.0.11, 233.0.0.1), uptime 13:08:24, expires 00:00:12
  Incoming interface: vlan100, RPF neighbor 100.0.0.1
  Outgoing interface list:
    vlan200  uptime/expiry-time: 13:07:50/00:01:39
    vlan122  uptime/expiry-time: 12:33:21/Never

(71.0.0.22, 233.0.0.1), uptime 13:08:45, expires 00:00:18
  Incoming interface: vlan100, RPF neighbor 100.0.0.1
  Outgoing interface list:
    vlan200  uptime/expiry-time: 13:22:52/00:01:45
    vlan124  uptime/expiry-time: 12:42:28/Never

```

```

sonic# show ip pim topology 225.1.1.1 101.0.0.22

PIM multicast routing table for VRF: default
(101.0.0.22, 225.1.1.1), uptime 13:07:51, expires 00:06:09
  Incoming interface: vlan105, RPF neighbor 105.0.0.1
  Outgoing interface list:
    vlan200  uptime/expiry-time: 13:03:50/00:01:39
    vlan123  uptime/expiry-time: 13:02:40/Never

```

```

sonic# show ip pim rpf

PIM RPF information for VRF: default
Source      Group        RpfIface     RpfAddress      RibNextHop      Metric      Pref
71.0.0.11   233.0.0.1   Vlan100      100.0.0.1      100.0.0.1      0           1
71.0.0.22   235.0.0.1   Vlan100      100.0.0.1      100.0.0.1      0           1

```

```

sonic# show ip pim multicast | no-more

PIM multicast information for VRF: default
VRF Name :default
Router MLAG Role :NONE

Total Multicast Routes In VRF :0
Total Dynamic Multicast Routes In VRF :0
Total Dynamic Uninstalled Multicast Routes In VRF :0
Total Static Multicast Routes In VRF :0
Total Static Uninstalled Multicast Routes In VRF :0
Total Static Failed Multicast Routes In VRF :0
Total Uninstalled Multicast Routes In VRF :0
Total Multicast Routes In VRF :0

Total Dynamic Multicast Routes Across All VRFs :0
Total Dynamic Uninstalled Multicast Routes Across All VRFs :0
Total Static Multicast Routes Across All VRFs :0
Total Static Uninstalled Multicast Routes Across All VRFs :0
Total Uninstalled Multicast Routes Across All VRFs :0
Total Multicast Routes Across All VRFs :0

Upstream Join Timer in secs :60

```

```

JoinPrune Holdtime in secs :
PIM ECMP :Disable
PIM ECMP Rebalance :Disable

rpfCacheRefreshDelayMsecs :50
rpfCacheRefreshTimer :0
rpfCacheRefreshRequests :0
rpfCacheRefreshEvents :0
rpfCacheRefreshLast :---:---
nexthopLookups :0
nexthopLookupsAvoided :0

Multicast Count:
-----
Interface      State     Address      ifIndex      Vif      PktsIn
PktsOut      BytesIn   BytesOut
Ethernet1       up        1.1.1.1      30          1          0          0
          0          0
pimreg         up        0.0.0.0      71          0          0          0
          0          0

```



```

sonic# show ip pim interface traffic
PIM interface traffic information for VRF: default
Interface           HELLO          JOIN          PRUNE          REGISTER
REGISTER-STOP      ASSERT         BSM
                    Rx/Tx          Rx/Tx          Rx/Tx          Rx/Tx
Rx/Tx              Rx/Tx          Rx/Tx
-----
```

Interface	HELLO	JOIN	PRUNE	REGISTER
REGISTER-STOP	ASSERT	BSM	Rx/Tx	Rx/Tx
Rx/Tx	Rx/Tx	Rx/Tx	Rx/Tx	Rx/Tx
Ethernet32	8981/20486	0/0	0/0	0/0
0/0	0/0	0/0	0/0	0/0
Ethernet33	20490/20490	0/0	0/0	0/0
0/0	0/0	0/0	0/0	0/0
Ethernet34	20487/20488	0/0	0/0	0/0
0/0	0/0	0/0	0/0	0/0
Ethernet35	20486/20487	0/0	0/0	0/0
0/0	0/0	0/0	0/0	0/0

Releases 3.2 or later

show ip prefix-list

Displays IPv4 prefix-list configuration information.

Command show ip prefix-list [*list-name*]

Options *list-name*—(Optional) Prefix-list name

Modes EXEC

Usage Use this command to display IPv4 prefix-list configuration information.

Examples

```

sonic# show ip prefix-list
IP prefix list test:
    seq 1 permit 1.1.1.1/32
sonic# show ip prefix-list test
IP prefix list test:
    seq 1 permit 1.1.1.1/32

```

```

sonic# show ip prefix-list prflst657
IP prefix list prflst657:
    permit 157.1.1.0/24

```

Releases 3.0 or later

show ip rest

Displays the settings that are used in REST API authentication.

Command	show ip rest [cipher-suite]
Options	None
Modes	EXEC
Usage	To display the settings for REST API authentication, use the ip rest command.
Example	<pre>sonic# show ip rest Log level is 0 Port is 443 Request limit is not-set Read timeout is 15 seconds Client authentication mode is password,jwt Security profile is not-set API timeout is 900 seconds Cipher suite is ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with- chacha20- poly1305-SHA256</pre>

Releases	4.1.0 or later
-----------------	----------------

show ip rest authentication

Displays REST authentication modes.

Command	show ip rest authentication
Options	None
Modes	EXEC
Usage	Use this command to display the currently enabled authentication modes for the REST API.
Example	<pre>sonic# show ip rest authentication Client authentication mode is password,jwt</pre>

Releases	4.1.0 or later
-----------------	----------------

show ip rest cipher-suite

Displays the configured REST server cipher suites.

Command	show ip rest cipher-suite
Options	None
Modes	EXEC
Usage	To configure the REST server cipher suite with the cryptographic algorithms used for secure communication between the REST server running in an Enterprise SONiC switch and REST clients that are external to the switch, use the ip rest cipher-suite command. To display the settings for REST API authentication, use the ip rest command.
Example	<pre>sonic# show ip rest cipher-suite Cipher suite is ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-</pre>

```
chacha20-
poly1305-SHA256
```

Releases

4.4.1 or later

show ip route

Displays information about IPv4 routing table entries.

Command `show ip route [vrf {all summary | vrfname} | address | prefix | bgp | connected | nexthop-group | ospf | static | summary]`

Options

- *vrfname*—(Optional) Name of the VRF to view information.
- *address*—(Optional) Prefix in A.B.C.D format.
- *prefix*—(Optional) Prefix in A.B.C.D/mask format.
- *nexthop-group*—(Optional) Next-hop group information.
- *connected*—Displays the connected routes.
- *bgp*—Displays only BGP routes.
- *ospf*—Displays only OSPF routes.
- *static*—Displays only static routes.
- *summary*—Displays number of routes present.

Modes

EXEC

Usage

Use this command to view information about IPv4 routing table entries.

Example

```
sonic# show ip route
Codes: K - kernel route, C - connected, S - static, B - BGP, O - OSPF
      > - selected route, * - FIB route, q - queued route,
      r - rejected route, # - not installed in hardware
      Destination      Gateway                      Dist/Metric  Last Update
-----
S>* 20.20.20.0/24  via 10.10.10.12    Ethernet52  1/0          00:00:07 ago
K>* 0.0.0.0/0      via 100.94.192.254 Management0  0/202        00:00:07 ago
O>* 11.0.0.0/28    via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.16/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.32/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.48/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.64/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.80/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.96/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.112/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.128/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.144/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.160/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.176/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.192/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.208/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.224/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.0.240/28  via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.1.0/28    via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.1.16/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
O>* 11.0.1.32/28   via 99.201.0.10   Ethernet60   110/3        00:01:07 ago
--more--

sonic# show ip route summary
Route Source      Routes          FIB   (vrf default)
connected          1               1
ebgp              71              71
ibgp              2               2
-----
Totals             74              74
```

Releases

3.2 or later

show ip sla

Displays IP SLA instance information.

Command show ip sla [*sla-id* [history | detail]]

- Options**
- *sla-id*—(Optional) SLA ID.
 - *history*—(Optional) Display history.
 - *detail*—Display detailed information.

Modes EXEC

Usage Use this command to display IP SLA summary information of all instances on a system. You can also display IP SLA detailed information for a specific instance or history information of a particular instance.

Examples

```
sonic# show ip sla
SLA# Type State Target VRF Transitions Last change
---- -- -- -----
10 ICMP-echo Up 30.30.1.2 default 1 00:06:41 ago
20 TCP-connect Up 40.40.1.2(100) default 1 00:05:40 ago
```

```
sonic# show ip sla 10
IP SLA Operation Number: 10
Type of Operation: ICMP-echo
ICMP destination IP address: 30.30.1.2
ICMP source IP address: 30.30.1.1
ICMP source interface:
ICMP request data size: 32
ICMP Time-To-Live(TTL): 0
ICMP Type-of-Service(ToS): 0
Source VRF: default
Operation frequency (sec): 30
Operation timeout (sec): 5
Operation threshold: 3
Operation state: Up
Operation state transitions: 1
Operation last state change: 00:08:39 ago
ICMP Echo Request counter: 107
ICMP Echo Reply counter: 107
ICMP Error counter: 0
ICMP Invalid responses: 0
```

```
sonic# show ip sla 20
Type of Operation: TCP-connect
TCP destination IP address: 40.40.1.2
TCP destination port: 100
TCP source IP address: 40.40.1.1
TCP source port: 200
TCP source interface:
TCP Time-To-Live(TTL): 0
TCP Type-of-Service(ToS): 0
Source VRF: default
Operation frequency (sec): 30
Operation timeout (sec): 3
Operation threshold: 3
Operation state: Up
Operation state transitions: 1
Operation last state change: 00:28:59 ago
TCP connect request counter: 58
TCP connect success counter: 58
TCP connect error counter: 0
```

```
sonic# show ip sla 20 history
Timestamp Event
-----
Sat Jun 20 10:27:27 2020 Started
Sat Jun 20 10:27:27 2020 Pkt send error(Network is unreachable)
Sat Jun 20 10:29:25 2020 State changed to: Up
```

Releases 3.1 or later

show ip static-anycast-gateway

Displays IPv4 static Anycast gateway information.

Command	show ip static-anycast-gateway		
Options	None		
Modes	EXEC		
Usage	Use this command to display IPv4 static anycast address, VRF, and admin operation status.		
Example	<pre>sonic# show ip static-anycast-gateway Configured Anycast Gateway MAC address: 00:00:00:01:02:03 Router MAC for Forwarding : No IPv4 Anycast Gateway MAC address: enable Total number of gateway: 1024 Total number of gateway admin UP: 1024 Total number of gateway oper UP: 1024 Interfaces Gateway Address Vrf Admin/Oper ----- ----- ----- Vlan1 172.16.0.254/24 Vrf001 up/up Vlan2 172.16.1.254/24 Vrf001 up/up Vlan3 172.16.2.254/24 Vrf001 up/up Vlan4 172.16.3.254/24 Vrf001 up/up Vlan5 172.16.4.254/24 Vrf001 up/up Vlan6 172.16.5.254/24 Vrf001 up/up Vlan7 172.16.6.254/24 Vrf001 up/up Vlan8 172.16.7.254/24 Vrf001 up/up Vlan9 172.16.8.254/24 Vrf001 up/up Vlan10 172.16.9.254/24 Vrf001 up/up</pre>		
Releases	3.0 or later		

show ip telemetry

Displays the settings that are used in client authentication for telemetry services, including gNMI.

Command	show ip telemetry {api-timeout authentication jwt-refresh jwt-valid log-level port security-profile vrf}		
Options	None		
Modes	EXEC		
Usage	To configure the settings for gNMI authentication, use the ip telemetry command.		
Example	<pre>sonic# show ip telemetry Log level is 0 JWT valid is 3600 seconds JWT refresh is 900 seconds Port is 8080 Client authentication mode is password,jwt Security profile is not-set</pre>		

```
API timeout is 0 seconds
vrf is not-set

sonic# show ip telemetry api-timeout
API timeout is 0 seconds

sonic# show ip telemetry authentication
Client authentication mode is password,jwt

sonic# show ip telemetry jwt-refresh
JWT refresh is 900 seconds

sonic# show ip telemetry jwt-valid
JWT valid is 3600 seconds

sonic# show ip telemetry log-level
Log level is 0

sonic# show ip telemetry port
Port is 8080

sonic# show ip telemetry vrf
vrf is mgmt
```

Releases

4.1.0 or later

show ip vrf

Display all VRF instance information, or for a specific VRF instance.

Command`show ip vrf [vrf-name | mgmt]`**Options**

vrf-name—(Optional) VRF name (up to 15 characters)

Modes

EXEC

Usage

Use this command to view the VRFs configured on the switch and the interfaces mapped to the VRFs.

Examples

```
sonic# show ip vrf
VRF-NAME           INTERFACES
-----
mgmt              Management0
Vrf_red           Ethernet16
                      Ethernet8
```

```
sonic# show ip vrf Vrf_red
VRF-NAME           INTERFACES
-----
Vrf_red           Ethernet16
                      Ethernet8
```

```
sonic# show ip vrf mgmt
VRF-NAME           INTERFACES
```

mgmt	Management0
Releases	3.0 or later

show ipv6 access-group

Displays IPv6 access-group information.

Command	show ipv6 access-group
Options	None
Modes	EXEC
Usage	Use this command to view the configuration information for both ingress and egress IPv6 access groups.
Example	<pre>sonic# show ipv6 access-group Ingress IPV6 access-list ipv6acl-example on Ethernet0</pre>

Releases	3.1 or later
-----------------	--------------

show ipv6 access-lists

Displays IPv6 access lists information.

Command	show ipv6 access-lists [access-list-name {{[interface { Ethernet PortChannel Vlan eth-sub-if-id po-sub-if-id}] } [Switch]}}]
Options	<ul style="list-style-type: none"> • <i>access-list-name</i> — (Optional) ACL name (up to 63 characters) • <i>interface</i> — (Optional) Displays ACLs by interface • <i>PortChannel</i> — (Optional) Port channel ID (1 to 128) • <i>Vlan</i> — (Optional) VLAN ID (1 to 4094) • <i>eth-sub-if-id</i> — (Optional) Ethernet subinterface ID • <i>po-sub-if-id</i> — (Optional) PortChannel subinterface ID • <i>switch</i> — (Optional) Switch
Modes	EXEC
Usage	ACL name and interface names are optional. If ACL name is not specified, all IPv6 ACLs display. ACL statistics are shown only if the ACL is applied globally or to any interface.
Example	<pre>sonic# show ipv6 access-lists ipv6 access-list ipv6acl-example seq 100 permit ipv6 host abcd::1 host bcde::1 (0 packets) [0 bytes] seq 200 permit tcp host abcd::2 host bcde::2 (0 packets) [0 bytes] seq 300 permit udp host abcd::3 host bcde::3 (0 packets) [0 bytes]</pre>

Releases	3.2 or later
-----------------	--------------

show ipv6 dhcp snooping

Displays DHCP snooping IPv6 global information.

Command	show ipv6 dhcp snooping
Options	None
Modes	EXEC

Usage

Use this command to check whether DHCP snooping is enabled or disabled, identify the VLANs it is configured on, and which ports are marked as Trusted. It also displays any dynamic VLANs where DHCP snooping is automatically enabled when showing the VLANs.

Examples

```
sonic# show ipv6 dhcp snooping
DHCP snooping is Enabled
DHCP snooping source MAC verification is Enabled
DHCP snooping is enabled on the following VLANs: 100
DHCP snooping trusted interfaces: Ethernet10
```

Releases

4.0 or later

show ipv6 dhcp snooping binding

Displays the IPv6 DHCP snooping binding database.

Command show ipv6 dhcp snooping binding

Options None

Modes EXEC

Usage Use this command to view the IPv6 DHCP snooping binding database.

Examples

```
sonic# show ipv6 dhcp snooping binding
Total number of Dynamic bindings: 0
Total number of Static bindings: 1
Total number of Tentative bindings: 0
MAC address           IP Address     VLAN      Interface      Type
Lease (Secs)
-----
---  
00:00:00:00:00:01   10.1.1.1       100       Ethernet15    Static      NA
```

Releases

4.0 or later

show ipv6 dhcp snooping statistics

Displays the IPv6 DHCP snooping statistics.

Command show ipv6 dhcp snooping statistics

Options None

Modes EXEC

Usage Use this command to view the DHCP snooping packet validation statistics.

Examples

```
sonic# show ipv6 dhcp snooping statistics
      Interface  MAC Verify  Client Ifc      DHCP Server
                  Failures  Mismatch      Msgs Recvd
-----
-----  
Ethernet0      0          0            0
Ethernet1      0          0            0
```

Releases

4.0 or later

show ipv6 dhcp snooping statistics detail

Displays the IPv6 DHCP snooping detailed statistics.

Command show ipv6 dhcp snooping statistics detail

Options None

Modes EXEC

Usage Use this command to view the DHCP snooping detailed statistics.

Examples

```
sonic# show ipv6 dhcp snooping statistics detail
DHCPv6 Snooping Detailed Statistics
-----
Error receiving from DHCP snooping socket : 0
DHCP message too big : 0
Illegal source IP address in snooped packet : 0
Illegal source MAC in snooped packet : 0
Error sending from DHCP snooping socket : 0
Number of DHCP messages intercepted : 0
Number of DHCP messages processed : 0
Number of DHCP messages filtered : 0
Number of DHCP messages forwarded : 0
Rx RELEASE or DECLINE from client not in bindings db : 0
Number of bindings added to bindings table : 0
Number of bindings removed from bindings table : 0
MAC verification failures/server frames recv'd on untrusted ports : 0
Number of DHCP messages dropped as static binding exists : 0
Packets dropped due to no outgoing interface or interface down : 0
```

Releases 4.0 or later

show ipv6 dhcp-relay

Displays IPv6 DHCP relay information.

Command show ipv6 dhcp-relay {[brief] | {[detailed {[intfName1] | [pchName1] | [vlanName1]}]} | {[statistics {[intfName] | [pchName] | [vlanName]}]}}

Options

- *intfName1* — (Optional) Displays detailed information on all interfaces or for a specific interface
- *pchName1* — (Optional) Displays statistical information on all PortChannels or for a specific PortChannel
- *vlanName1* — (Optional) Displays statistical information on all VLANs or for a specific VLAN
- *intfName* — (Optional) Displays statistical information for a specific interface
- *pchName* — (Optional) Displays statistical information for a specific PortChannel
- *vlanName* — (Optional) Displays statistical information for a specific VLAN

Modes EXEC

Usage Use this command to display DHCPv6 statistics, relay configuration, or relay statistics for a given interface. If the interface name is not specified, this command displays information for all interfaces enabled for DHCP relay. If the given interface is not enabled for DHCP relay, this command returns an error message. If the source interface is not configured, the command output displays as *Not Configured*.

Examples

```
sonic# show ipv6 dhcp-relay brief
-----
Interface      DHCP Helper Address
-----
Ethernet0      300::1
Ethernet0      400::1
Ethernet0      500::1
```

```
sonic# show ipv6 dhcp-relay detailed Vlan100
Relay Interface: Vlan100
Server Address: 2000::2
```

```

Server VRF: VrfRed
Source Interface: Not Configured
VRF Select: enable
Max Hop Count: 10

```

```

sonic# show ipv6 dhcp-relay statistics Vlan100
DHCPv6 SOLICIT messages received by the relay agent: 1
DHCPv6 ADVERTISEMENT messages sent by the relay agent: 1
DHCPv6 REQUEST messages received by the relay agent: 1
DHCPv6 REPLY messages sent by the relay agent: 1
DHCPv6 CONFIRM messages received by the relay agent: 0
DHCPv6 RELEASE messages received by the relay agent: 0
DHCPv6 DECLINE messages received by the relay agent: 0
DHCPv6 REBIND messages received by the relay agent: 0
DHCPv6 RECONFIGURE messages sent by the relay agent: 0
DHCPv6 INFO-REQUEST messages received by the relay agent: 0
DHCPv6 RELAY-REPLY messages received by the relay agent: 2
DHCPv6 RELAY-FORWARD messages sent by the relay agent: 2
Total number of DHCPv6 packets dropped by the relay agent: 0
Number of DHCPv6 packets dropped due to an invalid opcode: 0
Number of DHCPv6 packets dropped due to an invalid option: 0
Packets relayed from server to client: 2
Errors relaying packets from servers: 0
Errors relaying packets from clients: 0
Packets with wrong message type dropped on downstream interface: 0
Packets with wrong message type dropped on upstream interface: 0
DHCPv6 RENEW packets received from client: 0
DHCPv6 LEASE-QUERY packets received from client: 0
DHCPv6 DHCPV4-QUERY packets received from client: 0
DHCPv6 INFORM-REQUEST packets received from downstream: 0
DHCPv6 LEASE QUERY packets sent to client: 0
DHCPv6 DHCPV4 RESPONSE packets sent to client: 0
Packets dropped on exceeding the max hop count: 0
DHCPv6 ADVERTISE packets sent to client on other downstream interface: 0
DHCPv6 REPLY packets sent to client on other downstream interface: 0
DHCPv6 RECONFIGURE packets sent to client on other downstream interface: 0
DHCPv6 LEASE QUERY packets sent to client on other downstream interface: 0
DHCPv6 DHCPV4 RESPONSE packets sent to client on other downstream interface: 0

```

Releases

3.2 or later

show ipv6 interfaces

Displays IPv6 configuration information for all interfaces.

Command show ipv6 interfaces

Options None

Modes EXEC

Usage Use this command to display all interfaces that are configured with an IPv6 address.

Example

```

sonic# show ipv6 interfaces

leaf1# show ipv6 interfaces
Flags: U-Unnumbered interface, A-Anycast IP
-----
Interface      IP address/mask          VRF        Admin/Oper   Flags
Management0    fe80::2a0:c9ff:fe0:0/64 mgmt       up/up
Ethernet10     fe80::2a0:c9ff:fe00:2/64
Ethernet64     fe80::2a0:c9ff:fe00:2/64
PortChannel11  fe80::2a0:c9ff:fe00:2/64
PortChannel21  fe80::2a0:c9ff:fe00:2/64
Vlan3001       fe80::2a0:c9ff:fe00:2/64 Vrf001     up/up
Vlan3002       fe80::2a0:c9ff:fe00:2/64 Vrf002     up/up
Vlan3003       fe80::2a0:c9ff:fe00:2/64 Vrf003     up/up
Vlan3004       fe80::2a0:c9ff:fe00:2/64 Vrf004     up/up
Vlan3005       fe80::2a0:c9ff:fe00:2/64 Vrf005     up/up
Vlan3006       fe80::2a0:c9ff:fe00:2/64 Vrf006     up/up
Vlan3007       fe80::2a0:c9ff:fe00:2/64 Vrf007     up/up
Vlan3008       fe80::2a0:c9ff:fe00:2/64 Vrf008     up/up
Vlan3009       fe80::2a0:c9ff:fe00:2/64 Vrf009     up/up
Vlan3010       fe80::2a0:c9ff:fe00:2/64 Vrf010     up/up

```

Vlan3011	fe80::2a0:c9ff:fe00:2/64	Vrf011	up/up	
Vlan3012	fe80::2a0:c9ff:fe00:2/64	Vrf012	up/up	
Vlan3013	fe80::2a0:c9ff:fe00:2/64	Vrf013	up/up	
Vlan3014	fe80::2a0:c9ff:fe00:2/64	Vrf014	up/up	
Vlan3015	fe80::2a0:c9ff:fe00:2/64	Vrf015	up/up	
Vlan1	2001:172:16:0::254/64	Vrf001	up/up	A
Vlan2	2001:172:16:1::254/64	Vrf001	up/up	A
Vlan3	2001:172:16:2::254/64	Vrf001	up/up	A
Vlan4	2001:172:16:3::254/64	Vrf001	up/up	A
Vlan5	2001:172:16:4::254/64	Vrf001	up/up	A
Vlan6	2001:172:16:5::254/64	Vrf001	up/up	A
Vlan7	2001:172:16:6::254/64	Vrf001	up/up	A
Vlan8	2001:172:16:7::254/64	Vrf001	up/up	A
Vlan9	2001:172:16:8::254/64	Vrf001	up/up	A
Vlan10	2001:172:16:9::254/64	Vrf001	up/up	A
Vlan11	2001:172:16:a::254/64	Vrf001	up/up	A
Vlan12	2001:172:16:b::254/64	Vrf001	up/up	A

Releases

3.0 or later

show ipv6 nd ra-interfaces

Displays the IPv6 neighbor discovery configuration on all interfaces.

Command show ipv6 nd ra-interfaces [Ethslot/port | Vlan *vlan-id* | PortChannel *portchannel-number*]

Options None

Modes EXEC

Usage Use this command to verify the configuration of neighbor discovery (ND) router advertisements on Ethernet, routed VLAN, port channel interfaces and on subinterfaces.

Examples

```
sonic# show ipv6 nd ra-interfaces
Interfaces:
  Vlan100
    ND advertised reachable time is 0 milliseconds
    ND advertised retransmit interval is 0 milliseconds
    ND advertised hop-count limit is 64 hops
    ND router advertisements sent: 0 rcvd: 0
    ND router advertisements are sent every 600 seconds
    ND router advertisements lifetime tracks ra-interval
    ND router advertisement default router preference is MEDIUM
    Hosts use stateless autoconfig for addresses.
    ND router advertisements with Adv. Interval option.
    Advertised Link MTU is 1200
    rdnss 2001::1 1234
    rdnss 2002::1 infinite
    rdnss 2003::1
    dnssl mybroadcom1 1234
    dnssl mybroadcom2
    dnssl mybroadcom3 infinite
    prefix 2001::1/128 5000 4000
    prefix 2002::1/128 no-autoconfig off-link
  Vlan200
    ND advertised reachable time is 0 milliseconds
    ND advertised retransmit interval is 0 milliseconds
    ND advertised hop-count limit is 64 hops
    ND router advertisements sent: 0 rcvd: 0
    ND router advertisements are sent every 600 seconds
    ND router advertisements lifetime tracks ra-interval
    ND router advertisement default router preference is MEDIUM
    Hosts use stateless autoconfig for addresses.
    Ethernet64
    ND advertised reachable time is 0 milliseconds
    ND advertised retransmit interval is 0 milliseconds
    ND advertised hop-count limit is 64 hops
```

```

ND router advertisements sent: 0 rcvd: 0
ND router advertisements are sent every 1234 milliseconds
ND router advertisements lifetime tracks ra-interval
ND router advertisement default router preference is MEDIUM
Hosts use stateless autoconfig for addresses.
Advertised Link MTU is 900
rdnss 2001::1 infinite
    PortChannel15
        ND advertised reachable time is 0 milliseconds
        ND advertised retransmit interval is 0 milliseconds
        ND advertised hop-count limit is 64 hops
        ND router advertisements sent: 0 rcvd: 0
        ND router advertisements are sent every 600 seconds
        ND router advertisements lifetime tracks ra-interval
        ND router advertisement default router preference is MEDIUM
        Hosts use stateless autoconfig for addresses.
    Ethernet64.12
        ND advertised reachable time is 0 milliseconds
        ND advertised retransmit interval is 0 milliseconds
        ND advertised hop-count limit is 64 hops
        ND router advertisements sent: 0 rcvd: 0
        ND router advertisements are sent every 600 seconds
        ND router advertisements lifetime tracks ra-interval
        ND router advertisement default router preference is MEDIUM
        Hosts use stateless autoconfig for addresses.
    PortChannel15.20
        ND advertised reachable time is 0 milliseconds
        ND advertised retransmit interval is 0 milliseconds
        ND advertised hop-count limit is 64 hops
        ND router advertisements sent: 0 rcvd: 0
        ND router advertisements are sent every 600 seconds
        ND router advertisements lifetime tracks ra-interval
        ND router advertisement default router preference is MEDIUM
        Hosts use stateless autoconfig for addresses.
...

```

Releases

4.0.3 or later

show ipv6 neighbors

Displays IPv6 discovery information.

Command

```
show ipv6 neighbors [vrf {vrfname | mgmt | all}] {[ip-addr] | {[mac-address mac-addr]} | [summary]}
```

Options

- *vrfname* — (Optional) VRF name prefixed by Vrf
- *ip-addr* — (Optional) IPv6 address in A::B format
- *mac-addr* — (Optional) IPv6 address in nn:nn:nn:nn:nn:nn format

Modes

EXEC

Usage

Use this command to display NDP table entries. To filter the output, specify an interface, port channel, or VLAN, an IPv6 address, a MAC address, or a combination of more than one value to match. You can also display total number of ARP entries using the *summary* option.

Examples

```

sonic# show ipv6 neighbors
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address          Hardware address      Interface      Egress Interface  Type   Action
-----
20::1            00:01:02:03:44:55  Ethernet8       -           Dynamic   Fwd
20::2            00:01:02:03:ab:cd  PortChannel1200 -           Dynamic   Fwd
20::3            00:01:02:03:04:05  Vlan100        Ethernet4     Dynamic   Fwd
fe80::e6f0:4ff:fe79:34c7 00:01:e8:8b:44:71  Management0 -           Dynamic   Fwd

```

```

sonic# show ipv6 neighbors Vlan 100
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address          Hardware address      Interface      Egress Interface  Type   Action

```

```

20::3          00:01:02:03:04:05  Vlan100    Ethernet4      Dynamic Fwd

sonic# show ipv6 neighbors interface Management 0
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address           Hardware address   Interface   Egress Interface Type Action
-----
fe80::e6f0:4ff:fe79:34c7 00:01:e8:8b:44:71  Management0 -           Dynamic Fwd

sonic# show ipv6 neighbors 20::2
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address           Hardware address   Interface   Egress Interface Type Action
-----
20::2            00:01:02:03:ab:cd  PortChannel1200 -           Dynamic Fwd

sonic# show ipv6 neighbors mac-address 00:01:02:03:04:05
Type: R - Remote Neighbor entries (EVPN or MLAG Separate IP)
-----
Address           Hardware address   Interface   Egress Interface Type Action
-----
20::3            00:01:02:03:04:05  Vlan100    Ethernet4      Dynamic Fwd

```

Releases 3.1 or later

show ipv6 neighbors interface

Displays IPv6 neighbor interface configuration information.

Command	<code>show ipv6 neighbors interface {{[phy-if-name [summary]]} {[subif-name [summary]]} {Loopback {lo-id [summary]}} {Management {mgmt-if-id [summary]}} {PortChannel {lag-id [summary]}} {Vlan {vlan-id [summary]}} {Vxlan {vxlan-if-name [summary]}}}</code>
Options	<ul style="list-style-type: none"> • <i>phy-if-name</i>—Ethernet ID (1 to 65535) • <i>subif-name</i>—Subinterface ID (1 to 65535) • <i>lo-id</i>—Loopback ID (0 to 16383) • <i>mgmt-if-id</i>—Management interface ID (0) • <i>lag-id</i>—PortChannel ID (1 to 128) • <i>vlan-id</i>—VLAN ID (1 to 4094) • <i>vxlan-if-id</i>—VXLAN ID
Modes	EXEC
Usage	Use this command to view a summary of IPv6 neighbor interface entries or the entries for a specific interface.

Example

```

sonic# show ipv6 neighbors interface Management 0
-----
Address           Hardware address   Interface   Egress Interface
-----
fe80::e6f0:4ff:fe79:34c7  e4:f0:04:79:34:c7  Management0 -
```

Releases 3.2 or later

show ipv6 prefix-list

Displays IPv6 prefix-list configuration information.

Command	<code>show ipv6 prefix-list [list-name]</code>
Options	<i>prefix-list list-name</i> —(Optional) Prefix-list name
Modes	EXEC

Usage

Use this command to display IPv6 prefix-list configuration information.

Examples

```
sonic# show ipv6 prefix-list
IPv6 prefix list prflst758:
    permit 1758:5523::/64 ge 67 le 68
IPv6 prefix list prflst759:
    permit 1759:5567::/64

sonic# show ipv6 prefix-list prflst758
IPv6 prefix list prflst758:
    permit 1758:5523::/64 ge 67 le 68
```

Releases

3.0 or later

show ipv6 route

Displays information about IPv6 BGP routing table entries.

Command

```
show ipv6 route [vrf {all summary | vrfname} | address | prefix | bgp | connected | nexthop-group | static | summary]
```

Options

- *vrf vrfname*—(Optional) Name of the VRF to view information that is exchanged between BGP neighbors corresponding to that VRF.
- *address*—(Optional) IP address in A::B format.
- *prefix*—(Optional) Route prefix in A::B/mask format.
- *nexthop-group*—(Optional) Next-hop group information.

Modes

EXEC

Usage

Use this command to view information about all IPv6 BGP routing table entries, or for a specific prefix.

Example

```
sonic# show ipv6 route static
Codes: K - kernel route, C - connected, S - static, B - BGP, O - OSPF
      > - selected route, * - FIB route, q - queued route, r -
      rejected route,
      # - not installed in hardware
      Destination      Gateway                      Dist/Metric  Last Update
-----
S# 2001:db5::/32  Direct          Ethernet8        1/0          00:05:57 ago
S# 3020::/64      via 7070::7070  Ethernet0        1/0          00:00:41 ago
S# 3030::3300/120 via 3030::3301  Ethernet12       36/0         00:06:44 ago

sonic# show ipv6 route vrf mgmt static
Codes: K - kernel route, C - connected, S - static, B - BGP, O - OSPF
      > - selected route, * - FIB route, q - queued route, r - rejected route,
      # - not installed in hardware
      Destination      Gateway                      Dist/Metric  Last Update
-----
S  2001:db5::/32  Direct          Ethernet64        1/0          00:01:26 ago
S  2001:db8::/32  via 3030::3302  Vlan100(vrf Vrf-common) 200/0        00:01:38 ago
```

Releases

3.2 or later

show ipv6 static-anycast-gateway

Displays IPv6 static Anycast gateway configuration information.

Command

```
show ipv6 static-anycast-gateway
```

Options

None

Modes

EXEC

Usage

Use this command to display IPv6 static anycast address, VRF, and admin operation status.

Example

```
sonic# show ipv6 static-anycast-gateway
Configured Anycast Gateway MAC address: 00:00:00:01:02:03
Router MAC for Forwarding : No
IPv6 Anycast Gateway MAC address: enable
Total number of gateway: 1024
Total number of gateway admin UP: 1024
Total number of gateway oper UP: 1024
Interfaces          Gateway Address      Vrf      Admin/Oper
-----
Vlan1              2001:172:16:0::254/64  Vrf001    up/up
Vlan2              2001:172:16:1::254/64  Vrf001    up/up
Vlan3              2001:172:16:2::254/64  Vrf001    up/up
Vlan4              2001:172:16:3::254/64  Vrf001    up/up
Vlan5              2001:172:16:4::254/64  Vrf001    up/up
Vlan6              2001:172:16:5::254/64  Vrf001    up/up
Vlan7              2001:172:16:6::254/64  Vrf001    up/up
Vlan8              2001:172:16:7::254/64  Vrf001    up/up
Vlan9              2001:172:16:8::254/64  Vrf001    up/up
Vlan10             2001:172:16:9::254/64  Vrf001    up/up
Vlan11             2001:172:16:a::254/64  Vrf001    up/up
Vlan12             2001:172:16:b::254/64  Vrf001    up/up
Vlan13             2001:172:16:c::254/64  Vrf001    up/up
Vlan14             2001:172:16:d::254/64  Vrf001    up/up
Vlan15             2001:172:16:e::254/64  Vrf001    up/up
Vlan16             2001:172:16:f::254/64  Vrf001    up/up
```

Releases

3.0 or later

show kdump files

Displays the kernel core dump files which are stored locally.

Command

show kdump files

Options

None

Modes

EXEC

Usage

Use this command to view the kernel core dump files which are stored locally after a kernel crash.

Example

```
sonic# show kdump files
Record Key           Filename
-----
1 202002101809 /var/crash/202002101809/dmesg.202002101809
                  /var/crash/202002101809/kdump.202002101809
```

Releases

3.0 or later

show kdump log

Displays kernel core dump log from a locally stored file.

Command

show kdump log record [lines]

Options

- *record*—Enter the record number.
- *lines*—(Optional) Enter the number of lines to retrieve from the kernel log file; the default is 20.

Modes

EXEC

Usage

The mandatory parameter is the record number of the kernel core dump file which is stored locally. The optional parameter is the number of lines displayed (20 is the default number of lines to view).

Example

```
sonic# show kdump log 1 5
File: /var/crash/202002101809/dmesg.202002101809
```

```
[326785.222049]  [<fffffffffa0c0484e>] ?
entry_SYSCALL_64_after_swapgs+0x58/0xc6
[326785.229926]  Code: 41 5c 41 5d 41 5e 41 5f e9 6c 2f cf ff 66 2e 0f 1f
84 00 00 00 00 00 66 90 0f 1f 44 00 00 c7 05 29 28 a8 00 01 00 00 00 0f
ae f8 <c6> 04 25 00 00 00 00 01 c3 0f 1f 44 00 00 0f 1f 44 00 00 53 8d
[326785.251451] RIP  [<fffffffffa0a2a562>] sysrq_handle_crash+0x12/0x20
[326785.258463] RSP <fffffafd2c6523e78>
[326785.262453] CR2: 0000000000000000
```

Releases 3.0 or later

show kdump memory

Displays the amount of memory that is reserved for kernel core dump.

Command show kdump memory

Options None

Modes EXEC

Usage Use this command to view the amount of memory that is reserved by default for kernel crash dump files depending on the RAM size.

Example

```
sonic# show kdump memory
Memory Reserved: 0M-2G:256M, 2G-4G:256M, 4G-8G:384M, 8G-:448M
Memory Allocated: 448M
```

Releases 3.0 or later

show kdump num-dumps

Displays the maximum number of kernel core dump files that can be stored locally.

Command show kdump num-dumps

Options None

Modes EXEC

Usage Use this command to view the maximum number of kernel core dump files that can be stored locally.

Example

```
sonic# show kdump num-dumps
Maximum number of Kernel Core files Stored: 3
```

Releases 3.0 or later

show kdump status

Displays kernel core dump status information.

Command show kdump status

Options None

Modes EXEC

Usage Use this command to view whether the kdump feature is configured. You can also use it to verify the amount of memory that is reserved and allocated, the maximum number of kernel core files that can be stored, and the core dump files.

Examples

```
sonic# show kdump status
Kdump Administrative Mode: Enabled
Kdump Operational State: Ready
Memory Reserved: 512M
Maximum number of Kernel Core files Stored: 3
Record Key           Filename
-----
1 202002101809 /var/crash/202002101809/dmesg.202002101809
                  /var/crash/202002101809/kdump.202002101809
```

Releases

3.0 or later

show ldap-server

Displays LDAP server information.

Command show ldap-server

Options None

Modes EXEC

Usage Use this command to view the LDAP server configuration details.

Example

```
sonic# show ldap-server
-----
LDAP Global Configuration
-----
base          : dc=force10networks,dc=com
bind-dn       : cn=System Directory Manager
bindpw configured : Yes
vrf-name      : mgmt
-----
LDAP NSS Configuration
-----
bindpw configured : No
-----
LDAP PAM Configuration
-----
bindpw configured : No
-----
LDAP SUDO Configuration
-----
bindpw configured : No
source-interface : Management0
-----
HOST          USE-TYPE   PORT     PRIORITY SSL      RETRY
-----
100.104.100.219 -         -        -          ON       -
-----
LDAP Maps
-----
ATTRIBUTE:
  member          : uniqueMember
CUSTOM SONIC ROLES ATTRIBUTE VALUE:
  admin          : sonicAdminGroup
  netadmin       : sonicNetAdminGroup
  operator       : sonicOperatorGroup
  secadmin       : sonicSecAdminGroup
```

Releases

3.1 or later

show link state tracking

Displays link state tracking configuration information.

Command	show link state tracking [<i>grp-name</i>]
Options	<i>grp-name</i> — (Optional) Group name (up to 63 characters)
Modes	EXEC
Usage	Link state tracking group name can be of maximum 63 characters. The name must begin with A-Z, a-z or 0-9. Underscore and hyphens can be used except as the first character. If the group name is not specified then a summary of all configured groups display.

Example	<pre>sonic# show link state tracking FooBar Name: FooBar Description: Example description Timeout: 120 seconds Upstream Interfaces: Ethernet0 (Up) Ethernet4 (Up) Vlan100 (Up) Downstream Interfaces: PortChannel1 (Up) PortChannel2 (Up) Ethernet4 (Up)</pre>
Releases	3.0 or later

show lldp neighbor

Displays LLDP neighbor configuration information.

Command	show lldp neighbor [<i>ifname</i>]
Options	<i>ifname</i> —(Optional) Specify the interface name.
Modes	EXEC
Usage	Use this command to view the detailed information about the LLDP neighbor.

Example	<pre>sonic# show lldp neighbor Interface: Ethernet48,via: LLDP Chassis: ChassisID: 3c:2c:30:6d:72:80 SysName: 10025 SysDescr: SONiC Software TTL: 120 MgmtIP: 100.104.78.100 MgmtIP: fe80::3e2c:30ff:fe6d:7280 Capability: ROUTER, ON Port PortID: Ethernet48 PortDescr: Eth1/13 PortVlanID: 10 LLDP-MED Device Type: Network Connectivity Device Capability: Capabilities, yes Capability: Ext_mdi_power_pd, yes Capability: Inventory, yes Capability: Network_policy, yes Inventory Hardware Rev: 3.40.0.9-10 Software Rev: 5.10.0-8-2-amd64 Firmware Rev: 3.40.0.9-10 Serial Number: CN01WJVTCES0094Q0015 Manufacturer: Dell EMC Model: S5232F-ON</pre>
Releases	3.0 or later

show lldp statistics

Displays LLDP statistics information.

Command show lldp statistics [*ifname*]

Options *ifname*—(Optional) Enter the interface name.

Modes EXEC

Usage Use this command to view the LLDP packet statistics for all the interfaces.

Examples

```
sonic# show lldp statistics
LLDP Statistics
-----
Interface: Ethernet0
    Transmitted      : 10
    Received        : 12
    Discarded       : 1
    Unrecognized TLV : 0
    Ageout          : 0
-----
```

Releases 3.2 or later

show lldp table

Displays brief LLDP neighbor configuration information.

Command show lldp table

Options None

Modes EXEC

Usage Use this command to view the local port and remote device information.

Example

```
sonic# show lldp table
-----
LocalPort   RemoteDevice  RemotePortID   Capability   RemotePortDescr
-----
Ethernet80  AG2          Ethernet12     R           Eth1/4
Ethernet84  AG2          Ethernet16     R           Eth1/5
Ethernet88  AG2          Ethernet20     R           Eth1/6
Ethernet92  AG1          Ethernet0      R           Eth1/1/1
Ethernet96  AG1          Ethernet8       R           Eth1/2/1
Ethernet100 AG1          Ethernet16     R           Eth1/3/1
```

Releases 3.0 or later

show locator-led chassis

Displays the locator LED state.

Command show locator-led chassis

Options None

Modes EXEC

Usage This command displays the state and color of the chassis LED. Chassis locator LED color is platform-specific. The output of color can vary depending on the system states. Also, if the system cannot retrieve the locator LED color, it displays the color as unknown.

Examples

When the locator LED is on, the output for this command displays:

```
sonic# show locator-led chassis  
  
State      Color  
-----  -----  
on        blue_blink
```

When the locator LED is off, the output for this command displays:

```
sonic# show locator-led chassis  
  
State      Color  
-----  -----  
off        off
```

```
sonic# show locator-led chassis  
  
State      Color  
-----  -----  
off        unknown
```

Releases

3.2 or later

show logging

Displays logging information.

Command

```
sonic# show logging [count | lines [number] | servers | filter {level level  
| since date-time | type log-type}]
```

Options

- **count** - Displays the number of logged messages.
- **lines [number]** - Enter the number of lines to display. The range is from 1-65535.
- **servers** - View the configured system log servers.
- **filter {level level | since date-time | type message-type}** - Filter the displayed logs using a specified and higher severity levels, a date and time in the format *month day hh:mm:ss*, or a message type.

Modes

EXEC

Usage

Use this command to view the messages that are stored in the system log.

Example

```
sonic# show logging  
May 11 16:43:07.853550 2021 sonic NOTICE admin: Running sonic-clear  
logging  
May 16 02:13:53.107861 2021 sonic ERR pidof[30142]: can't get program  
name from /proc/30123/stat  
May 17 13:24:44.587237 2021 sonic WARNING snmp#snmp-subagent  
[sonic_ax_impl] WARNING: Missing lldp_loc_man_addr from APPL DB  
May 18 09:48:59.883892 2021 sonic ERR pidof[12624]: can't get program  
name from /proc/12611/stat  
May 20 12:42:07.712024 2021 sonic NOTICE root: hello
```

```
sonic# show logging | grep portchannel  
May 21 17:14:20.885341 2021 sonic NOTICE teamd#teammgrd: :-  
setLagAdminStatus: Received admin status PortChannel1 for portchannel up.
```

```
sonic# show logging lines 3  
May 17 13:24:44.587237 2021 sonic WARNING snmp#snmp-subagent  
[sonic_ax_impl] WARNING: Missing lldp_loc_man_addr from APPL DB  
May 18 09:48:59.883892 2021 sonic ERR pidof[12624]: can't get program  
name from /proc/12611/stat  
May 20 12:42:07.712024 2021 sonic NOTICE root: hello
```

Releases 3.1 or later

show logging count

Displays the total number of messages in the system log.

Command show logging count

Options None

Command mode EXEC

Usage Use this command to view the total number of messages in the system log.

Example

```
sonic# show logging count  
19805
```

Releases 3.1 or later

show logging filter

Displays log based on the given filters.

Command show logging filter {level log-level {since date-time} | severity severity-level {since date-time} | since date-time {level log-level | severity severity-level} | type {syslog filter {level log-level {since date-time} | severity severity-level {since date-time} | since date-time {level filter-level | severity severity-level} | inmem filter {level log-level {since date-time} | severity severity-level {since date-time} | since date-time {level filter-level | severity severity-level} | all filter {level log-level {since date-time} | severity severity-level {since date-time} | since date-time {level log-level | severity severity-level}}}}

- Options**
- severity <severity-level>—Logs in a given severity
 - type syslog—Syslogs
 - type inmem—In-memory logs
 - type all —All logs
 - level *log-level*—Logs in a given severity and higher
 - since *since-date*—Logs since a given date or time

Modes EXEC

Usage The log levels are DEBUG, INFO, WARNING, NOTICE, ERR, and CRIT.

Examples

```
sonic# show logging filter since 2/1  
Feb 01 02:00:46.640058+02:00 2022 sonic WARNING system#monitor: :-  
operator():  
Key 'SYSTEM_READY|SYSTEM_STATE' field 'Status' unavailable in database  
'STATE_DB'  
Feb 01 02:00:46.641385+02:00 2022 sonic WARNING system#monitor: :-  
operator():  
Key 'SYSTEM_READY_ALL|SYSTEM_STATE' field 'Status' unavailable in  
database 'STATE_DB'  
Feb 01 02:05:46.745125+02:00 2022 sonic WARNING system#monitor: :-  
operator():  
Key 'SYSTEM_READY|SYSTEM_STATE' field 'Status' unavailable in database  
'STATE_DB'  
Feb 01 02:05:46.745592+02:00 2022 sonic WARNING system#monitor: :-  
operator():  
Key 'SYSTEM_READY_ALL|SYSTEM_STATE' field 'Status' unavailable in  
database 'STATE_DB'  
Feb 01 02:10:46.843736+02:00 2022 sonic WARNING system#monitor: :-  
operator():
```

```

Key 'SYSTEM_READY|SYSTEM_STATE' field 'Status' unavailable in database
'STATE_DB'
Feb 01 02:10:46.8444807+02:00 2022 sonic WARNING system#monitor: :-
operator():
Key 'SYSTEM_READY_ALL|SYSTEM_STATE' field 'Status' unavailable in
database 'STATE_DB'
Feb 01 02:15:46.946450+02:00 2022 sonic WARNING system#monitor: :-
operator():
Key 'SYSTEM_READY|SYSTEM_STATE' field 'Status' unavailable in database
'STATE_DB'
Feb 01 02:15:46.947171+02:00 2022 sonic WARNING system#monitor: :-
operator():
Key 'SYSTEM_READY_ALL|SYSTEM_STATE' field 'Status' unavailable in
database 'STATE_DB'
Feb 01 02:20:47.048853+02:00 2022 sonic WARNING system#monitor: :-
operator():
Key 'SYSTEM_READY|SYSTEM_STATE' field 'Status' unavailable in database
'STATE_DB'
Feb 01 02:20:47.050342+02:00 2022 sonic WARNING system#monitor: :-
operator():
Key 'SYSTEM_READY_ALL|SYSTEM_STATE' field 'Status' unavailable in
database 'STATE_DB'
Feb 01 02:25:47.150017+02:00 2022 sonic WARNING system#monitor: :-
operator():
Key 'SYSTEM_READY|SYSTEM_STATE' field 'Status' unavailable in database
'STATE_DB'
Feb 01 02:25:47.151793+02:00 2022 sonic WARNING system#monitor: :-
operator():
Key 'SYSTEM_READY_ALL|SYSTEM_STATE' field 'Status' unavailable in
database 'STATE_DB'

```

Releases

4.0 or later

show logging lines

Displays the output of the last number of lines.

Command show logging lines [*lines*]

Options *lines*—(Optional) Specify the number of lines.

Modes EXEC

Usage Use this command to view only the specified number of lines from the recent logs.

Examples

```

sonic# show logging lines 3
Dec 2 23:54:44.315479 2020 st-sjc-<platform>-26 INFO dhclient[3114]: DHCPREQUEST of 100.94.192.17 on
Management0 to 100.94.192.82 port 67
Dec 2 23:54:44.355747 2020 st-sjc-<platform>-26 INFO dhclient[3114]: DHCPCPACK of 100.94.192.17 from
100.94.192.82
Dec 2 23:54:45.689359 2020 st-sjc-<platform>-26 INFO dhclient[3114]: bound to 100.94.192.17 --
renewal in 241 seconds.

```

Releases

3.1 or later

show logging servers

Displays a list of configured remote syslog servers.

Command show logging servers

Options None

Modes EXEC

Usage Use this command to view the detailed information of the list of configured remote syslog servers.

Example

```
sonic# show logging servers
-----
HOST          PORT   SOURCE-INTERFACE  VRF      MESSAGE-TYPE    SEVERITY    PROTOCOL
-----
100.94.196.9  514    Management0       mgmt    log           notice     udp
```

Releases

3.1 or later

show mab

Displays a summary of the global MAB configuration and summary information of the MAB configuration for all ports.

Command

show mab

Options

None

Modes

EXEC

Usage

This command is used to show a summary of the global MAB configuration and summary information of the MAB configuration for all ports. This command also provides the detailed MAB sessions for a specified port.

Examples

```
sonic# show mab

MAB Request Fmt Attr1 Groupsize ..... 2
MAB Request Fmt Attr1 Separator..... legacy(:)
MAB Request Fmt Attr1 Case..... uppercase

Interface Admin Mode Auth-type
-----
Eth1      Disabled   N/A
Eth2      Disabled   N/A
Eth3      Disabled   N/A
```

Releases

4.0 or later

show mab interface

Displays MAB information of the client interface.

Command

show mab [interface Ethernet port]

Options

port—Specify the physical interface ID.

Modes

EXEC

Usage

Use this command to view MAB information of the host-connected interface.

Examples

```
sonic# show mab interface Eth1/10
Interface Admin Mode Auth-type
-----
Eth1/10   Enabled    eap-md5
```

Releases

4.0 or later

show mac access-group

Displays MAC ACL binding summary.

Command

show mac access-group

Options

None

Modes

EXEC

Usage

Use this command to view the MAC access-lists applied on interfaces.

Example

```
sonic# show mac access-group  
Ingress MAC access-list macacl-example on Vlan100
```

Releases

3.1 or later

show mac access-lists

Displays MAC access-lists information.

Command

```
show mac access-lists [access-list-name {{{interface {Ethernet |  
PortChannel | Vlan | eth-sub-if-id | po-sub-if-id}} | [Switch]}}]
```

Options

- *access-list-name* — (Optional) ACL name (up to 63 characters)
- *interface* — Displays ACL information on interfaces
- *PortChannel* — Port channel ID (1 to 128)
- *Vlan* — VLAN ID (1 to 4094)
- *eth-sub-if-id* — Ethernet subinterface ID
- *po-sub-if-id* — PortChannel subinterface ID

Modes

EXEC

Usage

ACL name and interface names are optional. If ACL name is not specified, all MAC ACLs display. ACL statistics are shown only if the ACL is applied globally or to any interface.

Example

```
sonic# show mac access-lists  
mac access-list macacl-example  
      seq 10 permit host 00:00:10:00:00:01 host 00:00:20:00:00:01 (10 packets) [1000 bytes]  
      seq 20 permit host 00:00:10:00:00:02 host 00:00:20:00:00:02 (20 packets) [2000 bytes]  
      seq 30 permit host 00:00:10:00:00:03 host 00:00:20:00:00:03 (30 packets) [3000 bytes]  
      seq 40 permit host 00:00:10:00:00:04 host 00:00:20:00:00:04 (40 packets) [4000 bytes]
```

Releases

3.2 or later

show mac address-table

Displays all MAC address-table configuration information.

Command

```
show mac address-table
```

Options

None

Modes

EXEC

Usage

Use this command to view the MAC address-table configuration information.

Example

```
sonic# show mac address-table  
-----  
VLAN      MAC-ADDRESS        TYPE      INTERFACE  
-----  
10        00:00:00:00:00:01  STATIC    Ethernet0  
11        00:00:00:00:00:01  STATIC    Ethernet0  
100       00:00:00:00:00:10  DYNAMIC   Ethernet36  
20        00:00:00:00:00:02  DYNAMIC   Ethernet4  
30        00:00:00:00:00:03  STATIC    Ethernet8  
40        00:00:00:00:00:04  DYNAMIC   Ethernet12  
50        00:00:00:00:00:05  STATIC    Ethernet16  
60        00:00:00:00:00:06  DYNAMIC   Ethernet20  
70        00:00:00:00:00:07  STATIC    Ethernet24
```

80	00:00:00:00:00:08	DYNAMIC	Ethernet28
90	00:00:00:00:00:09	STATIC	Ethernet32
10	00:00:00:00:00:98	STATIC	Ethernet0
99	00:00:00:00:00:99	STATIC	PortChannel10

Releases 3.0 or later

show mac address-table address

Displays address-table configuration information for a specific MAC address.

Command show mac address-table address *mac-addr*

Options *mac-addr*—Specify the MAC address in the nn:nn:nn:nn:nn:nn format.

Modes EXEC

Usage Use this command to view the address-table configuration information for a specific MAC address.

Example

```
sonic# show mac address-table address 00:00:00:00:00:01
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
10        00:00:00:00:00:01  STATIC    Ethernet0
11        00:00:00:00:00:01  STATIC    Ethernet0
```

Releases 3.0 or later

show mac address-table aging-time

Displays MAC address-table aging-time configuration information.

Command show mac address-table aging-time

Options None

Modes EXEC

Usage Use this command to view the MAC address-table aging-time configuration information.

Example

```
sonic# show mac address-table aging-time
Global aging time: 600 seconds
```

Releases 3.0 or later

show mac address-table count

Displays address-table count information.

Command show mac address-table count

Options None

Modes EXEC

Usage Use this command to view MAC address-table count information.

Example

```
sonic# show mac address-table count
MAC Entries for all vlans : 13
Dynamic Address Count : 5
```

```

Static Address (User-defined) Count : 8
Total MAC Addresses in Use: 13

```

Releases 3.0 or later

show mac address-table dynamic

Displays address-table information for dynamic MAC addresses.

Command `show mac address-table dynamic {{[address] mac-addr} | {[Vlan]} | {[interface] {{Ethernet phy-if-id} | {PortChannel port-channel-id}}}}`

Options

- *mac-addr*—Specify the MAC address in the nn:nn:nn:nn:nn:nn format.
- *phy-if-id*—Specify the physical interface ID (0 to 255).
- *port-channel-id*—Specify the PortChannel ID (1 to 128).

Modes EXEC

Usage Use this command to view the dynamic MAC address-table for specific address or any specific interface.

Examples

```

sonic# show mac address-table dynamic
-----
VLAN      MAC-ADDRESS        TYPE      INTERFACE
-----
1         00:1a:01:00:00:0a   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:01   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:02   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:03   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:04   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:05   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:06   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:07   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:08   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:1a:01:00:00:09   DYNAMIC   VxLAN    DIP: 7.7.7.7
1         00:44:0c:0b:0a:01   DYNAMIC   VxLAN    DIP: 5.5.5.5
1         00:44:0c:0b:0a:02   DYNAMIC   VxLAN    DIP: 5.5.5.5
1         00:44:0c:0b:0a:03   DYNAMIC   VxLAN    DIP: 5.5.5.5
1         00:44:0c:0b:0a:04   DYNAMIC   VxLAN    DIP: 5.5.5.5
1         00:44:0c:0b:0a:05   DYNAMIC   VxLAN    DIP: 5.5.5.5
1         00:44:a1:11:00:01   DYNAMIC   Ethernet0

```

```

sonic# show mac address-table dynamic address 00:00:00:00:00:06
-----
VLAN      MAC-ADDRESS        TYPE      INTERFACE
-----
60        00:00:00:00:00:06   DYNAMIC   Ethernet20

```

```

sonic# show mac address-table dynamic Vlan 60
-----
VLAN      MAC-ADDRESS        TYPE      INTERFACE
-----
60        00:00:00:00:00:06   DYNAMIC   Ethernet20

```

```

sonic# show mac address-table dynamic interface Ethernet 12
-----
VLAN      MAC-ADDRESS        TYPE      INTERFACE
-----
40        00:00:00:00:00:04   DYNAMIC   Ethernet12

```

```

sonic# show mac address-table dynamic interface PortChannel 11
-----
VLAN      MAC-ADDRESS        TYPE      INTERFACE
-----
98        00:00:00:00:00:95   DYNAMIC   PortChannel11

```

Releases

3.0 or later

show mac address-table interface

Displays MAC address-table information for Ethernet and PortChannel interfaces.

Command

```
show mac address-table interface {phy-if-name | PortChannel}
```

Options

- *phy-if-id*—Specify the physical interface ID (0 to 255)
- *PortChannel*—Specify the PortChannel ID (1 to 128)

Modes

EXEC

Usage

Use this command to view the MAC address for any specified interfaces.

Examples

```
sonic# show mac address-table interface Ethernet 0
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
1          00:44:a1:11:00:01  DYNAMIC   Ethernet0
2          00:44:a1:12:00:01  DYNAMIC   Ethernet0
3          00:44:a1:11:00:02  DYNAMIC   Ethernet0
4          00:44:a1:12:00:02  DYNAMIC   Ethernet0
5          00:44:a1:11:00:03  DYNAMIC   Ethernet0

sonic# show mac address-table interface PortChannel 10
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
99        00:00:00:00:00:99  STATIC    PortChannel10
```

Releases

3.2 or later

show mac address-table static

Displays address-table information for static MAC addresses.

Command

```
show mac address-table static {{[address mac-addr] | [Vlan] | {[interface
{phy-if-name | PortChannel}]}}}
```

Options

- *mac-addr*—Specify the MAC address in the nn:nn:nn:nn:nn:nn format
- *phy-if-id*—Specify the physical interface ID (0 to 255)
- *port-channel*—Specify the PortChannel ID (1 to 128)

Modes

EXEC

Usage

Use this command to view the static MAC address-table for specific address or any specific interface.

Examples

```
sonic# show mac address-table static
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
10        00:00:00:00:00:01  STATIC    Ethernet0
11        00:00:00:00:00:01  STATIC    Ethernet0
30        00:00:00:00:00:03  STATIC    Ethernet8
50        00:00:00:00:00:05  STATIC    Ethernet16
70        00:00:00:00:00:07  STATIC    Ethernet24
90        00:00:00:00:00:09  STATIC    Ethernet32
```

```

10      00:00:00:00:00:98  STATIC      Ethernet0
99      00:00:00:00:00:99  STATIC      PortChannel10

sonic# show mac address-table static address 00:00:00:00:00:01
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
10      00:00:00:00:00:01  STATIC      Ethernet0
11      00:00:00:00:00:01  STATIC      Ethernet0

show mac address-table static Vlan 11
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
11      00:00:00:00:00:01  STATIC      Ethernet0

sonic# show mac address-table static interface Ethernet 8
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
30      00:00:00:00:00:03  STATIC      Ethernet8

sonic# show mac address-table static interface PortChannel 10
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
99      00:00:00:00:00:99  STATIC      PortChannel10

```

Releases 3.2 or later

show mac address-table Vlan

Displays the MAC address-table for a specific VLAN.

Command show mac address-table Vlan *vlan-id*

Options *vlan-id*—Specify the VLAN ID (1 to 4094)

Modes EXEC

Usage Use this command to view the MAC address-table for any specific VLAN.

Example

```

sonic# show mac address-table Vlan 1
-----
VLAN      MAC-ADDRESS      TYPE      INTERFACE
-----
1      00:1a:01:00:00:0a  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:01  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:02  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:03  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:04  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:05  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:06  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:07  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:08  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:1a:01:00:00:09  DYNAMIC    VxLAN DIP: 7.7.7.7
1      00:44:0c:0b:0a:01  DYNAMIC    VxLAN DIP: 5.5.5.5
1      00:44:0c:0b:0a:02  DYNAMIC    VxLAN DIP: 5.5.5.5
1      00:44:0c:0b:0a:03  DYNAMIC    VxLAN DIP: 5.5.5.5
1      00:44:0c:0b:0a:04  DYNAMIC    VxLAN DIP: 5.5.5.5
1      00:44:0c:0b:0a:05  DYNAMIC    VxLAN DIP: 5.5.5.5
1      00:44:a1:11:00:01  DYNAMIC    Ethernet0

```

Releases 3.0 or later

show mac dampening

Displays the MAC dampening configuration.

Command show mac dampening

Options None

Modes EXEC

Usage Use this command to view the MAC dampening threshold and interval configuration.

Example

```
sonic# show mac dampening
MAC Move Dampening Threshold : 5
MAC Move Dampening Interval  : 5
```

Releases 3.1 or later

show mac dampening-disabled-ports

Displays the MAC dampening-disabled-ports configuration.

Command show mac dampening-disabled-ports

Options None

Modes EXEC

Usage Use this command to view the list of disabled ports due to MAC dampening.

Example

```
sonic# show mac dampening-disabled-ports

Ports disabled due to MAC Dampening:

Ethernet22
Ethernet23
```

Releases 3.1 or later

show mclag brief

Displays MCLAG domain and interface information.

Command show mclag brief

Options None

Modes EXEC

Usage Use this command to view the MCLAG configuration and the interface state.

Example

```
sonic# show mclag brief

Domain ID          : 1
Role               : active
Session Status     : up
Peer Link Status   :
Source Address    : 100.104.78.38
Peer Address       : 100.104.78.39
Session Vrf        : mgmt
Peer Link          : Eth1/13
Keepalive Interval : 1 secs
Session Timeout    : 30 secs
Delay Restore      : 300 secs
```

```

System Mac          : 3c:2c:30:85:db:04
Mclag System Mac   : 00:01:01:01:01:01

Number of MLAG Interfaces:1
-----
MLAG Interface      Local/Remote Status
-----
PortChannel10        up/up

```

Releases 3.0 or later

show mclag mac remote

Displays MCLAG remote MAC information.

Command show mclag mac remote [[count] | [Ethernet port] [PortChannel ID] [Vlan *vlan-id*]]

- Options**
- *count*—(Optional) Displays MCLAG remote mac count
 - *port*—(Optional) Physical interface details
 - *ID*—(Optional) PortChannel interface details (1 to 256)
 - *vlan-id*—(Optional) VLAN ID (1 to 4094)

Modes EXEC

Usage Use this command to view the MCLAG remote MAC information.

Examples

```

sonic# show mclag mac remote
=====
  Vlan      Mac           Port      Type
=====
  Vlan1    24:01:00:1a:00:0a  PortChannel100 dynamic
  Vlan1    24:01:00:1a:00:0b  PortChannel100 dynamic
  Vlan1    24:01:00:1a:00:0c  PortChannel100 dynamic
  Vlan1    24:01:00:1a:00:0d  PortChannel100 dynamic
  Vlan1    24:01:00:1a:00:0e  PortChannel100 dynamic
  Vlan1    24:01:00:1a:00:0f  PortChannel100 dynamic
Total count : 6

```

Releases 4.1.0 or later

show mclag interface

Displays MCLAG interface information.

Command show mclag interface *ifid domain_id*

- Options**
- *ifid*—Specify the MCLAG interface ID.
 - *domain-id*—Specify the MCLAG domain ID.

Modes EXEC

Usage Use this command to view the MCLAG local and remote status.

Example

```

sonic# show mclag interface 10 100
Local/Remote Status  : down/down
TrafficDisable       : No
IsolateWithPeerLink  : No

```

Releases 3.0 or later

show mclag peer-gateway-interfaces

Displays the VLAN interfaces on which the MCLAG peer gateway is configured.

Command show mclag peer-gateway-interfaces

Options None

Modes EXEC

Usage Use this command to view the list of VLAN interfaces on which the MCLAG peer gateway is configured.

Examples

```
sonic-cl# show mclag peer-gateway-interfaces
Interface Name
=====
Vlan10
=====
Total count : 1
=====
```

Releases 4.0 or later

show mclag separate-ip-interfaces

Displays VLAN interfaces that MCLAG separate IP address is configured on.

Command show mclag separate-ip-interfaces

Options None

Modes EXEC

Usage Use this command to view the list of VLAN interfaces on which MCLAG separate IP address is configured on.

Example

```
sonic# show mclag separate-ip-interfaces
Interface Name
=====
Vlan10
=====
Total count : 1
=====
```

Releases 3.1 or later

show mirror-session

Displays configured mirror-session information.

Command show mirror-session [session-name]

Options mirror-session session-name—(Optional) Specify the session name

Modes EXEC

Usage Use this command to view all configured mirror-sessions (ERSPAN and SPAN) information.

Example

```
sonic# show mirror-session
ERSPAN Sessions
-----
Name Status SRC-IP DST-IP GRE DSCP TTL Queue Policer SRC-Port Direction
-----
Mirror2 active 11.1.1.1 10.1.1.1 0x88ee 10 10 10
SPAN Sessions
```

Name	Status	DST-Port	SRC-Port	Direction
Mirror1	active	Ethernet0	Ethernet4	rx

Releases

3.0 or later

show nat

Displays network address translation information.

Command show nat {{translations [count]} | statistics | {config {[static] | [pool] | [bindings] | [globalvalues] | [zones]]}}}

Options

- translations—NAT translation
- statistics—NAT statistics
- config—NAT configuration
- bindings—NAT static bindings
- globalvalues—NAT static globals
- pool—NAT pool configuration
- static—NAT static configuration
- zones—NAT zones

Modes

EXEC

Usage

Use this commands to display the NAT configuration and operation, and NAT table entries.

Examples

```
sonic# show nat translations count

Static NAT Entries ..... 4
Static NAPT Entries ..... 2
Dynamic NAT Entries ..... 0
Dynamic NAPT Entries ..... 4
Static Twice NAT Entries ..... 0
Static Twice NAPT Entries ..... 4
Dynamic Twice NAT Entries ..... 0
Dynamic Twice NAPT Entries ..... 0
Total SNAT/SNAPT Entries ..... 9
Total DNAT/DNAPT Entries ..... 9
Total Entries ..... 14
```

```
sonic# show nat translations

Protocol Source Destination Translated Source Translated Destination
----- -----
all 10.0.0.1 --- 65.55.42.2 --- 10.0.0.1
all --- 65.55.42.2 --- 10.0.0.1
all 10.0.0.2 --- 65.55.42.3 --- 10.0.0.2
all --- 65.55.42.3 --- 10.0.0.2
tcp 20.0.0.1:4500 --- 65.55.42.1:2000 --- 20.0.0.1:4500
tcp --- 65.55.42.1:2000 --- 20.0.0.1:4500
udp 20.0.0.1:4000 --- 65.55.42.1:1030 --- 20.0.0.1:4000
udp --- 65.55.42.1:1030 --- 20.0.0.1:4000
tcp 20.0.0.1:6000 --- 65.55.42.1:1024 --- 20.0.0.1:6000
tcp --- 65.55.42.1:1024 --- 20.0.0.1:6000
tcp 20.0.0.1:5000 65.55.42.1:2000 65.55.42.1:1025 20.0.0.1:4500
tcp 20.0.0.1:4500 65.55.42.1:1025 65.55.42.1:2000 20.0.0.1:5000
```

```
sonic# show nat statistics

Protocol Source Destination Packets Bytes
----- -----
all 100.100.100.100 200.200.200.5 15 12785
all 17.17.17.17 15.15.15.15 10 12754
all 12.12.12.14 --- 0 0
all --- 138.76.28.1 12 12500
tcp 12.12.15.15:1200 --- 0 0
tcp --- 138.76.29.2:250 8 85120
tcp 100.100.101.101:251 200.200.201.6:276 21 21654
tcp 17.17.18.18:1251 15.15.16.16:1201 18 21765
```

```
sonic# show nat config static
Global L4 Local IP Local L4 Twice-Nat
```

```

Nat Type IP Protocol Global IP Port Port Port Id
----- -----
dnat all 65.55.45.5 --- 10.0.0.1 --- ---
dnat all 65.55.45.6 --- 10.0.0.2 --- ---
dnat tcp 65.55.45.7 2000 20.0.0.1 4500 1
snat tcp 20.0.0.2 4000 65.55.45.8 1030 1

sonic# show nat config pool
Pool Name Global IP Range Global L4 Port Range
-----
Pool1 65.55.45.5 1024-65535
Pool2 65.55.45.6-65.55.45.8 ---
Pool3 65.55.45.10-65.55.45.15 500-1000

sonic# show nat config bindings
Binding Name Pool Name Access-List Nat Type Twice-Nat Id
-----
Bind1 Pool1 --- snat ---
Bind2 Pool2 1 snat 1
Bind3 Pool3 2 snat --

sonic# show nat config globalvalues
Admin Mode : enabled
Global Timeout : 600 secs
TCP Timeout : 86400 secs
UDP Timeout : 300 secs

sonic# show nat config zones
Port Zone
-----
Ethernet0 1
Loopback0 1
Vlan5 0
PortChannel12 2

```

Releases 3.1 or later

show neighbor-suppress-status

Displays ARP and ND suppression information.

Command show neighbor-suppress-status [vlan-id]

Options *vlan-id*—(Optional) Specify the VLAN ID (1 to 4094)

Modes EXEC

Usage Use this command to view the ARP and ND suppression status.

Example

```

sonic# show neighbor-suppress-status
-----
VlanId SuppressionStatus
-----
Vlan1001 on
Vlan1002 on
Vlan1003 on
Vlan1004 on
Vlan1005 on
Vlan1006 on
Vlan1007 on
Vlan1008 on
Vlan1009 on
Vlan1010 on
Vlan1011 on
Vlan1012 on
Vlan1013 on
Vlan1014 on
Vlan1015 on
Vlan1016 on

```

```

Vlan1017    on
Vlan1018    on
Vlan1019    on
Vlan2000    off
Vlan1020    on
--more--

sonic# show neighbor-suppress-status 1
-----
VlanId      SuppressionStatus
-----
Vlan1       on

```

Releases 3.1 or later

show ntp associations

Displays NTP associations.

Command	show ntp associations
Options	None
Modes	EXEC
Usage	<p>Command output:</p> <ul style="list-style-type: none"> • * — Switch is synchronized with this server or peer • number — Switch is not yet synchronized with this server or peer • + — Switch selected this server or peer for time synchronization • - — Switch considers this server or peer as a candidate for time synchronization • ~ — Server or peer is statically configured • remote — IP address of the NTP server or peer • refid — IP address of the remote device with which the server or peer synchronizes • st — Stratum level; number of hops that the NTP server or peer is from the time-source device (0 to 16). 0 indicates that the device is the time source; 1 indicates that the device is directly connected to the time source; 2 indicates that the device is connected to the stratum 1 device, and so on. 16 means that the device is not synchronized with a time source. As an NTP client, the switch automatically uses the server or peer with the lowest stratum number. • t — Type of NTP device: <ul style="list-style-type: none"> ◦ u — Unicast or anycast NTP client ◦ b — Broadcast or multicast NTP client ◦ l — Local reference clock on switch ◦ s — Symmetric peer ◦ A — Anycast NTP server ◦ B — Broadcast NTP server ◦ M — Multicast NTP server • when — Time (in seconds) since an NTP packet update was received or since the time was last synchronized • poll — Polling interval (in seconds) used by the switch to send NTP time requests (8 to 5160; 36 hours) • reach — Reachability of the NTP server; if the reach value is nonzero, the server is reachable. If the value is 0, the server is unreachable. The reach value is a peer variable that records when a valid NTP packet is received when an NTP packet is sent. • delay — Round-trip delay (in milliseconds) to the NTP server • offset — Time difference (in milliseconds) between the switch and the NTP server or another NTP peer • jitter — Mean deviation in times between the switch and the NTP server based on multiple time samples

Example

```

sonic# show ntp associations
remote      refid      st t when poll reach delay  offset  jitter
=====
```

```
+10.11.0.1 10.11.8.1 4 u 9 64 1 0.232 -2.570 0.062
*10.11.0.2 10.11.8.1 4 u 8 64 1 0.262 -0.747 0.033
* master (synced), # master (unsynced), + selected, - candidate
```

Releases 3.1 or later

show ntp global

Displays global NTP information.

Command show ntp global

Options None

Modes EXEC

Usage Use this command to the global NTP configuration.

Example

```
sonic# show ntp global
-----
NTP Global Configuration
-----
NTP source-interface:   Ethernet8
                        Loopback100
NTP vrf:               mgmt
```

Releases 3.1 or later

show ntp server

Displays NTP server information.

Command show ntp server

Options None

Mode EXEC

Usage Use this command to view the NTP server details. NTP server preference setting is available from the 4.1 release.

Example

```
sonic# show ntp server
-----
NTP Servers           minpoll maxpoll Prefer Authentication key ID
-----
10.89.192.129          6      10    False
134.214.100.6          6      10    True
144.126.242.176        6      10    True
159.138.166.199        6      10    True
```

Releases 3.1 or later

show object-groups

Displays the details of object group used for clients that share the dynamic ACLs applied by PAC.

Command show object-groups {group-name | type {network}}

Options

- *group-name*—Object group information using name (up to 63 characters)
- *network*—All Object groups

Modes EXEC

Usage

Dynamic ACLs applied by the PAC can be shared by multiple clients. Such common client IPs are grouped by using network object groups. Use this command to get the details of the object group. Object group type and name are optional. If the object group name and type are not specified, all the object groups are displayed. If the object group type is specified, all the object groups of a given type are displayed. If the object group name is specified, the specific object group is displayed.

Examples

```
sonic# show object-groups object-group-example type network
description: Object group example
network-object host 1.1.1.1
```

Releases

4.0 or later

show pbf next-hop-group

Displays the policy-based forwarding next-hop groups configuration and references.

Command

```
show pbf next-hop-group {[show-fbs-group-name] | [type]} {ip | ipv6}
```

Options

show-fbs-group-name—(Optional) Specify the flow-based service group name (up to 32 characters)

Modes

EXEC

Usage

Use this command to view the policy-based forwarding (PBF) next-hop groups.

Example

```
sonic# show pbf next-hop-group ipv4-test

Next-hop-group ipv4-test Type ip
  Description:
  Threshold type: percentage
  Threshold up: 80
  Threshold down: 30
  Members:
    entry 1 next-hop 10.1.1.1 recursive
    entry 2 next-hop 10.1.1.2 vrf VrfRed non-recursive
    entry 3 next-hop 10.1.1.3
  Referenced in flows:
    policy-map pbr-test at priority 100
```

Releases

3.2 or later

show pbf next-hop-group status interface

Displays the operational state and members of the policy-based forwarding next-hop group applied on an interface.

Command

```
show pbf next-hop-group status interface {eth-if-id | po-if-id | vlan-if-
id | eth-sub-if-id | po-sub-if-id} {[show-fbs-group-name] | [type]} {ip | 
ipv6}
```

Options

- *eth-if-id*—Ethernet interface ID (0 to 255)
- *po-if-id*—PortChannel interface ID (1 to 128)
- *vlan-if-id*—VLAN interface ID (1 to 4094)
- *eth-sub-if-id*—Ethernet subinterface ID
- *po-sub-if-id*—PortChannel subinterface ID
- *show-fbs-group-name*—(Optional) Flow-based services group name (up to 32 characters)

Modes

EXEC

Usage

Use this command to view the policy-based forwarding next-hop group status for an interface.

Example

```
sonic# show pbf next-hop-group status Ethernet 0

Ethernet0
```

```

Next-hop-group ipv4-test Type ip
  Status: Active
  Members:
    Entry 1 next-hop 10.1.1.1 recursive (Active)
    Entry 2 next-hop 10.1.1.2 vrf VrfRed non-recursive
    Entry 3 next-hop 10.1.1.3 (Active)
  Replication paths:
    IP:10.1.1.1 Vlan:100 Port:Ethernet0
    IP:10.1.1.2 Port:Ethernet1
    IP:10.1.1.3 Port:Ethernet2.100
    IP:10.1.1.4 Port:Tunnel 1.1.1.1 VNI:10000

```

Releases 3.2 or later

show pbf next-hop-group status Switch

Displays the operational state and members of the policy-based forwarding next-hop group that is applied on switch-level.

Command show pbf next-hop-group status Switch {[*show-fbs-group-name*] | [*type*]} {ip | ipv6}

Options *show-fbs-group-name*—(Optional) Flow-based services group name (up to 32 characters)

Modes EXEC

Usage Use this command to view the policy-based forwarding next-hop group status on the switch.

Examples

```

sonic#
show pbf next-hop-group status Switch
Switch
  Next-hop-group pbf_nh_group Type ip
    Status: Active
    Members:
      Entry 1 next-hop 192.168.1.2 (Active)
      Entry 2 next-hop 192.168.2.2 (Active)
      Entry 3 next-hop 192.168.3.2 (Active)

```

Releases 3.2 or later

show pbf replication-group

Displays the operational state and members of the PBF replication-group status.

Command show pbf replication-group { *show-fbs-group-name* | status | type {ip | ipv6} }

Options

- *show-fbs-group-name*—(Optional) Flow-based services group name (up to 32 characters)
- *status*—(Optional) Display group information
- *type*—(Optional) Display all replication groups using the group type

Modes EXEC

Usage Use this command to view the policy-based forwarding replication-group status.

Examples

```

sonic# show pbf replication-group
Replication-group group1 Type ip
  Description:
  Members:
  Referenced in flows:

```

Releases 4.0 or later

show pbf replication-group status interface

Displays the policy-based forwarding next-hop group replication-group status for an interface.

Command show pbf replication-group status interface {Ethernet *phy-if-name* | PortChannel *port-ch-id* | Vlan *vlan-id*} [type {ip | ipv6}]

- Options**
- *phy-if-name*—Enter the physical interface details.
 - *port-ch-id*—Enter the PortChannel details (1 to 128).
 - *vlan-id*—Enter the VLAN interface ID (1 to 4094).
 - *type*—Display all replication groups using the group type.

Modes EXEC

Usage Use this command to view the policy-based forwarding replication-group status for an interface.

Examples

```
sonic# show pbf replication-group status interface Ethernet 23
Ethernet23
    Replication-group pbf_repl_group Type ip
        Status: Active
        Members:
            Entry 1 next-hop 192.168.1.2 single-copy (Active)
            Entry 2 next-hop 192.168.2.2 single-copy (Active)
            Entry 3 next-hop 192.168.3.2 single-copy (Active)
        Replication Paths:
            NextHop:192.168.1.2 L3Intf:Ethernet20
            NextHop:192.168.2.2 L3Intf:Ethernet21
            NextHop:192.168.3.2 L3Intf:Ethernet22
sonic#
```

Releases 4.0 or later

show pbf replication-group status Switch

Displays the operational state and members of the PBF replication-group that are applied on switch-level.

Command show pbf replication-group status Switch [*fbs-group-name* | [type {ip | ipv6}]]

- Options**
- *fbs-group-name*—(Optional) Flow-based services group name (up to 63 characters).
 - *type*—Display all replication groups using the group type.

Modes EXEC

Usage None

Examples

```
sonic# show pbf replication-group status Switch
Switch
    Replication-group pbf_repl_group Type ip
        Status: Active
        Members:
            Entry 1 next-hop 192.168.1.2 single-copy (Active)
            Entry 2 next-hop 192.168.2.2 single-copy (Active)
            Entry 3 next-hop 192.168.3.2 single-copy (Active)
        Replication Paths:
            NextHop:192.168.1.2 L3Intf:Ethernet20
            NextHop:192.168.2.2 L3Intf:Ethernet21
            NextHop:192.168.3.2 L3Intf:Ethernet22
```

Releases 4.0 or later

show pending

Displays the MST configuration that is not activated.

Command	show pending
Options	None
Modes	SPANNING TREE
Usage	Apply the pending configuration using activate command. Cancel the pending configuration using abort command.

Examples

```
sonic-cl(i(config)# spanning-tree mst configuration
sonic-cl(i(config-mst)# show pending
Pending MST Configuration
Name [test]
Revision 10 Instances configured 4
Instance Vlans mapped
-----
0      1-9,11-19,21-4093
1      10
2      20
4094   4094
-----
sonic-cl(i(config-mst) #
```

Releases	4.0 or later
-----------------	--------------

show platform environment

Displays platform environment information including fan, temperature, power supply, and adapter status.

Command	show platform environment
Options	None
Modes	EXEC
Usage	Use this command to verify platform environment details such as fan, temperature, power supply, and adapter status.

Example

```
sonic# show platform environment
Onboard Temperature Sensors :
    CPU Temp          : 30.0 degrees C
    NPU Temp          : 63.0 degrees C
    NPU Rear Temp    : 32.0 degrees C
    INLET Left Temp  : 26.0 degrees C
    INLET Right Temp : 26.0 degrees C
    OUTLET Left Temp : 21.0 degrees C
    OUTLET Right Temp: 22.0 degrees C
    OSFP Rear Temp   : 26.0 degrees C
    CPUCD Front Temp: 23.0 degrees C
    PSU1 AF Temp     : 31.0 degrees C
    PSU1 MID Temp   : 45.0 degrees C
    PSU1 Rear Temp   : 43.0 degrees C
    PSU2 AF Temp     : 32.0 degrees C
    PSU2 MID Temp   : 41.0 degrees C
    PSU2 Rear Temp   : 43.0 degrees C
Fan Trays :
    FanTray1 :
        Fan1 Speed      : 7504 RPM
        Fan1 State      : Normal
        Fan1 Airflow    : Exhaust
        Fan2 Speed      : 6901 RPM
        Fan2 State      : Normal
        Fan2 Airflow    : Exhaust
```

```

FanTray2 :
    Fan1 Speed      : 7504 RPM
    Fan1 State       : Normal
    Fan1 Airflow     : Exhaust
    Fan2 Speed      : 6968 RPM
    Fan2 State       : Normal
    Fan2 Airflow     : Exhaust

FanTray3 :
    Fan1 Speed      : 7504 RPM
    Fan1 State       : Normal
    Fan1 Airflow     : Exhaust
    Fan2 Speed      : 6968 RPM
    Fan2 State       : Normal
    Fan2 Airflow     : Exhaust

FanTray4 :
    Fan1 Speed      : 7571 RPM
    Fan1 State       : Normal
    Fan1 Airflow     : Exhaust
    Fan2 Speed      : 6968 RPM
    Fan2 State       : Normal
    Fan2 Airflow     : Exhaust

PSUs :
    PSU1 :
        Input Voltage      : 207.0 Volts
        Input Power         : 432.0 Watts
        Input Current       : 2.1 Amps
        Output Current      : 33.6 Amps
        Output Power        : 408.0 Watts
        Output Voltage      : 12.0 Volts
        AF Temp Temperature : 31.0 degrees C
        MID Temp Temperature: 45.0 degrees C
        Rear Temp Temperature: 43.0 degrees C
        FAN RPM             : 6885 RPM
        Airflow              : Exhaust

    PSU2 :
        Input Voltage      : 207.0 Volts
        Input Power         : 432.0 Watts
        Input Current       : 2.1 Amps
        Output Current      : 33.6 Amps
        Output Power        : 408.0 Watts
        Output Voltage      : 12.0 Volts
        AF Temp Temperature : 32.0 degrees C
        MID Temp Temperature: 41.0 degrees C
        Rear Temp Temperature: 43.0 degrees C
        FAN RPM             : 7395 RPM
        Airflow              : Exhaust

```

Releases 3.0 or later

show platform fanstatus

Displays hardware information about the fan status.

Command	show platform fanstatus
Options	None
Modes	EXEC
Usage	<p>Use this command to view the fan status.</p> <ul style="list-style-type: none"> • OK—Fan is installed and operational. • NOT OK—Fan is installed and not operational. • NOT PRESENT—Fan is not installed.

Example

```
sonic# show platform fanstatus
```

Fan	Status	Speed (RPM)	Direction
FAN 1	OK	8520	exhaust
FAN 2	OK	7680	exhaust
FAN 3	OK	8520	exhaust
FAN 4	OK	7680	exhaust
FAN 5	OK	8640	exhaust
FAN 6	OK	7920	exhaust
FAN 7	OK	8760	exhaust
FAN 8	OK	7800	exhaust

Releases

3.1 or later

show platform firmware

Displays the platform firmware installed on a switch.

Command show platform firmware

Options None

Modes EXEC

Usage Use this command to verify the firmware installed on a switch. The firmware components are displayed in alphabetical order.

Examples This output example is from a Z9432F-ON platform.

```
sonic# show platform firmware
-----
Chassis  Module  Component      Version   Description
-----
Z9432F-ON N/A    BIOS          1CAWT005  Performs initialization of hardware...
                                BMC           3.03    Platform management controller for...
                                FPGA          9.0     Used for managing the system LEDs
                                PCIe          2.12    ASIC PCIe firmware
                                Secondary CPLD 1 6.0    Used for managing SFP28/QSFP28 port...
                                Secondary CPLD 2 6.0    Used for managing SFP28/QSFP28 port...
                                System CPLD    15.0   Used for managing the CPU power
                                         sequence...
```

Releases

3.2 or later

show platform firmware detail

Displays detailed information of the firmware installed on a switch.

Command show platform firmware detail

Options None

Modes EXEC

Usage Use this command to view the firmware version details of each component and its description.

Examples

```
sonic# show platform firmware detail
-----
Platform Firmware Information
-----
Chassis:          Z9864F-ON
Module:           N/A
Component:        BIOS
Firmware Version: 1CAWT005
Description:      Performs initialization of hardware components
during booting
```

```

Chassis: Z9864F-ON
Module: N/A
Component: BMC
Firmware Version: 3.03
Description: Platform management controller for on-board
temperature monitoring,
in-chassis power, Fan and LED control

Chassis: Z9864F-ON
Module: N/A
Component: FPGA
Firmware Version: 9.0
Description: Used for managing the system LEDs

Chassis: Z9864F-ON
Module: N/A
Component: PCIe
Firmware Version: 2.12
Description: ASIC PCIe firmware

Chassis: Z9864F-ON
Module: N/A
Component: Secondary CPLD 1
Firmware Version: 6.0
Description: Used for managing OSFP112 port transceivers (OSFP112
1-32)

Chassis: Z9864F-ON
Module: N/A
Component: Secondary CPLD 2
Firmware Version: 6.0
Description: Used for managing OSFP112 port transceivers (OSFP112
33-64)

Chassis: Z9864F-ON
Module: N/A
Component: System CPLD
Firmware Version: 15.0
Description: Used for managing the CPU power sequence and CPU
states

```

Releases 3.2 or later

show platform psustatus

Displays hardware information for the power supply unit (PSU) status.

Command show platform psustatus

Options None

Modes EXEC

Usage Use this command to view the hardware information for the power supply unit (PSU) status.

- OK—Power supply is installed and operational.
- NOT OK—Power supply is installed and not operational.
- NOT PRESENT—Power supply is not installed.

Example

```

sonic# show platform psustatus
-----
PSU          Status
-----
PSU 1        OK
PSU 2        OK

```

Releases 3.1 or later

show platform psusummary

Displays summary hardware information about the power supply unit (PSU).

Command show platform psusummary

Options None

Modes EXEC

Usage The show platform psusummary command displays N/A for Output Current, Output Power, Output Voltage on the N3248PXE-ON and E3248PXE-ON platforms for external PSUs.

Example

```
sonic# show platform psusummary
PSU 1:
    Description      :DPS-1600AB-34 C
    Fans            :1
    Mfg Name        :DELTA
    Name             :PSU 1
    Oper Status     :OK
    Serial Number   :xxxxxxxxxxxx
    Status LED:    :None
    Type (AC/DC)    :AC
    Input Current (A):3.00
    Input Power (W) :669.00
    Input Voltage (V):225.80
    Output Current (A):11.30
    Output Power (W) :629.00
    Output Voltage (V):55.60
    Fan Speed (RPM) :8352
    Fan Direction   :exhaust
    Temperature     :35.40
PSU 2:
    Description      :DPS-1600AB-34 C
    Fans            :1
    Mfg Name        :DELTA
    Name             :PSU 2
    Oper Status     :OK
    Serial Number   :xxxxxxxxxxxx
    Status LED:    :None
    Type (AC/DC)    :AC
    Input Current (A):3.00
    Input Power (W) :681.00
    Input Voltage (V):225.20
    Output Current (A):11.70
    Output Power (W) :646.00
    Output Voltage (V):55.50
    Fan Speed (RPM) :7920
    Fan Direction   :exhaust
    Temperature     :33.20
PSU 3:
    Description      :04JR64
    Fans            :0
    Mfg Name        :DELTA
    Name             :PSU 3
    Oper Status     :OK
    Serial Number   :xxxxxxxxxxxxxx
    Status LED:    :None
    Type (AC/DC)    :Unknown
    Input Current (A):N/A
    Input Power (W) :N/A
    Input Voltage (V):N/A
    Output Current (A):22.90
    Output Power (W) :1276.00
    Output Voltage (V):55.70
    Fan Speed (RPM) :0
    Fan Direction   :none
    Temperature     :N/A
```

Releases

3.1 or later

show platform sbstatus

Displays Secure Boot status.

Command	show platform sbstatus
Options	None
Modes	EXEC
Usage	Use the show platform sbstatus command to check if an Enterprise SONiC switch supports secure boot. (The Z9864F-ON, Z9664F-ON, Z9432F-ON, and S5448-ON switches support Secure Boot.)
Examples	If a switch does not support secure boot: sonic# show platform sbstatus SecureBoot is not supported on this system
	If a switch supports secure boot: sonic# show platform sbstatus SecureBoot is Enabled
Releases	4.0 or later

show platform ssdhealth

Displays solid-state drive (SSD) health information for an Enterprise SONiC switch.

Command	show platform ssdhealth
Options	None
Modes	EXEC
Usage	Use the show platform ssdhealth command to display the health status of the solid-state drive. A low health percentage in the output indicates that the SSD is nearing end-of-life and should be replaced to avoid a switch crash.
Example	sonic# show platform ssdhealth Firmware Version : SBR13067 Health : 100.0 Device Model : SFSA120GM3AA2TO-C-OC-23P-DEL Serial Number : 000060203793A4000120 Temperature : 32C
Releases	4.1.0 or later

show platform syseeprom

Displays platform system EEPROM information.

Command	show platform syseeprom
Options	None
Modes	EXEC
Usage	Use this command to view the system EEPROM information.
Example	sonic# show platform syseeprom ----- Attribute Value/State

```

-----
Base Mac Address          :e8:b2:65:b9:cc:5b
Crc 32                   :0xAA6EFAC6
Platform                 :x86_64-dell_z9864f-r0
Device Version           :1
Diag Version             :v2.0.0
Hardware Version          :X02a
Product Name              :Z9864F-ON
Location                  :Slot 1
Mac Addresses             :768
Manufacture Country       :TW
Mfg Date                 :2024-02-20
Mfg Name                  :DNT00
Onie Version              :v2.0.0
Part Number               :0V1Y60
Serial Number              :TWOV1Y60DNT004250007
Service Tag                :8XXM9Q3
Vendor Ext                :0x00 0x00 0x02 0xA2
Vendor Name                :Dell

```

Releases 3.0 or later

show platform temperature

Displays hardware information about the switch sensor temperature.

Command show platform temperature

Options None

Modes EXEC

Usage Use this command to view the hardware information about the switch sensor temperature.

Example

```

sonic# show platform temperature
TH - Threshold
-----
Name      Temperature  High TH  Low TH  Critical High TH  Critical Low TH  Warning  Timestamp
-----
ASIC On-board    40        78      0       80      N/A     false   20210107 22:46:35
CPU On-board     36        90      0       94      N/A     false   20210107 22:46:34
Inlet Airflow Sensor 29        0       0       0       N/A     false   20210107 22:46:37
PSU1 Airflow Sensor 29        0       0       0       N/A     false   20210107 22:46:37
PSU2 Airflow Sensor 30        0       0       0       N/A     false   20210107 22:46:38
System Front Left 24        59      0       62      N/A     false   20210107 22:46:35
System Front Middle 35        0       0       0       N/A     false   20210107 22:46:36
System Front Right 25        0       0       0       N/A     false   20210107 22:46:36

```

Releases 3.1 or later

show platform temperature detail

Displays detailed temperature sensor information.

Command show platform temperature detail

Options None

Modes EXEC

Usage Use this command to view the detailed hardware information about the switch sensor information.

Example

```

sonic# show platform temperature detail

Platform Temperature Sensor Details
-----
Sensor name:          ASIC On-board
Temperature:          32
High threshold:       78
Low threshold:        0
Critical High threshold: 80

```

```

Critical Low threshold: N/A
Warning status: False
Timestamp: 2020-12-03T01:11:24Z

Sensor name: CPU On-board
Temperature: 27
High threshold: 90
Low threshold: 0
Critical High threshold: 94
Critical Low threshold: N/A
Warning status: False
Timestamp: 2020-12-03T01:11:24Z

Sensor name: Inlet Airflow Sensor
Temperature: 22
High threshold: 0
--more--

```

Releases 3.1 or later

show poe

Displays global-level POE information.

Command show poe

Options None

Modes EXEC

Usage Use this command to view the current POE configuration and the system-wide status information.

Examples

```

sonic# show poe

Firmware Version      : 3.55
Total Power Available : 1056 Watts
Threshold Power       : 950.0 Watts
Total Power Consumed  : 97.0 Watts
Usage Threshold       : 90 %
Power Management Mode: Dynamic

```

Releases 4.0 or later

show poe port configuration

Displays port-level POE configuration information.

Command show poe port configuration { all | Ethernet *intf-name* }

- **all**—All PoE ports
- ***intf***—Ethernet interface number

Modes EXEC

Usage Use this command to view the POE information of all the ports or a specific port.

Examples

```

sonic# show poe port configuration all

```

Port	Admin Mode	Priority	Power Limit (mW)	Power Limit Type	High Power	Power-Up Mode	Detection Type
Eth1/1	Enabled	Low	99900	Class Based		dot3bt	dot3bt+legacy
Eth1/2	Enabled	Low	99900	Class Based		dot3bt	Dot3bt
Eth1/3	Enabled	Low	99900	Class Based		dot3bt	dot3bt+legacy
Eth1/46	Enabled	Low	99900	Class Based		dot3bt	dot3bt+legacy

Eth1/47	Enabled	Low	99900	Class Based	dot3bt	dot3bt+legacy
Eth1/48	Enabled	Low	99900	Class Based	dot3bt	dot3bt+legacy

Releases 4.0 or later

show poe port info

Displays port-level POE operational information.

Command show poe port info { all | Ethernet *intf-name* }

- Options**
- **all**—All PoE ports
 - **Ethernet *intf-name***—Ethernet interface number

Modes EXEC

Usage Use this command to display POE port information.

Examples

```
sonic-clli# show poe port info all
-----
Port      Class Requested   Class Assigned   Output Power (mW)   Output Current (mA)   Output Voltage (V)   Temp (C)   Status   Fault Status
----- 
Ethernet0  Yes           32000          Unknown        0             0               0               0             0           0
Disabled   No Error
Ethernet1  Yes           32000          Unknown        0             0               0               0             0           0
Disabled   No Error
Ethernet2  Yes           32000          Unknown        0             0               0               0             0           0
Disabled   No Error
Ethernet3  Yes           32000          Unknown        0             0               0               0             0           Disabled
No Error
Ethernet4  Yes           32000          Unknown        0             0               0               0             0           Disabled
No Error
Ethernet5  Yes           32000          Unknown        0             0               0               0             0           Disabled
No Error
Ethernet6  Yes           32000          Unknown        0             0               0               0             0           Disabled
No Error
```

```
sonic# show poe port info Eth1/48
-----
Port      Class Requested   Class Assigned   Output Power (mW)   Output Current (mA)   Output Voltage (V)   Temp (C)   Status   Fault Status
Status
----- 
Eth1/48   2              2              2700          49            56.1            N/A           Delivering  No
Error

Overload Counter : 0
Short Counter   : 0
Power Denied Counter : 0
Absent Counter  : 0
Invalid Signature Counter : 0
```

Table 12. show poe port info Fields

Field	Description
Class Requested	The power class requested by the Powered Device (PD).
Class Assigned	The power class identified by the Power Sourcing Equipment (PSE).
Output Power	The total power minus the guard band, and if usage exceeds this value, new ports are not powered up.

Table 12. show poe port info Fields (continued)

Field	Description
Output Current	The current that this port is supplying to an attached device, which is measured in millamps.
Output Voltage	The voltage that this port is supplying to an attached device, which is measured in volts.
Temperature	The temperature measured at this PSE port, in degrees Celsius.
Status	The operational status of the port PD detection.
Fault Status	The error description when the PSE port is in fault status.

Releases

4.0 or later

show policy-map

Displays flow-based services (FBS) policy information.

Command

```
show policy-map {[show-fbs-policy-name] | [type]}] {qos | monitoring | forwarding | copp}
```

Options

- *show-fbs-policy-name*—(Optional) Flow-based services policy name (up to 63 characters)
- *type qos*—Display QOS policies that do DSCP/PCP remarking, policing, and setting traffic class.
- *type monitoring*—Display monitoring policies for SPAN and ERSPAN.
- *type forwarding*—Display forwarding policies that route traffic to a specified next hop, forward L2 traffic to the specified interface, drop the packets.
- *type copp*—Display ACL CoPP policies that police traffic destined to CPU, and set CPU queue.

Modes

EXEC

Usage

Policy-map type and policy-map name arguments are optional. If the type argument or policy-map name is not provided, all policy-map information displays. You can also display corresponding policy-map information of a given type or given name.

Example

```
sonic# show policy-map
Policy policy_mirror Type monitoring
  Description:
    Flow class1 at priority 10
      Description:
        set mirror-session mirror1
    Applied to:
      Vlan100 at Ingress

Policy policy_qos Type qos
  Description:
    Flow class_permit_ipv6 at priority 10
      Description:
        police cir 3000000000 cbs 3000000000 pir 3000000000 pbs 3000000000
    Flow class_permit_ip at priority 10
      Description:
        police cir 3000000000 cbs 3000000000 pir 3000000000 pbs 3000000000
    Applied to:
      Vlan100 at Egress

Policy policy_vrf Type forwarding
  Description:
    Flow class_permit_ipv6 at priority 10
      Description:
        set ipv6 nexthop 1211::2 priority 20
        set ipv6 nexthop 1212::2 vrf Vrf-BLUE priority 30
```

```

Flow class permit_ip at priority 10
Description:
set ip nexthop 12.12.1.2 vrf default priority 30
set ip nexthop 12.12.2.2 vrf Vrf-BLUE priority 20
set ip nexthop 12.12.1.2 priority 10
Applied to:
  Vlan100 at Ingress
  Switch at Ingress

```

Releases 3.1 or later

show PortChannel summary

Displays PortChannel summary information.

Command show PortChannel summary

Options None

Modes EXEC

Usage Use this command to display the status of all port channels.

Example

```

sonic# show PortChannel summary
Flags(oper-status): D - Down U - Up (portchannel)
                      P - Up in portchannel (members) I - LACP individual
-----
Group      PortChannel     Type       Protocol      Member Ports
-----
61         PortChannel61   (U)        Eth          LACP          Ethernet0(P)
                                         Ethernet4(P)
                                         Ethernet28(P)
                                         Ethernet29(P)
                                         Ethernet36(P)
                                         Ethernet40(P)
                                         Ethernet52(P)
                                         Ethernet56(P)
62         PortChannel62   (U)        Eth          LACP          Ethernet4(P)
                                         Ethernet28(P)
                                         Ethernet29(P)
                                         Ethernet36(P)
                                         Ethernet40(P)
                                         Ethernet52(P)
                                         Ethernet56(P)
100        PortChannel100  (U)        Eth          LACP          Ethernet0(P)
                                         Ethernet4(P)
                                         Ethernet28(P)
                                         Ethernet29(P)
                                         Ethernet36(P)
                                         Ethernet40(P)
                                         Ethernet52(P)
                                         Ethernet56(P)
200        PortChannel200  (U)        Eth          LACP          Ethernet4(P)
                                         Ethernet28(P)
                                         Ethernet29(P)
                                         Ethernet36(P)
                                         Ethernet40(P)
                                         Ethernet52(P)
                                         Ethernet56(P)

```

Releases 3.0 or later

show port-group

Displays the list of port groups, member ports, and valid speeds.

Command show port-group

Options None

Modes EXEC

Usage The port-group is not supported on all hardware platforms.

Example

```

sonic# show port-group
-----
Port-group  Interface range    Valid speeds  Default Speed  Current
-----
1           Eth1/1 - Eth1/4    10G, 25G     25G          10G
2           Eth1/5 - Eth1/8    10G, 25G     25G          10G
3           Eth1/9 - Eth1/12   10G, 25G     25G          25G
4           Eth1/13 - Eth1/16  10G, 25G     25G          25G
5           Eth1/17 - Eth1/20  10G, 25G     25G          25G
6           Eth1/21 - Eth1/24  10G, 25G     25G          25G
7           Eth1/25 - Eth1/28  10G, 25G     25G          10G
8           Eth1/29 - Eth1/32  10G, 25G     25G          10G
9           Eth1/33 - Eth1/36  10G, 25G     25G          10G

```

10	Eth1/37 - Eth1/40	10G, 25G	25G	10G
11	Eth1/41 - Eth1/44	10G, 25G	25G	25G
12	Eth1/45 - Eth1/48	10G, 25G	25G	25G

Releases 3.1 or later

show port-security

Displays port MAC address security information.

Command show port-security

Options None

Modes EXEC

Usage Use this command to display information for all MAC-security-enabled ports after enabling port security feature on the ports.

Examples

```
sonic# show port-security
Secure Port      isEnabled      MaxSecureAddr   FdbCount      ViolationCount
SecurityAction
-----
Ethernet1        Y             11              11            360                      PROTECT
```

Releases 4.0 or later

show port-security interface

Displays interface-level port security information.

Command show port-security interface *interface-name*

Options *interface-name*—Interface name (up to 63 characters)

Modes EXEC

Usage Use this command to get port security information for a specified port after enabling port security on the ports.

Examples

```
sonic# show port-security interface Ethernet1
Interface : Ethernet1
Port MAC Security is Enabled : True
Maximum allowed Secure MAC   : 11
Action taken on Violation    : PROTECT
Total MAC address            : 11
Security Violation Count    : 360
```

Releases 4.0 or later

show priority-flow-control

Displays the priority flow-control (PFC) summary.

Command show priority-flow-control watchdog

Options None

Modes EXEC

Usage Use this command to check if the PFC watchdog is enabled or not and the configured polling interval.

Example

```
sonic# show priority-flow-control watchdog

Watchdog Summary
-----
Polling Interval:      : Not Configured (default 100ms)
Flex Counters:         : enabled
```

Releases

3.1 or later

show priority-group

Displays priority group information for watermarks and persistent-watermarks.

Command

```
show priority-group {{watermark {{headroom {[interface {[Ethernet phy-if-id]}]}} | {shared {[interface {Ethernet phy-if-id}]}}}} | {persistent-watermark {{headroom {[interface {Ethernet phy-if-id}]}}} | {shared {[interface {Ethernet phy-if-id}]}}}
```

Options

- *phy-if-id* — (Optional) Ethernet ID

Modes

EXEC

Usage

Use this command to display priority group watermarks, persistent-watermarks, and so on. There are various CLI options available to display information for shared, headroom, and interface watermarks.

Examples

```
sonic# show priority-group watermark shared
Ingress shared pool watermark per PG:
-----
Port      PG0   PG1   PG2   PG3   PG4   PG5   PG6   PG7
-----
Ethernet0  0     0     0     0     0     0     0     0
Ethernet4  0     0     0     0     0     0     0     0
Ethernet8  0     0     0     0     0     0     0     0
Ethernet12 0     0     0     0     0     0     0     0
Ethernet16 0     0     0     0     0     0     0     0
```

```
sonic# show priority-group persistent-watermark headroom
Ingress headroom persistent watermark per PG:
-----
Port      PG0   PG1   PG2   PG3   PG4   PG5   PG6   PG7
-----
Ethernet0  0     0     0     0     0     0     0     0
Ethernet4  0     0     0     0     0     0     0     0
Ethernet8  0     0     0     0     0     0     0     0
Ethernet12 0     0     0     0     0     0     0     0
Ethernet16 0     0     0     0     0     0     0     0
Ethernet20 0     0     0     0     0     0     0     0
Ethernet24 0     0     0     0     0     0     0     0
```

Releases

3.1 or later

show qos to switchport commands

Topics:

- show qos
- show qos map dot1p-tc
- show qos map dscp-tc
- show qos map pfc-priority-pg
- show qos map pfc-priority-queue
- show qos map tc-dot1p
- show qos map tc-dscp
- show qos map tc-pg
- show qos map tc-queue
- show qos scheduler-policy
- show qos wred-policy
- show queue
- show radius-server
- show radius-server dynamic-author
- show reboot-cause
- show route-map
- show running-configuration
- show running-configuration bfd
- show running-configuration bgp
- show running-configuration bgp as-path-access-list
- show running-configuration bgp community-list
- show running-configuration bgp extcommunity-list
- show running-configuration bgp neighbor
- show running-configuration bgp peer-group
- show running-configuration class-map
- show running-configuration dropcounters
- show running-configuration hardware
- show running-configuration hardware access-list
- show running-configuration hardware tcam
- show running-configuration igmp
- show running-configuration interface
- show running-configuration interface Loopback
- show running-configuration interface Management
- show running-configuration interface PortChannel
- show running-configuration interface Vlan
- show running-configuration interface vxlan
- show running-configuration ip access-list
- show running-configuration ip prefix-list
- show running-configuration ipv6 access-list
- show running-configuration ipv6 prefix-list
- show running-configuration line vty
- show running-configuration link state tracking
- show running-configuration mac access-list
- show running-configuration mclag
- show running-configuration mirror-session
- show running-configuration nat
- show running-configuration ospf

- show running-configuration ospf interface
- show running-configuration pbf next-hop-group
- show running-configuration pbf replication-group
- show running-configuration policy-map
- show running-configuration route-map
- show running-configuration spanning-tree
- show running-configuration subinterface
- show running-configuration tam
- show running-configuration vrf
- show service-policy
- show service-policy interface
- show service-policy policy-map
- show service-policy summary
- show sflow
- show sflow interface
- show snmp counters
- show snmp-server
- show snmp-server community
- show snmp-server group
- show snmp-server host
- show snmp-server interface-traps
- show snmp-server traps
- show snmp-server user
- show snmp-server view
- show spanning-tree
- show spanning-tree bpdu-guard
- show spanning-tree counters
- show spanning-tree inconsistentports
- show spanning-tree mst
- show spanning-tree mst configuration
- show spanning-tree mst detail
- show spanning-tree mst interface
- show ssh-server vrf
- show storm-control
- show storm-control interface
- show subinterfaces status
- show switch-profiles
- show switch-resource drop-monitor
- show switch-resource route-scale
- show switch-resource vlan-stacking
- show switching-mode
- show system
- show system cpu
- show system memory
- show system processes
- show system processes cpu
- show system processes mem-usage
- show system processes mem-util
- show system processes pid
- show system status
- show system vlan
- show tacacs-server
- show tacacs-server global
- show tacacs-server host
- show tam collectors
- show tam drop-monitor

- show tam drop-monitor sessions
- show tam features
- show tam flowgroups
- show tam ifa
- show tam ifa sessions
- show tam samplers
- show tam switch
- show tam tail-stamping
- show tam tail-stamping sessions
- show tech-support
- show tech-support cancel
- show techsupport-export
- show tech-support status
- show tech-support terminal
- show threshold breaches
- show threshold buffer-pool
- show threshold device
- show threshold priority-group
- show threshold queue
- show tpcm list
- show tpcm name
- show udld global
- show udld interface
- show udld neighbors
- show udld statistics
- show udld statistics interface
- show uptime
- show users
- show users configured
- show version
- show Vlan
- show vrrp
- show vrrp6
- show vxlan counters
- show vxlan interface
- show vxlan remote mac
- show vxlan remote mac count
- show vxlan remote nexthop-group
- show vxlan remote vni
- show vxlan remote vni count
- show vxlan tunnel
- show vxlan tunnel count
- show vxlan vlanvnimap
- show vxlan vlanvnimap count
- show vxlan vrfvnimap
- show vxlan vrfvnimap count
- show warm-restart
- show watermark interval
- show watermark telemetry
- show ztp-status
- shutdown
- snmp-server agentaddress
- snmp-server community
- snmp-server contact
- snmp-server enable trap
- snmp-server engine

- snmp-server group
- snmp-server host
- snmp-server location
- snmp-server user
- snmp-server view
- snmp trap enable
- soft-reconfiguration
- solo
- source-address
- source-interface
- source-ip
- source-port
- source-vrf
- spanning-tree bpdufilter
- spanning-tree bpduguard
- spanning-tree cost
- spanning-tree edge-port
- spanning-tree enable
- spanning-tree forward-time
- spanning-tree guard
- spanning-tree guard
- spanning-tree hello-time
- spanning-tree link-type
- spanning-tree loopguard
- spanning-tree max-age
- spanning-tree mode
- spanning-tree mst configuration
- spanning-tree mst forward-time
- spanning-tree mst hello-time
- spanning-tree mst max-age
- spanning-tree mst max-hops
- spanning-tree mst priority
- spanning-tree port
- spanning-tree portfast
- spanning-tree port-priority
- spanning-tree priority
- spanning-tree uplinkfast
- spanning-tree vlan
- spanning-tree vlan
- speed
- speed auto
- ssh-server vrf
- standalone-link-training
- startup-delay
- static
- storm-control broadcast
- storm-control unknown-multicast
- storm-control unknown-unicast
- strict-capability-match
- switch-id
- switch-resource
- switching-mode cut-through
- switchport access
- switchport trunk
- switchport vlan-mapping
- system-mac

- system resource-stats-polling-interval
- system vlan

show qos

Displays Quality of Service (QoS) information.

Command show qos interface {CPU | {*phy-intf-name* {[queue *queue-id*]}} {[priority-flow-control {statistics [queue]}]} } | *po-intf-name* | *vlan-intf-name* | *phy-sub-if-name*

- Options**
- *phy-intf-name*—Ethernet ID (0 to 255)
 - *queue-id*—(Optional) Queue ID
 - *po-intf-name*—Port channel ID (1 to 128)
 - *vlan-intf-name*—VLAN ID (1 to 4094)
 - *phy-sub-if-name*—Physical subinterface name

Modes EXEC

Usage Use this command to check the QoS configurations and priority flow control statistics.

Examples

```
sonic# show qos interface Eth 1/1
```

```
    scheduler policy: ROCE
    dscp-tc-map: ROCE
    dot1p-tc-map: ROCE
    tc-queue-map: ROCE
    tc-pg-map: ROCE
    pfc-priority-queue-map: ROCE
    pfc-priority-pg-map: ROCE
    pfc-asymmetric: off
    pfc-priority : 2,3
    PFC Watchdog
        Status          : on
        Action          : drop
        Detection Time : 200ms
        Restoration Time : 400ms
```

```
sonic# show qos interface Eth all
```

		Interface Maps												
Priority-Flow-Control		Scheduler		dscp	dot1p	fg-	fg	fg-	fg-	pfc-	pfc-	WATCHDOG		
Interface	detect	Policy	restore	-fg	-fg	queue	-pg	dscp	dot1p	p2q	p2pg mode	priority	action	
Eth1/1	200	400		ROCE	ROCE	ROCE	ROCE				ROCE	ROCE off	2,3	DROP
Eth1/2	200	400		ROCE	ROCE	ROCE	ROCE				ROCE	ROCE off	2,3	DROP
Eth1/3	200	400		ROCE	ROCE	ROCE	ROCE				ROCE	ROCE off	2,3	DROP
Eth1/4/1	200	400		ROCE	ROCE	ROCE	ROCE				ROCE	ROCE off	2,3	DROP
Eth1/4/2	200	400		ROCE	ROCE	ROCE	ROCE				ROCE	ROCE off	2,3	DROP
Eth1/4/3	200	400		ROCE	ROCE	ROCE	ROCE				ROCE	ROCE off	2,3	DROP
Eth1/4/4	200	400		ROCE	ROCE	ROCE	ROCE				ROCE	ROCE off	2,3	DROP

```
sonic# show qos interface Ethernet 0 priority-flow-control statistics
```

Flow Control frames received								
Interface	PFC0	PFC1	PFC2	PFC3	PFC4	PFC5	PFC6	PFC7
Ethernet0	0	0	0	0	0	0	0	0

Flow Control frames transmitted								
Interface	PFC0	PFC1	PFC2	PFC3	PFC4	PFC5	PFC6	PFC7
Ethernet0	0	0	0	0	0	0	0	0

```
sonic# show qos interface Ethernet 0 queue 3 priority-flow-control statistics
```

PFC Watchdog Statistics		Storms	Transmitted	Received	TX Last	RX Last
-------------------------	--	--------	-------------	----------	---------	---------

Interface	Queue	Status	Detected	Restored	OK	Drop	OK	Drop	OK	Drop	OK	Drop
Ethernet0	0	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	1	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	2	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	3	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	4	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	5	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	6	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	7	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	8	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	9	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	10	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	11	N/A	0	0	0	0	0	0	0	0	0	0
Ethernet0	12	N/A	0	0	0	0	0	0	0	0	0	0

Releases 3.2 or later

show qos map dot1p-tc

Displays QoS dot1p to traffic class mapping for all or for a specific name.

Command show qos map dot1p-tc [*name*]

Options *name*—(Optional) QoS map name (up to 32 characters)

Modes EXEC

Usage Use this command to view the QoS dot1p to traffic class mapping for all or for a specific name.

Example

```
sonic# show qos map dot1p-tc
DOT1P-TC-MAP: ROCE
-----
  DOT1P  TC
-----
    0      0
    1      0
    2      0
    3      3
    4      4
    5      0
    6      0
    7      0
-----
```

Releases 3.1 or later

show qos map dscp-tc

Displays QoS DSCP to traffic class mapping for all or for a specific name.

Command show qos map dscp-tc [*name*]

Options *name*—(Optional) QoS map name (up to 32 characters)

Modes EXEC

Usage Use this command to view the QoS DSCP to traffic class mapping for all or for a specific name.

Example

```
sonic# show qos map dscp-tc
DSCP-TC-MAP: ROCE
-----
  DSCP  TC
-----
    0      0
    ...
    4      4
    5      0
-----
```

```
      6      0
...
  23      0
  24      3
  25      0
  26      3
  27      0
...
  47      0
  48      6
  49      0
...
  63      0
-----
sonic#
```

Releases 3.1 or later

show qos map pfc-priority-pg

Displays the PFC priority-to-priority group mapping that is applied on all switch ports.

Command show qos map pfc-priority-pg

Options None

Modes EXEC

Usage This command displays the configured PFC priority-to-priority group mapping. To apply a PFC priority-to-priority group mapping on switch interfaces, use the [qos-map pfc-priority-pg](#) command.

Example

```
sonic# show qos map pfc-priority-pg
-----
PFC-Priority-Priority-Group-MAP: ROCE
-----
PFC Priority PG
-----
  0      0
  1      1
  2      2
  3      3
  4      4
  5      5
  6      6
  7      7
-----
```

Releases 4.2.1 or later

show qos map pfc-priority-queue

Displays QoS priority flow-control (PFC) queue mapping for all or for a specific name.

Command show qos map pfc-priority-queue [*name*]

Options *name*—(Optional) QoS map name (up to 32 characters)

Modes EXEC

Usage Use this command to view the QoS priority flow-control (PFC) queue mapping for all or for a specific name.

Example

```
sonic# show qos map pfc-priority-queue
PFC-Priority-Queue-MAP: ROCE
-----
```

PFC Priority	Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

sonic#

Releases 3.1 or later

show qos map tc-dot1p

Displays QoS traffic class to dot1p mapping for all or for a specific name.

Command show qos map tc-dot1p [*name*]

Options *name*—(Optional) QoS map name (up to 32 characters)

Modes EXEC

Usage Use this command to view the QoS traffic class to dot1p mapping for all or for a specific name.

Example

```
sonic# show qos map tc-dot1p
Traffic-Class-Dot1P-MAP: TC_DOT1P
-----
TC      DOT1P
-----
3       3
4       4
-----
```

Releases 3.1 or later

show qos map tc-dscp

Displays QoS traffic class to DSCP mapping for all or for a specific name.

Command show qos map tc-dscp [*name*]

Options *name*—(Optional) QoS map name (up to 32 characters)

Modes EXEC

Usage Use this command to view the QoS traffic class to DSCP mapping for all or for a specific name.

Example

```
sonic# show qos map tc-dscp
Traffic-Class-DSCP-MAP: TC_DSCP
-----
TC      DSCP
-----
3       26
4       4
-----
sonic#
```

Releases 3.1 or later

show qos map tc-pg

Displays QoS traffic class to priority group mapping for all or for a specific name.

Command show qos map tc-pg [*name*]

Options *name*—(Optional) QoS map name (up to 32 characters)

Modes EXEC

Usage Use this command to view QoS traffic class to priority group mapping for all or for a specific name.

Example

```
sonic# show qos map tc-pg
Traffic-Class-Priority-Group-MAP: ROCE
-----
TC      PG
-----
0       7
1       7
2       7
3       3
4       4
5       7
6       7
7       7
-----
```

Releases 3.1 or later

show qos map tc-queue

Displays QoS traffic class to queue mapping for all or for a specific name.

Command show qos map tc-queue [*name*]

Options *name*—(Optional) QoS map name (up to 32 characters)

Modes EXEC

Usage Use this command to view the QoS traffic class to queue mapping for all or for a specific name.

Example

```
sonic# show qos map tc-queue
Traffic-Class-Queue-MAP: ROCE
-----
TC      Queue
-----
0       0
1       1
2       2
3       3
4       4
5       5
6       6
7       7
-----
```

Releases 3.1 or later

show qos scheduler-policy

Displays QoS scheduler policy information for all or for a specific name.

Command show qos scheduler-policy [*name*]

Options	<i>name</i> —(Optional) QoS map name (up to 32 characters)
Modes	EXEC
Usage	Use this command to view the QoS scheduler policy information for all or for a specific name.
Example	

```
sonic# show qos scheduler-policy
Scheduler Policy: ROCE
    Queue: 0
        type: dwrr
        weight: 50
    Queue: 3
        type: dwrr
        weight: 50
    Queue: 4
        type: dwrr
        weight: 50
    Queue: 6
        type: strict
Scheduler Policy: copp-scheduler-policy
    Queue: 0
        type: wrr
        weight: 1
        meter-type: packets
        pir: 100          Pps
    Queue: 1
        type: wrr
        weight: 1
        meter-type: packets
        pir: 100          Pps
    Queue: 2
        type: wrr
        weight: 2
        meter-type: packets
        pir: 600          Pps
```

Releases	3.1 or later
-----------------	--------------

show qos wred-policy

Displays QoS WRED policy information for all or for a specific name.

Command	show qos wred-policy [<i>name</i>]
Options	<i>name</i> — (Optional) QoS map name (up to 32 characters)
Modes	EXEC
Usage	WRED policies are configured for interface queues. If the QoS map name is not specified, all policies display.
Example	

```
sonic# show qos wred-policy
-----
Policy           : ROCE
-----
ecn              : ecn_green
green-min-threshold : 1048      KBytes
green-max-threshold : 2097      KBytes
green-drop-probability : 5
```

Releases	3.1 or later
-----------------	--------------

show queue

Displays queue counters, watermarks, persistent-watermarks, and breaches.

Command show queue {[wred-ecn] counters {[interface {[phy-intf-name {[queue queue-id]}]} | {CPU {[queue queue-id]}]}]} | {watermark {[unicast {[interface {[phy-intf-name]}]} | {multicast {[interface {[phy-intf-name]}]}]} | CPU | {percentage {[unicast {[interface {[phy-intf-name]}]} | {multicast {[interface {[phy-intf-name]}]}]} | {persistent-watermark {[unicast {[interface {[phy-intf-name]}]} | {multicast {[interface {[phy-intf-name]}]}]} | CPU | {percentage {[unicast {[interface {[phy-intf-name]}]} | {multicast {[interface {[phy-intf-name]}]}]} | {CPU}}}}}}

- Options**
- *phy-intf-name*—Ethernet ID (0 to 255)
 - *queue-id*—(Optional) Queue ID

Modes EXEC

Usage Use this command to view the queue counters, watermarks, persistent-watermarks, and breaches. To clear all counters on a specified interface queue, enter the `clear queue counters interface Ethslot/port[/breakout-port] queue queue-number` command.

i **NOTE:** The `show queue watermark cpu` and `show queue persistent-watermark cpu` commands are not supported on Z9864F-ON switches.

Examples

```
sonic# show queue counters
-----
Port      TxQ  Counter/pkts  Counter/bytes  Drop/pkts  Drop/bytes
-----
Ethernet0  UC0  0            0              0          0
Ethernet0  UC1  0            0              0          0
Ethernet0  UC2  0            0              0          0
Ethernet0  UC3  0            0              0          0
Ethernet0  UC4  0            0              0          0
Ethernet0  UC5  0            0              0          0
Ethernet0  UC6  0            0              0          0
Ethernet0  UC7  0            0              0          0
Ethernet0  MC8  0            0              0          0
Ethernet0  MC9  0            0              0          0
Ethernet0  MC10 0           0              0          0
Ethernet0  MC11 0           0              0          0
Ethernet0  MC12 0           0              0          0
Ethernet0  MC13 0           0              0          0
Ethernet0  MC14 0           0              0          0
Ethernet0  MC15 0           0              0          0
```

```
sonic# show queue watermark unicast
Egress queue watermark per unicast queue:
-----
Port      UC0  UC1  UC2  UC3  UC4  UC5  UC6  UC7
-----
Ethernet0  0    0    0    0    0    0    0    0
Ethernet4  0    0    0    0    0    0    0    0
Ethernet8  0    0    0    0    0    0    0    0
Ethernet12 0    0    0    0    0    0    0    0
Ethernet16 0    0    0    0    0    0    0    0
Ethernet20 0    0    0    0    0    0    0    0
Ethernet24 0    0    0    0    0    0    0    0
```

```
sonic# show queue persistent-watermark multicast
Egress queue persistent watermark per multicast queue:
-----
Port      MC8  MC9  MC10 MC11 MC12 MC13 MC14 MC15
-----
Ethernet0  0    0    0    0    0    0    0    0
Ethernet4  0    0    0    0    0    0    0    0
Ethernet8  0    0    0    0    0    0    0    0
```

```

Ethernet12 0 0 0 0 0 0 0 0 0
Ethernet16 0 0 0 0 0 0 0 0 0
Ethernet20 0 0 0 0 0 0 0 0 0
Ethernet24 0 0 0 0 0 0 0 0 0
Ethernet28 0 0 0 0 0 0 0 0 0

```

```
sonic# show queue wred-ecn counters interface Eth1/56
```

TxQ	WRED Drops/Pkts	ECN Marked/Pkts	ECN Marked/Bytes
UC0	0	0	0
UC1	0	0	0
UC2	0	837922938	107207451904
UC3	390634	0	0
UC4	400000	0	0
UC5	0	0	0
UC6	0	0	0
UC7	0	0	0
UC8	0	0	0
UC9	0	0	0

Releases

3.2 or later

show radius-server

Displays RADIUS server configuration information.

Command show radius-server

Options None

Modes EXEC

Usage Use this command to view the RADIUS server configuration information.

Example

```

sonic# show radius-server
-----
RADIUS Global Configuration
-----
timeout      : 5
auth-type    : pap
key configured : Yes
-----
HOST          AUTH-TYPE KEY-CONFIG AUTH-PORT PRIORITY TIMEOUT RTSMT VRF   SI
-----
1.1.1.1      -           Yes        1812      -      -      -      -      -

```

Releases

3.0 or later

show radius-server dynamic-author

View the dynamic authorization server (DAS) parameters and detailed information.

Command show radius-server dynamic-author [statistics [client {all | ipv4 | ipv6 | host name }]]

Modes EXEC

Usage Use the show radius-server dynamic-author command to view the dynamic authorization server parameters, and the DAS global and per client counters.

Examples

```

sonic# show radius-server dynamic-author
AdminMode..... Enabled
Port..... 1700
Auth Type..... any

```

Global Secret Key.....	Yes
Ignore Server Key.....	Disabled
Ignore Session Key.....	Disabled
CoA Bounce Host Port.....	Accept
CoA Disable Host Port.....	Accept
Client Address	Secret
-----	-----
10.89.108.26	No
1.1.1.1	Yes

Table 13. show radius-server dynamic-author Field Descriptions

Field	Description
Admin Mode	The admin status of DAS on the switch.
Port	UDP port number on which DAS should run.
Auth Type	Type on which DAS should match while processing the requests from DAC.
Global Secret Key	Displays whether global server key is configured or not.
Ignore Server Key	Displays whether server-key that are received in the packet is ignored or not.
Ignore Session Key	Displays whether session-key that are received in the packet is ignored or not.
CoA Bounce Host Port	Displays whether "bounce-host-port" received as part of Cisco AVP in CoA message is accepted or not.
CoA Disable Host Port	Displays whether "disable-host-port" received as part of Cisco AVP in CoA message is accepted or not.
Client Address	This is the DAC Address. It can be IPv4 or IPv6 or DNS Hostname.
Secret	Displays whether per client secret key is configured or not. This takes precedence over the global secret.

View DAS global and per-client counters:

```
sonic# show radius-server dynamic-author statistics
Number of CoA Requests Received..... 5
Number of CoA ACK Responses Sent..... 2
Number of CoA NAK Responses Sent..... 3
Number of CoA Requests Ignored..... 1
Number of CoA Missing/Unsupported Attribute R.. 0
Number of CoA Session Context Not Found Reque.. 2
Number of CoA Invalid Attribute Value Request.. 0
Number of Administratively Prohibited Request.. 0

sonic# show radius-server dynamic-author statistics client all
DAC Address..... 10.89.108.26
Number of CoA Requests Received..... 4
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent..... 4
Number of CoA Requests Ignored..... 0
Number of CoA Missing/Unsupported Attribute Requests.. 0
Number of CoA Session Context Not Found Requests..... 4
Number of CoA Invalid Attribute Value Requests..... 0
Number of Administratively Prohibited Requests..... 0
```

```

DAC Address..... 10.52.139.190
Number of CoA Requests Received..... 3
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent..... 3
Number of CoA Requests Ignored..... 3
Number of CoA Missing/Unsupported Attribute Requests.. 0
Number of CoA Session Context Not Found Requests..... 0
Number of CoA Invalid Attribute Value Requests..... 0
Number of Administratively Prohibited Requests..... 0

sonic# show radius-server dynamic-author statistics client 10.89.108.26

DAC Address..... 10.89.108.26
Number of CoA Requests Received..... 4
Number of CoA ACK Responses Sent..... 0
Number of CoA NAK Responses Sent..... 4
Number of CoA Requests Ignored..... 0
Number of CoA Missing/Unsupported Attribute Requests.. 0
Number of CoA Session Context Not Found Requests..... 4
Number of CoA Invalid Attribute Value Requests..... 0
Number of Administratively Prohibited Requests..... 0

```

Table 14. show radius-server dynamic-author statistics Field Descriptions

Field	Description
Number of CoA Requests Received	Total number of requests received by DAS on the configured UDP port.
Number of CoA ACK Responses Sent	Total number of requests successfully handled by DAS.
Number of CoA NAK Responses Sent	Total number of requests not handled by DAS.
Number of CoA Requests Ignored	Total number of requests ignored by DAS.
Number of CoA Missing or Unsupported Attribute Requests	Total number of requests which does not contain supported session identifier attribute or which contain unsupported attributes by DAS.
Number of CoA Session Context Not Found Requests	Total number of requests which does not have matching session identifier attributes.
Number of CoA Invalid Attribute Value Requests	Total number of requests which contain invalid values of the attributes.
Number of Administratively Prohibited Requests	Total number of requests which DAS do not handle due to admin configuration restrictions.

Releases

4.1.0 or later

show reboot-cause

Displays the cause of the most recent reboot.

Command show reboot-cause

Options None

Modes EXEC

Usage Use this command to view the cause of the most recent reboot.

Example

```

sonic# show reboot-cause
User issued 'reboot' command [User: admin, Time: Wed Dec 2 00:17:16 UTC
2020]

```

Releases	3.1 or later
-----------------	--------------

show route-map

Displays route-map configuration information.

Command	show route-map [rt-map-name]
Options	route-map <i>rt-map-name</i> — (Optional) Route-map name (up to 63 characters)
Modes	EXEC
Usage	Use this command to view the route-map configuration information.
Example	<pre>sonic# show route-map Route map map1: permit, sequence 10 Match clauses: Set clauses: local preference 10 Call clauses: Actions: Exit routemap Route map map2: permit, sequence 2 Match clauses: med 10 Set clauses: Call clauses: Actions: Exit routemap</pre>

Releases	3.0 or later
-----------------	--------------

show running-configuration

Displays the current running configuration on the switch.

Command	show running-configuration
Options	None
Modes	EXEC
Usage	Use different suboptions available in the show running-configuration command to only display the configuration of the specific features.
Example	<pre>sonic# show running-configuration ! ip load-share hash ipv4 ipv4-dst-ip ip load-share hash ipv4 ipv4-src-ip ip load-share hash ipv4 ipv4-ip-proto ip load-share hash ipv4 ipv4-14-src-port ip load-share hash ipv4 ipv4-14-dst-port ip load-share hash ipv6 ipv6-dst-ip ip load-share hash ipv6 ipv6-src-ip ip load-share hash ipv6 ipv6-next-hdr ip load-share hash ipv6 ipv6-14-src-port ip load-share hash ipv6 ipv6-14-dst-port hostname sonic mac address-table aging-time 600 kdump enable kdump memory 0M-2G:256M,2G-4G:256M,4G-8G:384M,8G-:448M kdump num-dumps 3</pre>

```

core enable
factory default profile l3 confirm
ip arp timeout 1800
ipv6 nd cache expire 1800
!
!
qos scheduler-policy copp-scheduler-policy
!
queue 0
    type wrr
    weight 1
!
queue 1
    meter-type packets
    pir 100
    type wrr
    weight 1
!
queue 2
    meter-type packets
    pir 600
    type wrr
    weight 2
--more--

```

Releases 3.1 or later

show running-configuration bfd

Displays all BFD configurations.

Command	show running-configuration bfd
Options	None
Modes	EXEC
Usage	Use this command to view all BFD configurations.

Example

```

sonic# show running-configuration bfd
!
bfd
    peer 192.168.2.1 interface Ethernet0
        detect-multiplier 5
        echo-interval 200
        echo-mode
        receive-interval 200
        transmit-interval 200
    !
    peer 192.168.2.1 multihop local-address 192.168.2.2
        detect-multiplier 4
        receive-interval 150
        transmit-interval 150
    !

```

Releases 3.1 or later

show running-configuration bgp

Displays the current BGP configurations.

Command	show running-configuration bgp [vrf vrf-name-opt]
Options	vrf-name-opt—(Optional) VRF name prefixed by Vrf
Command mode	EXEC

Usage Use this command to view the current BGP configurations.

Example

```
sonic# show running-configuration bgp
!
router bgp 1 vrf Vrf1
router-id 1.0.1.1
timers 60 180
!
address-family ipv4 unicast
    redistribute connected
    maximum-paths 16
    maximum-paths ibgp 1
!
address-family ipv6 unicast
    redistribute connected
    maximum-paths 1
    maximum-paths ibgp 1
!
address-family l2vpn evpn
    advertise ipv4 unicast
    advertise ipv6 unicast
    rd 100:1
    route-target both 101:1
```

Releases 3.1 or later

show running-configuration bgp as-path-access-list

Displays the current BGP AS path access-list configuration.

Command show running-configuration bgp as-path-access-list [*aspath-list-name*]

Options *aspath-list-name*—(Optional) AS path list name

Command mode EXEC

Usage Use this command to view the current BGP AS path access-list configuration.

Example

```
sonic# show running-configuration bgp as-path-access-list
!
bgp as-path-list as_path seq 1 permit "^65500$"
bgp as-path-list as_path seq 2 deny "_100_"
```

Releases 3.1 or later

show running-configuration bgp community-list

Displays the current BGP community-list configuration.

Command show running-configuration bgp community-list [*community-list-name*]

Options *community-list-name*—(Optional) Community list name

Command mode EXEC

Usage Use this command to view the current BGP community-list configuration.

Example

```
sonic# show running-configuration bgp community-list
!
bgp community-list standard bgp_std_com permit 11:22 local-AS
```

Releases 3.1 or later

show running-configuration bgp extcommunity-list

Displays the current BGP extended community-list configuration.

Command show running-configuration bgp extcommunity-list [*extcommunity-list-name*]

Options *extcommunity-list-name*—(Optional) Extended community-list name

Command mode EXEC

Usage Use this command to view the current BGP extended community-list configuration.

Example

```
sonic# show running-configuration bgp extcommunity-list
!
bgp extcommunity-list standard bgp_ext_com permit rt 1.1.1.1:100
```

Releases 3.1 or later

show running-configuration bgp neighbor

Displays the current BGP neighbor configurations.

Command show running-configuration bgp neighbor vrf {*vrf-name* {[*ip*] | {[interface Ethernet | PortChannel | Vlan]}}} }

Options

- *vrf-name*—VRF name prefixed by Vrf
- *ip*—(Optional) IP address in A.B.C.D or A::B format

Command mode EXEC

Usage Use this command to view the current BGP neighbor configurations.

Example

```
sonic# show running-configuration bgp neighbor vrf Vrf-1
!
neighbor interface Eth1/45
peer-group leaf
!
neighbor interface Eth1/46
peer-group leaf
```

Releases 3.1 or later

show running-configuration bgp peer-group

Displays the current BGP peer-group configurations.

Command show running-configuration bgp peer-group vrf {*vrf-name* [*peer-group-name*] }

Options

- *vrf-name*—VRF name prefixed by Vrf
- *peer-group-name*—(Optional) Peer-group name

Command mode EXEC

Usage Use this command to view the current BGP peer-group configurations.

Example

```
sonic# show running-configuration bgp peer-group vrf default
!
peer-group leaf
remote-as external
timers connect 30
advertisement-interval 0
!
address-family ipv4 unicast
```

```
    activate
    send-community both
!
address-family ipv6 unicast
    activate
    send-community both
```

Releases	3.1 or later
-----------------	--------------

show running-configuration class-map

Displays the running configuration for class-maps.

Command	show running-configuration class-map [<i>show-fbs-class-name</i>]
Options	<i>show-fbs-class-name</i> —(Optional) Class name.
Command mode	EXEC
Usage	Class-map name is optional. If the class-map name is provided, it displays all running configuration of all class-maps configured.

Example

```
sonic# show running-configuration class-map
!
class-map class-oob-arp match-type fields match-all
match ethertype arp
!
class-map class-oob-dhcp-client match-type fields match-all
match ethertype ip
match ip protocol udp
match destination-port eq 68
!
class-map class-oob-dhcp-server match-type fields match-all
match ethertype ip
match ip protocol udp
match destination-port eq 67
!
class-map class-oob-ip-multicast match-type fields match-all
match ethertype ip
match destination-address ip 224.0.0.0/4
!
class-map class-oob-ipv6-multicast match-type fields match-all
match ethertype 0x86DD
match destination-address ipv6 ff00::/8
!
class-map copp-system-arp match-type copp
match protocol arp_req
--more--
```

Releases	3.1 or later
-----------------	--------------

show running-configuration dropcounters

Displays dropcounters configuration.

Command	show running-configuration dropcounters
Options	None
Modes	EXEC
Usage	None
Examples	<pre>sonic# show running-configuration dropcounters !</pre>

```
dropcounters drop
  no enable
  add-reason any
!
dropcounters drop1
  no enable
  alias counter
  add-reason mpls
```

Releases 4.0 or later

show running-configuration hardware

Displays the current hardware configuration.

Command show running-configuration hardware

Options None

Command mode EXEC

Usage Use this command to view the current hardware configuration.

Example

```
sonic# show running-configuration hardware
!
hardware
!
access-list
  counters per-entry
!
tcam
```

Releases 3.1 or later

show running-configuration hardware access-list

Displays the current hardware ACL configuration.

Command show running-configuration hardware access-list

Options None

Command mode EXEC

Usage None

Example

```
sonic# show running-configuration hardware access-list
!
access-list
  counters per-entry
```

Releases 3.1 or later

show running-configuration hardware tcam

Displays the current hardware TCAM configuration.

Command show running-configuration hardware tcam

Options None

Modes EXEC

Usage Use this command to view the current hardware TCAM configuration.

Examples

```
sonic# show running-configuration hardware tcam
!
tcam
ip-acl ingress key-profile pac
monitoring-fbs ingress key-profile ip
forwarding-fbs ingress key-profile ip
```

Releases 4.0 or later

show running-configuration igmp

Displays all IGMP configurations.

Command show running-configuration igmp

Options None

Modes EXEC

Usage Use this command to view all IGMP configurations.

Examples

```
sonic# show running-configuration igmp
interface Vlan301
  ip igmp
!
interface Vlan302
  ip igmp
!
interface Vlan303
  ip igmp
!
interface Vlan304
  ip igmp
!
interface Vlan1007
  ip igmp
  ip igmp snooping
!
interface Vlan1008
  ip igmp
!
```

Releases 4.1.0 or later

show running-configuration interface

Displays the current running configuration for all interfaces.

Command show running-configuration interface {[port] | {[Eth [iface_num]]} | {[Ethernet [iface_num]]}}}

Options

- *port* — Ethernet interface number
- *iface_num* — Ethernet interface slot and port

Modes EXEC

Usage Use this command to view the current running configuration for all interfaces.

Example

```
sonic# show running-configuration interface
!
interface Ethernet0
  mtu 9100
```

```

speed 100000
shutdown
!
interface Ethernet4
mtu 9100
speed 100000
shutdown
!
interface Ethernet8
mtu 9100
speed 100000
shutdown
!
interface Ethernet12
mtu 9100
speed 100000
shutdown
!
interface Ethernet16
mtu 9100
speed 100000
shutdown
!--more--

```

Releases

3.1 or later

show running-configuration interface Loopback

Displays the current running configuration for all Loopback interfaces or for a specific interface.

Commandshow running-configuration interface Loopback [*lo-id*]**Options***lo-id*—(Optional) Loopback interface ID**Modes**

EXEC

Usage

Use this command to view the current running configuration for all Loopback interfaces or for a specific interface.

Example

```

sonic# show running-configuration interface Loopback
!
interface Loopback 0
ip address 1.1.1.1/32
!
interface Loopback 1
ip address 12.12.12.12/32

```

```

sonic# show running-configuration interface loopback 11
!
interface Loopback 11
shutdown

```

Releases

3.1 or later

show running-configuration interface Management

Displays the running configuration for all Management interfaces or for a specific interface.

Commandshow running-configuration interface Management [*mgmt-if-id*]**Options***mgmt-if-id*—(Optional) Management interface ID**Modes**

EXEC

Usage

None

Example

```
sonic# show running-configuration interface Management
!
interface Management 0
  description Management0
  mtu 1500
  autoneg on
  speed 1000
```

Releases

3.1 or later

show running-configuration interface PortChannel

Displays the current running configuration for all port channel interfaces or for a specific interface.

Command

```
show running-configuration interface PortChannel [po-id]
```

Options

po-id—(Optional) Specify the port channel ID.

Mode

EXEC

Usage

Use this command to view the current running configuration for all port channel interfaces or for a specific interface.

Example

```
sonic# show running-configuration interface PortChannel
!
interface PortChannel 11
  switchport trunk allowed Vlan add 1001-1016
  mtu 9100
  no shutdown
!
interface PortChannel 31 fast_rate
  switchport access Vlan 2501
  switchport trunk allowed Vlan add 100-162,4093
  no shutdown
!
interface PortChannel 32 fast_rate
  switchport access Vlan 2501
  switchport trunk allowed Vlan add 100-162,4093
  no shutdown
!
interface PortChannel 41
  switchport trunk allowed Vlan add 100-162,4093
  no shutdown
!
interface PortChannel 42
  switchport trunk allowed Vlan add 100-162,4093
  no shutdown
!
--more--
```

Releases

3.1 or later

show running-configuration interface Vlan

Displays the current running configuration for all VLAN interfaces or for a specific interface.

Command

```
show running-configuration interface Vlan [vlan-id]
```

Options

vlan-id—(Optional) Specify the VLAN ID (1 to 4094).

Modes

EXEC

Usage

Use this command to view the current running configuration for all VLAN interfaces or for a specific interface.

Example

```
sonic# show running-configuration interface Vlan
!
interface Vlan100
    ip address 100.100.0.2/16
!
interface Vlan101
    ip address 100.101.0.2/16
!
interface Vlan102
    ip address 100.102.0.2/16
!
interface Vlan103
    ip address 100.103.0.2/16
!
interface Vlan104
    ip address 100.104.0.2/16
!
interface Vlan105
    ip address 100.105.0.2/16
!
interface Vlan106
    ip address 100.106.0.2/16
!
interface Vlan107
    ip address 100.107.0.2/16
--more--
```

Releases

3.1 or later

show running-configuration interface vxlan

Displays the current VXLAN configuration.

Command show running-configuration interface vxlan

Options None

Modes EXEC

Usage Use this command to view the current VXLAN configuration.

Example

```
sonic# show running-configuration interface vxlan
!
interface vxlan vtep-leaf
    source-ip 12.12.12.12
    map vni 1001 vlan 1001
    map vni 1002 vlan 1002
    map vni 1003 vlan 1003
    map vni 1004 vlan 1004
    map vni 1005 vlan 1005
    map vni 1006 vlan 1006
    map vni 1007 vlan 1007
    map vni 1008 vlan 1008
    map vni 1009 vlan 1009
    map vni 1010 vlan 1010
    map vni 1011 vlan 1011
    map vni 1012 vlan 1012
    map vni 1013 vlan 1013
    map vni 1014 vlan 1014
    map vni 1015 vlan 1015
    map vni 1016 vlan 1016
    map vni 1017 vlan 1017
    map vni 1018 vlan 1018
    map vni 1019 vlan 1019
    map vni 102000 vlan 2000
    map vni 1020 vlan 1020
--more--
```

Releases	3.1 or later
-----------------	--------------

show running-configuration ip access-list

Displays the current IPv4 ACL configuration.

Command show running-configuration ip access-list [*access-list-name*]

Options *access-list-name*—(Optional) Access-list name (up to 63 characters)

Command mode EXEC

Usage If an ACL name is not specified, all IPv4 ACLs are displayed.

Example

```
sonic# show running-configuration ip access-list ipacl
  seq 10 permit ip host 10.1.1.1 host 20.1.1.1
  seq 20 permit ip host 10.1.1.2 host 20.1.1.2
  seq 30 permit ip host 10.1.1.3 host 20.1.1.3
  seq 40 permit ip host 10.1.1.4 host 20.1.1.4
```

Releases	3.1 or later
-----------------	--------------

show running-configuration ip prefix-list

Displays the current IPv4 prefix-list configuration.

Command show running-configuration ip prefix-list [*prefix-list-name*]

Options *prefix-list-name*—(Optional) Specify the prefix-list name.

Command mode EXEC

Usage Use this command to view the current IPv4 prefix-list configuration.

Example

```
sonic# show ip prefix-list
IP prefix list match host routes:
    seq 1 permit 0.0.0.0/0 ge 32 le 32
```

Releases	3.1 or later
-----------------	--------------

show running-configuration ipv6 access-list

Displays the current IPv6 configuration.

Command show running-configuration ipv6 access-list [*access-list-name*]

Options *access-list-name*—(Optional) Access-list name (up to 63 characters)

Command mode EXEC

Usage If an ACL name is not specified, all IPv6 ACLs are displayed.

Example

```
sonic# show running-configuration ipv6 access-list ipv6acl
  seq 100 permit ipv6 host abcd::1 host bcde::1
  seq 200 permit tcp host abcd::2 host bcde::2
  seq 300 permit udp host abcd::3 host bcde::3
```

Releases	3.1 or later
-----------------	--------------

show running-configuration ipv6 prefix-list

Displays the current IPv6 prefix-list configuration.

Command show running-configuration ipv6 prefix-list [*prefix-list-name*]

Options *prefix-list-name*—(Optional) Prefix-list name

Command mode EXEC

Usage None

Example

```
sonic# show running-configuration ipv6 prefix-list prefix5
!
ipv6 prefix-list prefix5 seq 1 permit 2000::00/64
```

Releases 3.1 or later

show running-configuration line vty

Displays the current session configuration.

Command show running-configuration line vty

Options None

Command mode EXEC

Usage Use this command to view the terminal configuration.

Example

```
sonic# show running-configuration line vty
!
line vty
service-policy type qos in oob-qos-policy
```

Releases 3.1 or later

show running-configuration link state tracking

Displays the current link state tracking configuration.

Command show running-configuration link state tracking [*show-runn-grp-name*]

Options *show-runn-grp-name*—(Optional) Group name

Modes EXEC

Usage Use this command to view the current link state tracking configuration.

Example

```
sonic# show running-configuration link state tracking
!
link state track LinkStateTrackLeaf
    timeout 180
    downstream all-evpn-es
```

Releases 3.1 or later

show running-configuration mac access-list

Displays the running configuration of the MAC access-list.

Command show running-configuration mac access-list [*access-list-name*]

Options *access-list-name*—(Optional) Access-list name (up to 63 characters)

Command mode EXEC

Usage If an ACL name is not specified, all MAC ACLs are displayed.

Example

```
sonic# show running-configuration mac access-list macacl
  seq 10 permit host 00:00:10:00:00:01 host 00:00:20:00:00:01
  seq 20 permit host 00:00:10:00:00:02 host 00:00:20:00:00:02
  seq 30 permit host 00:00:10:00:00:03 host 00:00:20:00:00:03
  seq 40 permit host 00:00:10:00:00:04 host 00:00:20:00:00:04
```

Releases 3.1 or later

show running-configuration mclag

Displays the running configuration of the MLAG domain.

Command show running-configuration mclag

Options None

Modes EXEC

Usage Use this command to view the running configuration of the MLAG domain.

Examples

```
sonic# show running-configuration mclag
mclag domain 89
  source-ip 1.1.1.1
  peer-ip 1.1.1.2
  peer-link PortChannel2
  keepalive-interval 1
  session-timeout 30
```

Releases 3.2 or later

show running-configuration mirror-session

Displays the current mirror-session information.

Command show running-configuration mirror-session

Options None

Modes EXEC

Usage Use this command to view the current mirror-session information.

Example

```
sonic# show running-configuration mirror-session
!
mirror-session test
destination Ethernet0 source Ethernet24 direction rx
```

Releases 3.1 or later

show running-configuration nat

Displays all NAT configurations.

Command show running-configuration nat

Options None

Command mode EXEC

Usage Use this command to view all NAT configurations.

Example

```
sonic# show running-configuration nat
!
nat
enable
timeout 600
tcp-timeout 86400
udp-timeout 300
static udp 192.168.1.12 20001 80.0.0.0 30001 snat
```

Releases 3.1 or later

show running-configuration ospf

Displays all OSPFv2 router configurations.

Command show running-configuration ospf

Options None

Modes EXEC

Usage Use this command to view all OSPFv2 router configurations.

Example

```
sonic# show running-configuration ospf
!
router ospf
  ospf router-id 2.2.2.2
  redistribute static
  redistribute connected
  area 0.0.0.0
  area 0.0.0.0 range 100.3.1.0/24
  area 0.0.0.0 range 100.1.0.0/16
```

Releases 3.1 or later

show running-configuration ospf interface

Displays all OSPFv2 interface configurations.

Command show running-configuration ospf interface

Options None

Modes EXEC

Usage Use this command to view all OSPFv2 interface configurations.

Examples

```
sonic# show running-configuration ospf interface
interface Ethernet67
  mtu 9100
  speed 25000
  no shutdown
```

```

ip address 10.10.3.1/24
ip ospf area 0.0.0.1
ip ospf bfd
ip ospf cost 180
ip ospf priority 10
!
interface Vlan2
ip address 10.10.4.1/24
ip ospf area 0.0.0.1
ip ospf bfd
ip ospf cost 180
ip ospf priority 10
!
interface Vlan3
ip address 10.10.5.1/24
ip ospf area 0.0.0.1
ip ospf bfd
ip ospf cost 180
ip ospf priority 10
!
interface PortChannel 1
no shutdown
ip address 10.10.6.1/24
ip ospf area 0.0.0.1
ip ospf bfd
ip ospf cost 180
ip ospf priority 10
!
```

Releases 4.0 or later

show running-configuration pbf next-hop-group

Displays the current PBF next-hop group configuration.

Command show running-configuration pbf next-hop-group [*show-fbs-group-name*]

Options *show-fbs-group-name*—(Optional) FBS group name

Modes EXEC

Usage None

Examples

```

sonic# show running-configuration pbf next-hop-group
!
pbf next-hop-group test type ip
entry 1 next-hop 100.1.1.1
entry 2 next-hop 101.1.1.1
entry 3 next-hop 102.1.1.1
entry 4 next-hop 103.1.1.1
!
```

Releases 3.2 or later

show running-configuration pbf replication-group

Displays current PBF replication group configuration.

Command show running-configuration pbf replication-group [*show-repl-group-name*]

Options *show-repl-group-name*—(Optional) Replication group name (up to 63 characters)

Modes EXEC

Usage None

Examples

```
sonic# show running-configuration pbf replication-group
!
pbf replication-group pbf_repl type ip
  entry 1 next-hop 10.0.0.1
  entry 2 next-hop 10.0.0.2
!
```

Releases

4.0 or later

show running-configuration policy-map

Displays the running configuration of policy-maps.

Command

```
show running-configuration policy-map [show-fbs-policy-name]
```

Options

show-fbs-policy-name — (Optional) Policy name

Modes

EXEC

Usage

If you do not specify a policy-map name, all policy-maps configured display.

Example

```
sonic# show running-configuration policy-map policy_vrf
policy-map policy_vrf type forwarding
  class class_permit_ipv6 priority 10
    set ipv6 next-hop 1211::2 priority 20
    set ipv6 next-hop 1212::2 vrf Vrf-BLUE priority 30
  class class_permit_ip priority 10
    set ip next-hop 12.12.1.2 vrf default priority 30
    set ip next-hop 12.12.2.2 vrf Vrf-BLUE priority 20
    set ip next-hop 12.12.1.2 priority 10
```

Releases

3.1 or later

show running-configuration route-map

Displays the current route-map configuration.

Command

```
show running-configuration route-map [rt-map-name [seq-nu]]
```

Options

- *rt-map-name*—(Optional) Route-map name
- *seq-nu*—(Optional) Sequence number

Command mode

EXEC

Usage

Use this command to view the current route-map configuration.

Example

```
sonic# show running-configuration route-map
!
route-map test permit 1
  match ip address prefix-list test5
```

Releases

3.1 or later

show running-configuration spanning-tree

Displays the current spanning-tree configuration.

Command

```
show running-configuration spanning-tree
```

Options

None

Modes EXEC

Usage None

Example

```
sonic# show running-configuration spanning-tree
spanning-tree mode pvst
spanning-tree edge-port bpdufilter default
spanning-tree forward-time 4
spanning-tree guard root timeout 5
spanning-tree hello-time 1
spanning-tree max-age 40
spanning-tree priority 61440
!
no spanning-tree vlan 101
!
spanning-tree vlan 100 forward-time 5
spanning-tree vlan 100 hello-time 3
!
spanning-tree vlan 101 forward-time 15
!
interface Ethernet0
    spanning-tree bpdufilter enable
    spanning-tree vlan 100 cost 1
!
interface PortChannel10
    no spanning-tree enable
    no spanning-tree portfast
    spanning-tree cost 2
    spanning-tree vlan 100 cost 1
```

Releases 3.1 or later

show running-configuration subinterface

Displays the subinterface configuration.

Command show running-configuration subinterface {[*subifname*] | {[PortChannel [*pch_num*]}}}]

Options

- *subifname*—(Optional) Ethernet subinterface name
- *pch_num*—(Optional) PortChannel ID

Modes EXEC

Usage Use this command to view the subinterface configuration.

Examples

```
sonic# show running-configuration subinterface
!
interface Ethernet0.101
no shutdown
!
interface PortChannel100.101
no shutdown
```

Releases 3.2 or later

show running-configuration tam

Displays the current TAM configuration.

Command show running-configuration tam

Options None

Modes EXEC

Usage None

Example

```
sonic# show running-configuration tam
!
!
tam
  switch-id 3232
  enterprise-id 434
  collector c1 ip 1.1.1.1 port 1111 protocol UDP
  sampler s1 rate 1
  sampler s2 rate 655
  sampler s4 rate 65550
  sampler s5 rate 999999999
  flow-group f1 src-ip 10.1.1.10/24 dst-ip 30.1.1.10/24 protocol TCP 14-src-port 8080
  priority 100
  flow-group f2 src-ip 10.1.1.10/32 dst-ip 30.1.1.10/32 protocol UDP priority 100
!
  drop-monitor
    aging-interval 23
!
  ifa
    session ifa1 flowgroup f1 collector c1 node-type EGRESS
```

Releases 3.1 or later

show running-configuration vrf

Displays VRF configuration information.

Command show running-configuration vrf *vrf-name*

Options *vrf-name*—VRF name

Modes EXEC

Usage Use this command to view VRF configuration information.

Examples

```
sonic# show running-configuration vrf Vrf001
!
ip vrf Vrf001
!
interface Vlan1
description "L3 Vlan 1 in VRF Vrf001"
neigh-suppress
no autostate
ip vrf forwarding Vrf001
ip anycast-address 172.16.0.254/24
ipv6 anycast-address 2001:172:16:0::254/64
ip dhcp-relay 201.1.1.253 vrf Vrf001
ip dhcp-relay source-interface Loopback101
ip dhcp-relay link-select
!
interface Vlan2
description "L3 Vlan 2 in VRF Vrf001"
neigh-suppress
no autostate
ip vrf forwarding Vrf001
ip anycast-address 172.16.1.254/24
ipv6 anycast-address 2001:172:16:1::254/64
ip dhcp-relay 201.1.1.253 vrf Vrf001
ip dhcp-relay source-interface Loopback101
ip dhcp-relay link-select
--more--
```

Releases 3.2 or later

show service-policy

Displays all global service policy information that is configured on the switch or for a specific policy type.

Command `show service-policy {Switch | CtrlPlane} [type {qos | monitoring | forwarding | copp | acl-copp}]`

- Options**
- `type`—(Optional) Service policy type
 - `qos`—(Optional) QoS service policy type
 - `monitoring`—(Optional) Monitoring service policy type
 - `forwarding`—(Optional) Forwarding service policy type
 - `copp`—(Optional) CoPP service policy type

Modes EXEC

Usage Use this command to view all global service policy information that is configured on the switch or for a specific policy type.

Example

```
sonic# show service-policy Switch
Switch
  Policy policy_vrf type forwarding at ingress
    Description:
      Flow class_permit_ipv6 at priority 10 (Inactive)
        Description:
          set ipv6 nexthop 1211::2 priority 20
          set ipv6 nexthop 1212::2 vrf Vrf-BLUE priority 30
          Packet matches: 0 frames 0 bytes
      Flow class_permit_ip at priority 10 (Inactive)
        Description:
          set ip nexthop 12.12.1.2 vrf default priority 30
          set ip nexthop 12.12.2.2 vrf Vrf-BLUE priority 20
          set ip nexthop 12.12.1.2 priority 10
          Packet matches: 0 frames 0 bytes
```

Releases 3.2 or later

show service-policy interface

Displays service policies for all interfaces or for a specific interface.

Command `show service-policy interface {eth-if-id | po-if-id | vlan-if-id | eth-sub-if-id | po-sub-if-id | CPU} [type {qos | monitoring | forwarding | copp | acl-copp}]`

- Options**
- `eth-if-id`—Ethernet ID (0 to 255)
 - `po-if-id`—Port channel interface ID (1 to 128)
 - `vlan-if-id`—VLAN ID (1 to 4094)
 - `eth-sub-if-id`—Ethernet subinterface ID
 - `po-sub-if-id`—PortChannel subinterface ID

Modes EXEC

Usage Policy-map type is optional. If type is not specified, all policies applied to this given interface display. If type is also provided, only corresponding type policies applied on the given interface display.

Example

```
sonic# show service-policy interface Vlan 100
Vlan100
  Policy policy_mirror type monitoring at ingress
    Description:
      Flow class1 at priority 10 (Active)
        Description:
          Packet matches: 0 frames 0 bytes
  Policy policy_vrf type forwarding at ingress
    Description:
      Flow class_permit_ipv6 at priority 10 (Inactive)
        Description:
```

```

set ipv6 nexthop 1211::2 priority 20
set ipv6 nexthop 1212::2 vrf Vrf-BLUE priority 30
Packet matches: 0 frames 0 bytes
Flow class_permit_ip at priority 10 (Active)
Description:
set ip nexthop 12.12.1.2 vrf default priority 30
set ip nexthop 12.12.2.2 vrf Vrf-BLUE priority 20
set ip nexthop 12.12.1.2 priority 10
Packet matches: 0 frames 0 bytes
Policy policy_qos type qos at egress
Description:
Flow class_permit_ipv6 at priority 10 (Inactive)
Description:
police: cir 300000000 cbs 300000000 pir 300000000 pbs 300000000 (Active)
    type bytes mode color-blind
    operational cir 0 cbs 0 pir 0 pbs 0
    green 0 packets 0 bytes action forward
    yellow 0 packets 0 bytes action forward
    red 0 packets 0 bytes action drop
Packet matches: 0 frames 0 bytes
Flow class_permit_ip at priority 10 (Inactive)
Description:
police: cir 300000000 cbs 300000000 pir 300000000 pbs 300000000 (Active)
    type bytes mode color-blind
    operational cir 0 cbs 0 pir 0 pbs 0
    green 0 packets 0 bytes action forward
    yellow 0 packets 0 bytes action forward
    red 0 packets 0 bytes action drop
Packet matches: 0 frames 0 bytes

```

Releases

3.2 or later

show service-policy policy-map

Displays all service policies or for a specific policy.

Command	<code>show service-policy policy-map <i>fbs-policy-name</i> {[{interface {<i>eth-if-id</i> <i>po-if-id</i> <i>vlan-if-id</i> <i>eth-sub-if-id</i> <i>po-sub-if-id</i> CPU}}] [Switch] [CtrlPlane]}</code>
Options	<ul style="list-style-type: none"> • <i>fbs-policy-name</i> — Flow-based services policy name (up to 63 characters) • <i>eth-if-id</i> — (Optional) Ethernet interface ID (0 to 255) • <i>po-if-id</i> — (Optional) Port channel interface ID (1 to 128) • <i>vlan-if-id</i> — (Optional) VLAN interface ID (1 to 4094) • <i>eth-sub-if-id</i> — (Optional) Ethernet subinterface ID • <i>po-sub-if-id</i> — (Optional) PortChannel subinterface ID

Modes

EXEC

Usage

Policy-map interface is optional. If interface is not specified, all services applied interfaces information for given policy. If interface is also specified, service applied information for given policy name and given interface display.

Example

```

sonic# show service-policy policy-map policy_vrf
Vlan100
    Policy policy_vrf type forwarding at ingress
    Description:
        Flow class_permit_ipv6 at priority 10 (Inactive)
        Description:
            set ipv6 nexthop 1211::2 priority 20
            set ipv6 nexthop 1212::2 vrf Vrf-BLUE priority 30
            Packet matches: 0 frames 0 bytes
        Flow class_permit_ip at priority 10 (Inactive)
        Description:
            set ip nexthop 12.12.1.2 vrf default priority 30
            set ip nexthop 12.12.2.2 vrf Vrf-BLUE priority 20
            set ip nexthop 12.12.1.2 priority 10
            Packet matches: 0 frames 0 bytes
    Switch
        Policy policy_vrf type forwarding at ingress
        Description:
            Flow class_permit_ipv6 at priority 10 (Inactive)

```

```

Description:
set ipv6 nexthop 1211::2 priority 20
set ipv6 nexthop 1212::2 vrf Vrf-BLUE priority 30
Packet matches: 0 frames 0 bytes
Flow class permit_ip at priority 10 (Inactive)
Description:
set ip nexthop 12.12.1.2 vrf default priority 30
set ip nexthop 12.12.2.2 vrf Vrf-BLUE priority 20
set ip nexthop 12.12.1.2 priority 10
Packet matches: 0 frames 0 bytes

```

Releases

3.2 or later

show service-policy summary

Displays a summary of all applied service policies, by interface, or by service policy type.

Command show service-policy summary {{[interface {eth-if-id | po-if-id | vlan-if-id | eth-sub-if-id | po-sub-if-id | CPU}]] | [Switch] | [CtrlPlane]]} [type {qos | monitoring | forwarding | copp | acl-copp}]}

Options

- *eth-if-id* — (Optional) Ethernet ID (0 to 255)
- *po-if-id* — (Optional) Port channel ID (1 to 128)
- *vlan-if-id* — (Optional) VLAN ID (1 to 4094)
- *eth-sub-if-id* — (Optional) Ethernet subinterface ID
- *po-sub-if-id* — (Optional) PortChannel subinterface ID

Modes

EXEC

Usage

Interface is optional. If interface is not specified, all service applied interfaces and their policy information display. If interface is specified, service applied policy information for given interface display. If interface is Switch, global/Switch level service policies display.

Example

```

sonic# show service-policy summary
Vlan100
    monitoring policy policy_mirror at ingress
    forwarding policy policy_vrf at ingress
    qos policy policy_qos at egress
Switch
    forwarding policy policy_vrf at ingress
CtrlPlane
    qos policy oob-qos-policy at ingress

```

Releases

3.2 or later

show sflow

Displays global sFlow configuration information.

Command show sflow

Options None

Modes EXEC

Usage Use this command to show global sFlow configuration.

Example

```

sonic# show sflow
-----
Global sFlow Information
-----
    admin state:          down
    polling-interval:     default

```

```
agent-id:           default
sampling-rate:     256
configured collectors: 0
```

Releases 3.0 or later

show sflow interface

Displays sFlow interface configuration information.

Command show sflow interface

Options None

Modes EXEC

Usage Use this command to show the interface sFlow configuration.

Example

```
sonic# show sflow interface
-----
sFlow interface configurations
Interface          Admin State      Sampling Rate
Ethernet0          up               4000
Ethernet1          up               4000
Ethernet2          up               4000
Ethernet3          up               4000
Ethernet4          up               4000
Ethernet5          up               4000
Ethernet6          up               4000
Ethernet7          up               4000
Ethernet8          up               4000
Ethernet9          up               4000
Ethernet10         up               4000
Ethernet11         up               4000
Ethernet12         up               4000
Ethernet13         up               4000
Ethernet14         up               4000
Ethernet15         up               4000
Ethernet16         up               4000
Ethernet17         up               4000
Ethernet18         up               4000
Ethernet19         up               4000
Ethernet20         up               4000
Ethernet21         up               4000
Ethernet22         up               4000
Ethernet23         up               4000
Ethernet24         up               4000
Ethernet25         up               4000
Ethernet26         up               4000
Ethernet27         up               4000
Ethernet28         up               4000
Ethernet29         up               4000
```

Releases 3.0 or later

show snmp counters

Displays global SNMP counters statistics.

Command show snmp counters

Options None

Modes EXEC

Usage Use this command to view the global SNMP counters statistics.

Example

```
sonic# show snmp counters
37 SNMP packets input
0 Bad SNMP version errors
4 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
24 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
28 Get-next PDUs
0 Set-request PDUs
78 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
24 Response PDUs
13 Trap PDUs
```

Releases

3.1 or later

show snmp-server

Displays global SNMP server information.

Command show snmp-server**Options** None**Modes** EXEC**Usage** Use this command to view simple network management protocol (SNMP) server information including the physical location of the switch, the organization responsible for the network, SNMP engine identification, trap status, and the agent addresses, if configured. SNMP engine identification is derived from the device MAC address on an initial boot.**Example**

```
sonic# show snmp-server

Location      : "Santa Clara"
Contact       : "Dell"
EngineID      : 80:00:01:37:03:54:bf:64:c7:d7:c2
Traps         : enable

Agent Addresses:

          IP Address      UDP Port      Interface
----- 10.0.0.1           161
```

Releases

3.0 or later

show snmp-server community

Displays the configured SNMP communities.

Command show snmp-server community**Options** None**Modes** EXEC**Usage** Use this command to view the SNMP communities configured on the switch and the community group association, if configured. Communities are used by SNMPv2 protocol to access the switch.

Example

```
sonic# show snmp-server community
Community Name          Group Name
-----
comm1                  group-lab
comm2                  None
```

Releases

3.0 or later

show snmp-server group

Displays the configured SNMP groups.

Command show snmp-server group

Options None

Modes EXEC

Usage Use this command to view the SNMP groups configured on the switch. The model and security information indicate the SNMP protocol and security level used to access the system via the group. View names indicate the view that a group provides read, write or trap access to.

Example

```
sonic# show snmp-server group
Group Name      Model: Security      Read View     Write View     Notify View
-----
group-floor1    v2c: no-auth-no-priv  ro_view       wr_view       None
group-floor2    v3 : auth-priv        r_view        None         None
group-lab       v2c: no-auth-no-priv  None          None         None
```

Releases

3.0 or later

show snmp-server host

Displays the configured SNMP hosts.

Command show snmp-server host

Options None

Modes EXEC

Usage Use this command to view the SNMP hosts to which the trap or inform messages are sent by the SNMP agent. Timeout (T-out) indicates the number of seconds before the traps or informs time-out when sending to a host. Retries indicate the number of times the traps or informs are sent after timing out. The VRF and source interface from which notifications are sent are also displayed.

Example

```
sonic# show snmp-server host
Target Address  Port      Type   Community  Ver   T-Out  Retries  VRF  Source-Interface
-----
100.94.58.239  162      trap    fource     v2c   15     3        Eth1/1
1001::1        inform   user1   auth-priv  v3    200    10       Eth1/2
```

Releases

3.0 or later

show snmp-server interface-traps

Displays the interfaces on which SNMP traps are disabled.

Command show snmp-server interface-traps

Options None

Modes	EXEC
Usage	Use this command to view whether sending SNMP traps to an SNMP management station is disabled on switch interfaces. To disable (or re-enable) sending all SNMP traps and informs that are generated on switch interfaces, use the [no] <code>snmp-server enable trap</code> command. To disable (or re-enable) sending only <code>linkup</code> and <code>linkdown</code> traps, use the <code>snmp trap enable</code> command.
Example	<pre>sonic# show snmp-server interface-traps Interface Name Status ----- ----- Ethernet12 disable</pre>
Releases	4.1.0 or later

show snmp-server traps

Displays the SNMP traps that are enabled on the switch.

Command	<code>show snmp-server traps</code>
Options	None
Modes	EXEC
Usage	Use this command to view the types of SNMP traps that are enabled to be sent to a remote SNMP management station. To enable sending all or selected SNMP traps, use the <code>snmp-server trap enable</code> command.
Example	<pre>sonic# show snmp-server traps Trap Type Status ----- ----- Authentication failure enable BGP enable Config Change enable Link Down enable OSPF enable</pre>
Releases	4.4.0 or later

show snmp-server user

Displays the configured SNMPv3 users.

Command	<code>show snmp-server user</code>
Options	None
Modes	EXEC
Usage	Use this command to view the SNMPv3 users configured on the switch including any authentication and/or encryption algorithm for the user. The group name indicates a group that defines the SNMPv3 access parameters.
Example	<pre>sonic# show snmp-server user User Name Group Name Auth Privacy ----- ----- user1 group-lab md5 aes-128 user2 group-floor2 None None</pre>
Releases	3.0 or later

show snmp-server view

Displays SNMP views configuration information.

Command show snmp-server view

Options None

Modes EXEC

Usage Use this command to display SNMP views configured on the switch including the OID tree that the view includes or excludes.

Example

```
sonic# show snmp-server view
View Name          OID Tree           Type
-----
view1             1.2.3.4.5.6.7.8.9.1 included
view2             1.2.3.4.5.6.7.8.9.5.1 excluded
```

Releases 3.0 or later

show spanning-tree

Displays the spanning-tree configuration.

Command show spanning-tree [vlan] {vlan-id {[interface] name}}

- **vlan-id**—(Optional) VLAN ID (1 to 4094)
- **name**—(Optional) Interface name

Modes EXEC

Usage Use this command to view the spanning-tree states and parameters.

Examples

```
sonic# show spanning-tree
Spanning-tree Mode: PVST

VLAN 100 - STP instance 0
-----
STP Bridge Parameters:
Bridge Identifier      Bridge MaxAge   Bridge Hello   Bridge FwdDly   Hold Time   LastTopology Change   Topology Change
Identifier          MaxAge sec       Hello  sec       FwdDly sec       sec       sec       cnt
hex                sec      2          15        1         515      4
80643c2c99a704a0  20       2          15        1         515      4

RootBridge Identifier      RootPath Cost      DesignatedBridge Identifier      Root      Max Age   Hel lo   Fwd
Identifier          Cost      hex       Identifier      Port      Port   Age sec   sec   sec
hex                cost     hex       identifier      port      port   age sec   sec   sec
00646cb9c51613ca  1600     10643c2c992d8235 PortChannel120  PortChannel120 2        15

STP Port Parameters:
Port      Prio Path Port Uplink BPDU State      Designated Cost      Designated Designated
Port      Prio Path Port Fast  Filter State      Designated Cost      Designated Designated
Num      rity Cost Fast  Fast  Filter State      Designated Cost      Designated Designated
PortChannell 128 800 N      N      FORWARDING 800      00646cb9c51613ca 10643c2c992d8235
```

```
sonic# show spanning-tree vlan VLAN10
Spanning-tree Mode: RPVST
VLAN 10 - RSTP instance 0
-----
RSTP (IEEE 802.1w) Bridge Parameters:
Bridge Identifier      Bridge MaxAge   Bridge Hello   Bridge FwdDly   Hold
Identifier          MaxAge sec       Hello  sec       FwdDly sec       Hold
hex                sec      2          15        3
0001000480a04000  20       2          15        3

RootBridge Identifier      RootPath Cost      DesignatedBridge Identifier      Root      Max Age   Hel lo   Fwd
Identifier          Cost      hex       Identifier      Port      Port   Age sec   sec   sec
hex                cost     hex       identifier      port      port   age sec   sec   sec
0001000480a04000  0        0001000480a04000  Root      20      2        15

RSTP (IEEE 802.1w) Port Parameters:
Port      Prio PortPath link Edge BPDU Guard Role      State Designated cost Designated
Port      Prio PortPath type Port Filter Type      State Designated cost Designated
Num      rity Cost type  F      N      Loop  DISABLED  DISABLED  0      0000000000000000
Ethernet3 128 20000 P2P   F      N      Loop  DISABLED  DISABLED  0      0000000000000000
Ethernet13 128 20000 P2P   F      N      -      DISABLED  DISABLED  0      0000000000000000
```

Releases

3.0 or later

show spanning-tree bpdu-guard

Displays spanning-tree BPDU guard information for the ports.

Command show spanning-tree bpdu-guard

Options None

Modes EXEC

Usage Use this command to view the bpdu-guard enabled interfaces and its actions.

Example

```
sonic# show spanning-tree bpdu-guard
PortNum      Shutdown      Port shut
Configured   due to BPDU guard
-----
Ethernet2     Yes          No
Port-Channel2  No          NA
```

Releases 3.0 or later

show spanning-tree counters

Displays spanning-tree counter information.

Command show spanning-tree counters [vlan] *vlan-id*

Options *vlan vlan-id*—(Optional) VLAN ID (1 to 4094)

Modes EXEC

Usage Displays spanning-tree information for the given VLAN. You can specify a single VLAN ID, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. TCN TX/RX counters are not applicable for RPVST+. In RPVST+ mode, configuration BPDU TX/RX counters are updated only on receiving STP BPDUs.

Example

```
sonic# show spanning-tree counters
VLAN 100 - STP instance 3
-----
PortNum      BPDU Tx      BPDU Rx      TCN Tx      TCN Rx      Config BPDU Tx      Config BPDU Rx
Ethernet13    10           4             3             4             5               3
PortChannel15 20           6             4             1             4               2
```

Releases 3.0 or later

show spanning-tree inconsistentports

Displays spanning-tree root or loop inconsistent port information.

Command show spanning-tree inconsistentports [vlan] *vlan-id*

Options *vlan vlan-id*—(Optional) Enter the VLAN ID (1 to 4094).

Modes EXEC

Usage Use this command to view spanning-tree root or loop inconsistent port information.

Example

```
sonic# show spanning-tree inconsistentports
Loop guard default: Disabled
-----
PortNum      INST      Inconsistency State
-----
Ethernet26    0         Root Inconsistent
```

Releases	3.0 or later
-----------------	--------------

show spanning-tree mst

Displays a specific MST configuration using the instance ID.

Command	show spanning-tree mst [<i>inst-id</i> [detail]]
Options	<ul style="list-style-type: none">• <i>inst-id</i>—Enter the MST instance ID (0 to 4094).• <i>detail</i>—Displays detailed information about MST configuration.
Modes	EXEC
Usage	Use this command to view a specific MST configuration using the instance ID.
Examples	For MST instance:

```
sonic# show spanning-tree mst 1
##### MST1      Vlans mapped: 2,100,200
Bridge          Address 8001.80a2.3526.0c5e
Root            Address 8001.80a2.3526.0c5e
                Port      Root          Path cost 0      Rem hops 20
Interface       Role      State      Cost      Prio.Nbr Type
-----
Ethernet45     DESIGNATED FORWARDING 800      128.45   P2P
PortChannel120 DESIGNATED FORWARDING 2000     128.85   P2P
```

Detail:

```
sonic# show spanning-tree mst 1 detail
##### MST1      Vlans mapped: 2,100,200
Bridge          Address 8001.80a2.3526.0c5e
Root            Address 8001.80a2.3526.0c5e
                Port      Root          Path cost 0      Rem hops 20
Ethernet45 is DESIGNATED FORWARDING
Port info        port id 45    priority 128    cost 800
Designated root  Address 8001.80a2.3526.0c5e  cost 0
Designated bridge Address 8001.80a2.3526.0c5e  port id 45
Timers: forward transitions 0
Bpdus sent 91, received 0

PortChannel120 is DESIGNATED FORWARDING
Port info        port id 85    priority 128    cost 2000
Designated root  Address 8001.80a2.3526.0c5e  cost 0
Designated bridge Address 8001.80a2.3526.0c5e  port id 85
Timers: forward transitions 0
Bpdus sent 93, received 0
```

Releases	4.0 or later
-----------------	--------------

show spanning-tree mst configuration

Displays the MST configuration.

Command	show spanning-tree mst configuration
Options	None
Modes	EXEC
Usage	Use this command to view the spanning-tree MST configuration.

Examples

```
sonic-clli# show spanning-tree mst configuration
Name [test]
Revision 10 Instances configured 4
Instance Vlans mapped
-----
0      1-9,11-19,21-4093
1      10
2      20
4094  4094
-----
```

Releases

4.0 or later

show spanning-tree mst detail

Displays the MST configuration in detail.

Command show spanning-tree mst detail**Options** None**Modes** EXEC**Usage** Use this command to view all MST instances configuration in detail.**Examples**

```
sonic# show spanning-tree mst detail

##### MST1      Vlans mapped: 2,100,200
Bridge          Address 8001.80a2.3526.0c5e
Root           Address 8001.80a2.3526.0c5e
               Port     Root             Path cost 0      Rem hops 20

Ethernet45 is DESIGNATED FORWARDING
Port info        port id 45    priority 128    cost 800
Designated root   Address 8001.80a2.3526.0c5e  cost 0
Designated bridge  Address 8001.80a2.3526.0c5e  port id 45
Timers: forward transitions 0
Bpdus sent 91, received 0

PortChannel120 is DESIGNATED FORWARDING
Port info        port id 85    priority 128    cost 2000
Designated root   Address 8001.80a2.3526.0c5e  cost 0
Designated bridge  Address 8001.80a2.3526.0c5e  port id 85
Timers: forward transitions 0
Bpdus sent 93, received 0
```

Releases

4.0 or later

show spanning-tree mst interface

Displays interface-specific MST information.

Command show spanning-tree mst interface *name* [detail]

- *name*—Enter the name of the MST interface (up to 63 characters).
- *detail*—(Optional) Displays detailed information about MST configuration on an interface.

Modes EXEC**Usage** Use this command to view the interface-specific MST information.**Examples**

```
sonic# show spanning-tree mst interface Ethernet45
Link Type: P2P          Bpdu filter: False
Boundary: internal       Bpdu guard: False
```

Instance	Role	State	Cost	Pri.Nbr	Vlans mapped
0	DESIGNATED	FORWARDING	800	128.45	1,3-99,101-199,201-4094
1	DESIGNATED	FORWARDING	800	128.45	2,100,200

Releases 4.0 or later

show ssh-server vrf

Displays a list of VRFs that the SSH server is enabled on.

Command show ssh-server vrf {all | vrf-name}

Options

- all—Displays all VRFs.
- vrf-name—VRF name prefixed by Vrf (up to 15 characters)

Modes EXEC

Usage Use this command to view a list of VRFs that the SSH server is enabled on.

Example

```
sonic# show ssh-server vrf all
VRF Name          Status
-----
mgmt             enable
```

Releases 3.1 or later

show storm-control

Displays all BUM storm control information.

Command show storm-control

Options None

Modes EXEC

Usage Use this command to view all BUM storm control information.

Example

```
sonic# show storm-control
-----
Interface Name      Storm-type        Rate (kbps)
-----
Ethernet0           broadcast         10000
Ethernet0           unknown-unicast   20000
Ethernet0           unknown-multicast 30000
Ethernet4           unknown-unicast   20000
Ethernet4           unknown-multicast 30000
```

Releases 3.1 or later

show storm-control interface

Displays BUM storm control configuration information for a specific interface.

Command show storm-control interface *Ethernet*

Options *Ethernet*—Ethernet interface ID (0 to 255)

Modes EXEC

Usage Use this command to view BUM storm control configuration information for a specific interface.

Example

```
sonic# show storm-control interface Ethernet 4
-----
Interface Name      Storm-type          Rate (kbps)
-----
Ethernet4           unknown-unicast     20000
Ethernet4           unknown-multicast   30000
```

Releases 3.1 or later

show subinterfaces status

Displays subinterface status information.

Command show subinterfaces status

Options None

Modes EXEC

Usage Use this command to display the subinterface status and information.

Example

```
sonic# show subinterfaces status
-----
Sub port interface  Speed    MTU     Vlan Admin  Type
-----
Ethernet0.10        25000   2000    100    up    dot1q-encapsulation
PortChannel100.100  0       9100    1350   up    dot1q-encapsulation
```

Releases 3.2 or later

show switch-profiles

Displays all supported factory default configuration profiles.

Command show switch-profiles

Options None

Command mode EXEC

Usage Use this command to display the current active default configuration profile, which is used to create a startup configuration file when [write erase](#) is used.

Example

```
sonic# show switch-profiles
Factory Default: 13

Profile Name      Description
-----
12                Layer 2 Switch Configuration
13                Layer 3 Router Configuration
```

Releases 3.1 or later

show switch-resource drop-monitor

Displays the current drop-monitor switch resource configuration.

Command show switch-resource drop-monitor

Options None

Modes	EXEC
Usage	Use this command to view the current drop-monitor switch resource configuration.
Example	<pre>sonic# show switch-resource drop-monitor Drop-Monitor flows ----- Configured : none In use : min Needs reboot : true</pre>
Releases	3.1 or later

show switch-resource route-scale

Displays route-scale switch resource configuration.

Command	show switch-resource route-scale
Options	None
Modes	EXEC
Usage	Use this command to view the configured route-scale profile and current active profile. If required, reboot the switch to set the configured profile as active profile.
Examples	<pre>sonic# show switch-resource route-scale Configured routes : Configured hosts : layer2-layer3 In use : default Reboot needed : true</pre>
Releases	3.2 or later

show switch-resource vlan-stacking

Verify the operational status of VLAN stacking features on Z9432F-ON and S5448F-ON switches.

Command	show switch-resource vlan-stacking
Options	None
Modes	EXEC
Usage	You must enable VLAN stacking from the switch-resource command tree before you can configure Q-in-Q VLAN tunneling and VLAN translation (see vlan-stacking enable). After you save the configuration and reload the switch, verify that VLAN stacking is enabled. Then proceed with Q-in-Q VLAN or VLAN translation configuration.
Example	<pre>sonic(config)# switch-resource sonic(config-switch-resource)# vlan-stacking Config save and reboot is required for this change to take effect sonic(config-switch-resource)# exit sonic# write memory sonic# reload ! After reboot sonic# show switch-resource vlan-stacking Configured : enabled Operational : enabled</pre>

i **NOTE:** If you check the VLAN stacking status before you save and reload the switch, it is still operationally disabled:

```
sonic(config)# switch-resource
sonic(config-switch-resource)# vlan-stacking enable
Config save and reboot is required for this change to take effect
sonic(config-switch-resource)# do show switch-resource vlan-stacking
Configured : enabled
Operational : disabled
```

Releases

4.1.0 or later

show switching-mode

Displays the configured switching mode.

Command show switching-mode**Options** None**Command mode** EXEC**Usage** The default switching mode is store-and-forward. To enable cut-through switching, use the switching-mode cut-through command.**Example**

```
sonic# show switching-mode
Current switching mode: cut-through
```

Releases

4.2.0 or later

show system

Displays system information.

Command show system**Options** None**Modes** EXEC**Usage** Use this command to view the boot time, current date and time, and hostname.**Example**

```
sonic# show system
-----
Attribute          Value/State
-----
Boot Time          :00:02:27
Current Datetime   :2024-07-09T20:26:08Z
Hostname           :sonic
```

Releases

3.0 or later

show system cpu

Displays system CPU information.

Command show system cpu**Options** None**Modes** EXEC

Usage

Use this command to check the CPU usage. The CPU-ALL provides the average usage across all cores. The usage data is refreshed every resource-stats-polling-interval, which is set to 120 seconds by default. Use the system resource-stats-polling-interval command to change the interval at which system resource utilization metrics are polled.

Example

```
sonic# show system cpu
Polling Interval: 120.0 seconds
-----
CPU          %KERNEL    %USER    %IDLE
-----
CPU-ALL      3          8        87
CPU-0        3          8        87
CPU-1        3          8        87
CPU-2        3          9        86
CPU-3        3          8        87
CPU-4        3          8        87
CPU-5        5          9        85
CPU-6        3          9        87
CPU-7        4          9        86
```

Releases

3.0 or later

show system memory

Displays system memory information.

Command show system memory**Options** None**Modes** EXEC**Usage** Use this command to check the memory usage.**Example**

```
sonic# show system memory
-----
Attribute          Value/State
-----
Used              :1304976
Total             :8162872
```

Releases

3.0 or later

show system processes

Displays all system processes information.

Command show system processes**Options** None**Modes** EXEC**Usage** Use this command to check the CPU and memory usage of all processes.**Example**

```
sonic# show system processes
-----
PID    %CPU    %MEMORY   MEM-USAGE (Bytes)   NAME
-----
1      0        0          58761216      /sbin/init
10     0        0          0            [lru-add-drain]
100    0        0          0            [scsi_eh_0]
1000   0        0          409763840     docker
101    0        0          0            [scsi_tmf_0]
```

10179	0	0	12124160	/bin/bash
102	0	0	0	[scsi_eh_1]
10217	0	0	42135552	python
103	0	0	0	[scsi_tmf_1]
107	0	0	0	[bioset]
10862	0	0	256139264	/usr/sbin/rsyslogd
109	0	0	0	[kworker/3:1H]
11	0	0	0	[watchdog/0]
110	0	0	0	[kworker/2:1H]
11044	0	0	111427584	containerd-shim
11088	0	0	109920256	containerd-shim
111	0	0	0	[kworker/0:1H]
11119	0	0	109920256	containerd-shim
11140	0	0	59592704	/usr/bin/python
11177	0	0	111362048	containerd-shim
112	0	0	0	[kworker/1:1H]
11204	0	0	59600896	/usr/bin/python
11223	0	0	61095936	/usr/bin/python
11272	0	0	189263872	/usr/bin/orchagent
11308	0	0	58249216	/usr/bin/python

Releases 3.0 or later

show system processes cpu

Displays system processes that are sorted by CPU usage.

Command show system processes cpu

Options None

Command mode EXEC

Usage Use this command to view the system processes sorted by CPU usage.

Example

```
sonic# show system processes cpu
-----
PID          %CPU      %MEMORY    MEM-USAGE (Bytes)  NAME
-----
4333         22        2           1833492480      /usr/bin/syncd
9888         19        0           98504704       /usr/lib/frr/bfdd
2403         12        0           161193984      /usr/bin/python
1248         7         0           460005376      /usr/bin/redis-server
1245         6         0           99295232      /usr/bin/redis-server
2405         5         0           361672704      /usr/bin/python
3337         4         0           320245760      /usr/bin/orchagent
416          4         0           0              [kipmi0]
10377        3         0           365019136      python3.6
4407          3        0           193110016      /usr/bin/neighsyncd
1799          2        0           345231360      /usr/sbin/rsyslogd
10303        1         0           164511744      /usr/bin/python
2407          1        0           256139264      /usr/sbin/rsyslogd
3790          1        0           105349120      /usr/bin/portsyncd
7529          1        0           124157952      python2
1            0         0           59277312       /sbin/init
10           0         0           0              [lru-add-drain]
10007        0         0           12148736       /bin/bash
10011        0         0           409763840      docker
10118        0         0           100298752      /usr/sbin/ntpd
10266        0         0           49336320       python2.7
--more--
```

Releases 3.1 or later

show system processes mem-usage

Displays system processes that are sorted by memory usage.

Command show system processes mem-usage

Options None

Command mode EXEC

Usage

Use this command to view the system processes sorted by memory usage.

Example

```
sonic# show system processes mem-usage
-----
PID          %CPU      %MEMORY    MEM-USAGE (Bytes)  NAME
-----
4333         22        2           1833492480     /usr/bin/synccd
6822         0          1           1597079552     /usr/sbin/rest_server
8717         0          0           1329385472     /usr/lib/frr/zebra
510          0          0           1221566464     /usr/bin/containerd
6881         0          1           1057107968     telemetry
633          0          0           1044697088     /usr/bin/dockerd
3875         0          0           552374272      docker
6361         0          0           544243712      docker
4051         0          0           543981568      docker
1341         0          0           520667136      python
6591         0          0           477134848      docker
3102         0          0           476872704      docker
6476         0          0           476872704      docker
6742         0          0           476872704      docker
3831         0          0           476610560      docker
6631         0          0           476610560      docker
1248         7          0           460005376      /usr/bin/redis-server
1307         0          0           418418688      docker
9660         0          0           418418688      docker
6938         0          0           418156544      docker
6398         0          0           410025984      docker
--more--
```

Releases

3.1 or later

show system processes mem-util

Displays system processes that are sorted by memory utilization.

Command show system processes mem-util

Options None

Command mode EXEC

Usage

Use this command to view the system processes sorted by memory utilization.

Example

```
sonic# show system processes mem-util
-----
PID          %CPU      %MEMORY    MEM-USAGE (Bytes)  NAME
-----
4333         22        2           1833492480     /usr/bin/synccd
6822         0          1           1597079552     /usr/sbin/rest_server
6881         0          1           1057107968     telemetry
9868         0          1           355176448      /usr/lib/frr/ospfd
1            0          0           59277312      /sbin/init
10           0          0           0              [lru-add-drain]
10007        0          0           12148736      /bin/bash
10011        0          0           409763840     docker
10118        0          0           100298752     /usr/sbin/ntpd
10266        0          0           49336320      python2.7
10303        1          0           164511744     /usr/bin/python
10333        0          0           84725760      /usr/sbin/snmpd
10377        3          0           365019136     python3.6
10384        0          0           293613568     python3.6
104          0          0           0              [ata_sff]
105          0          0           0              [ixgbe]
10988        0          0           0              [kworker/1:0]
11            0          0           0              [watchdog/0]
1112         0          0           112869376     containerd-shim
1128         0          0           59650048      /usr/bin/python
11614         0          0           0              [kworker/3:2]
--more--
```

Releases

3.1 or later

show system processes pid

Displays system process information for a specific process ID.

Command show system processes pid *pid-no*

Options pid *pid-no*—Process ID

Modes EXEC

Usage Use this command to view the system process information for a specific process ID.

Example

```
sonic# show system processes pid 1
-----
Attribute          Value/State
-----
Cpu Usage System   :525
Cpu Usage User    :1068
Cpu Utilization   :0
Memory Usage       :59158528
Memory Utilization :0
Name               :/sbin/init
Pid                :1
Start Time         :2022-03-09 11:13:46+0000
Uptime             :1d22h52m
```

Releases 3.0 or later

show system status

Displays the system ready status.

Command show system status [brief | detail]

Options

- brief—(Optional) Displays the brief system ready status.
- detail—(Optional) Displays the detailed system ready status.

Modes EXEC

Usage Use this command to view the status of all services running in the system.

Examples

```
sonic# show system status brief
System is ready
```

```
sonic# show system status
System is ready
```

Service-Name	Service-Status	App-Ready-Status
Down-Reason		
swss	OK	OK
-		
bgp	OK	OK
-		
teamd	OK	OK
-		
pmon	OK	OK
-		
syncd	OK	OK
-		
database	OK	OK
-		
mgmt-framework	OK	OK
-		
gbsyncd	OK	OK
-		
auditd	OK	OK

-	autobreakoutmgrd	OK	OK
-	caclmgrd	OK	OK
-	ccd	OK	OK
-	config-chassisdb	OK	OK
-	config-setup	OK	OK
-	containerd	OK	OK
-	critical-monitoring	OK	OK
-	cron	OK	OK
-	database-chassis	OK	OK
-	db-post-startup	OK	OK
-	determine-reboot-cause	OK	OK
-	dhcp_relay	OK	OK
-	disk-log-rotate-daemon	OK	OK
-	docker	OK	OK
-	eventd	OK	OK
-	export	OK	OK
-	hamd	OK	OK
-	histogram	OK	OK
-	hostcfgd	OK	OK
-	hostname-config	OK	OK
-	iccpd	OK	OK
-	in-memory-log-rotate-daemon	OK	OK
-	in-memory	OK	OK
-	interfaces-config	OK	OK
-	ccdkdump-tools	OK	-
-	lacp-helper	OK	OK
-	lldp	OK	OK
-	nat	OK	OK
-	netfilter-persistent	OK	OK
-	ntp-config	OK	OK
-	ntp	OK	OK
-	opennsl-modules	OK	OK
-	platform-init	OK	OK
-	platfprm-modules-z9864f	OK	OK
-	platform-ready	OK	OK
-	portinitdone	OK	OK

procdockerstatsd	OK	OK
-		
radv	OK	OK
-		
ras-mc-ctl	OK	OK
-		
resrcmgrp	OK	OK
-		
rsyslog-config	OK	OK
-		
rsyslog	OK	OK
-		
sflow	OK	OK
-		
snmp	OK	OK
-		
sonic-hostservice	OK	OK
-		
sonic-init-updatedb	OK	OK
-		
ssh	OK	OK
-		
sysmonitor	OK	OK
-		
tam	OK	OK
-		
telemetry	OK	OK
-		
tcpm@default	OK	OK
-		
udld	OK	OK
-		
updategraph	OK	OK
-		
vrrp	OK	OK
-		
warmboot-finalizer	OK	OK
-		
watchdog-control	OK	OK
-		
ztp-config	OK	OK
-		
system-health	OK	OK
-		

sonic# show system status detail			
System is ready	Service-Name	Service-Status	App-Ready-Status
Service-Name	Status-UpdateTime	Service-Status	Down-Reason
swss	2023-06-30 04:57:11	OK	OK
bgp	2023-06-30 04:57:18	OK	OK
teamd	2023-06-30 04:55:45	OK	OK
pmon	2023-06-30 04:56:57	OK	OK
syncd	2023-06-30 04:56:11	OK	OK
database		OK	-
mgmt-framework		OK	-
gbsyncd		OK	-
cacimgrd		OK	-
ccd		OK	-
config-chassisdb		OK	-
config-setup		OK	-
containerd		OK	-
critical-monitoring		OK	-
cron		OK	-
database-chassis		OK	-
db-post-startup		OK	-
determine-reboot-cause		OK	-
dhcp_relay	2023-06-30 04:57:04	OK	OK
disk-log-rotate-daemon		OK	-
docker		OK	-
eventd		OK	-

```

20230630 04:55:04
hamd                      OK          OK          -          -
histogram                  OK          OK          -          -
hostcfgd                   OK          OK          -          -
hostname-config            OK          OK          -          -
iccpd                      OK          OK          -          -
2023-06-30 04:56:30
in-memory-log-rotate-daemon OK          OK          -          -
in-memory                  OK          OK          -          -
interfaces-config           OK          OK          -          -
kdump-tools                 OK          OK          -          -
l2mcd                      OK          OK          -          -
2023-06-30 04:56:57
lacp_helper                OK          OK          -          -
lldp                       OK          OK          -          -
2023-06-30 04:56:30
nat                         OK          OK          -          -
2023-06-30 04:56:28
netfilter-persistent         OK          OK          -          -
ntp-config                  OK          OK          -          -
ntp                         OK          OK          -          -
opennsl-modules              OK          OK          -          -
platform-init                OK          OK          -          -
platform-modules-s5248f      OK          OK          -          -
portinitdone                 OK          OK          -          -
procdockerstatsd            OK          OK          -          -
radv                        OK          OK          -          -
2023-06-30 04:57:03
ras-mc-ctl                  OK          OK          -          -
resrcmgrd                   OK          OK          -          -
rsyslog-config               OK          OK          -          -
rsyslog                      OK          OK          -          -
sflow                       OK          OK          -          -
2023-06-30 04:57:02
snmp                        OK          OK          -          -
2023-06-30 04:57:45
sonic-hostservice             OK          OK          -          -
ssh                          OK          OK          -          -
stp                          OK          OK          -          -
2023-06-30 04:56:30
sysmonitor                  OK          OK          -          -
tam                          OK          OK          -          -
20230630 04:57:28
telemetry                    OK          OK          -          -
20230630 04:56:25
tpcm@default                 OK          OK          -          -
udld                        OK          OK          -          -
2023-06-30 04:56:30
updategraph                  OK          OK          -          -
vrrp                        OK          OK          -          -
2023-06-30 04:57:01
warmboot-finalizer            OK          OK          -          -
watchdog-control              OK          OK          -          -
ztp-config                   OK          OK          -          -
tpcm@mgmt                   OK          OK          -          -
sonic#

```

Releases

4.0.0 or later

show system vlan

Displays reserved VLAN information.

Command show system vlan reserved

Options None

Modes EXEC

Usage Use this command to view the reserved VLAN information.

Example

```

sonic# show system vlan reserved
system vlan reservation: 3967-4094

```

Releases

4.0 or later

show tacacs-server

Displays all TACACS+ server information.

Command show tacacs-server

Options None

Modes EXEC

Usage Use this command to view the TACACS+ global configuration and server configuration.

Example

```
sonic# show tacacs-server
-----
TACACS Global Configuration
-----
timeout    : 5
auth-type  : pap
-----
HOST        AUTH-TYPE   KEY     PORT    PRIORITY  TIMEOUT   VRF
-----
100.94.192.82  pap          49      1        5           default
```

Releases 3.0 or later

show tacacs-server global

Displays global TACACS+ server information.

Command show tacacs-server global

Options None

Modes EXEC

Usage Use this command to view the global TACACS+ server information.

Example

```
sonic# show tacacs-server global
-----
TACACS Global Configuration
-----
source-interface : Loopback0
timeout : 10
auth-type : chap
key configured   : Yes
```

Releases 3.0 or later

show tacacs-server host

Displays TACACS+ server host information.

Command show tacacs-server host [address]

Options host address — (Optional) Host IP address in A.B.C.D format

Modes EXEC

Usage None

Examples

```
sonic# show tacacs-server host
-----
HOST        AUTH-TYPE   KEY-CONFIG  PORT    PRIORITY  TIMEOUT   VRF
-----
1.1.1.1      pap         Yes          11      11        10           mgmt
```

2.2.2.2	mschap	Yes	20	20	20	mgmt
<pre>sonic# show tacacs-server host 1.1.1.1 ----- HOST AUTH-TYPE KEY-CONFIG PORT PRIORITY TIMEOUT VRF ----- 1.1.1.1 pap Yes 11 11 10 mgmt</pre>						

Releases 3.0 or later

show tam collectors

Displays details for all TAM collectors or for a specific collector.

Command	show tam collectors [name]
Options	<i>name</i> —(Optional) TAM collector name (up to 63 characters)
Modes	EXEC
Usage	Use this command to view the details for all TAM collectors or for a specific collector.

Examples

```
sonic# show tam collectors
Name           IP Address      Port      Protocol
-----
IFA_Col_i19    192.168.78.121  7071     UDP
MOD_Col_m16   192.168.78.123  7076     UDP

sonic# show tam collectors IFA_Col_i19
Name      : IFA_Col_i19
IP Address : 192.168.78.121
Port      : 7071
Protocol  : UDP
```

Releases 3.1 or later

show tam drop-monitor

Displays the switch-wide attributes in use.

Command	show tam drop-monitor
Options	None
Command mode	EXEC
Usage	None
Example	

```
sonic# show tam drop-monitor

Status      : Active
Switch ID   : 2020
Aging Interval : 20
```

Releases 3.1 or later

show tam drop-monitor sessions

Displays the details for all drop-monitor sessions, or for a specific session.

Command show tam drop-monitor sessions [*name*]

Options *name* — (Optional) Drop-monitor session name

Command mode EXEC

Usage Only explicitly configured tuples in the associated flow-group display.

Examples

```
sonic# show tam drop-monitor sessions
Name           Flow Group          Collector        Sampler
-----          -----              -----          -----
ss1            f1                c1             s1
ss2            DEMO              c1             s2
ss91           f9                c2             s1
```

```
sonic# show tam drop-monitor sessions http_236
```

```
Session          : http_236
Flow Group Name : tcp_port_236
  Id            : 4025
  Priority      : 100
  SRC IP       : 13.92.96.32
  DST IP       : 7.72.235.82
  DST L4 Port  : 236
  Ingress Intf : Ethernet20
  Collector     : Col_i19
  Sampler       : aggressive
  Packet Count  : 7656
```

Releases 3.1 or later

show tam features

Displays the current status for all TAM features, or for a specific feature.

Command show tam features {[ifa] | [drop-monitor] | [tail-stamping]}

Options None

Command mode EXEC

Usage Use this command to view the current status of supported TAM features and also displays the unsupported TAM features.

Examples

```
sonic# show tam features
Name           Status
-----          -----
drop-monitor   Inactive
ifa            Active
tail-stamping Inactive
```

```
sonic# show tam features ifa
```

```
Name           : ifa
Status         : Active
```

```
sonic# show tam features
```

```
Name           Status
-----          -----

```

drop-monitor	Unsupported
ifa	Unsupported
tail-stamping	Inactive

Releases 3.1 or later

show tam flowgroups

Displays details for all flow-groups, or for a specific flow-group.

Command show tam flowgroups [name]

Options name — (Optional) Flow-group name

Command mode EXEC

Usage Only explicitly configured tuples display.

Examples

```
sonic# show tam flowgroups

Flow Group Name      : udp_port_239
  Id                : 4025
  Priority          : 100
  SRC IP            : 10.72.195.23
  DST L4 Port       : 239
  Ingress Intf     : Ethernet20
  Packet Count      : 10584

Flow Group Name      : udp_port_241
  Id                : 4022
  Priority          : 99
  SRC Port           : 1906
  DST L4 Port       : 241
  Packet Count      : 8654367
```

```
sonic# show tam flow-groups udp_port_239

Flow Group Name      : udp_port_239
  Id                : 4025
  Priority          : 100
  SRC IP            : 10.72.195.23
  DST L4 Port       : 239
  Packet Count      : 10584
```

Releases 3.1 or later

show tam ifa

Displays the switch-wide attributes in use.

Command show tam ifa

Options None

Command mode EXEC

Usage None

Example

```
sonic# show tam ifa

  Status             : Active
  Switch ID          : 2020
  Enterprise ID     : 2345
  Version            : 2.0
```

```
Number of sessions : 1
Number of collectors : 1
```

Releases 3.1 or later

show tam ifa sessions

Displays details for all IFA sessions, or for a specific session.

Command show tam ifa sessions [*name*]

Options *name* — (Optional) IFA session name

Command mode EXEC

Usage Only explicitly configured tuples display.

Examples

```
sonic# show tam ifa sessions
Name      Flow Group      Collector      Sampler      Node Type
-----  -----  -----  -----  -----
ssl       f9          s1           Ingress Node
```

```
sonic# show tam ifa sessions http_236

Session          : http_236 (Ingress)
Flow Group Name : tcp_port_236
Id              : 4025
Priority        : 100
SRC IP          : 13.92.96.32
DST IP          : 7.72.235.82
DST L4 Port     : 236
Ingress Intf    : Ethernet20
Collector        : None
Sampler          : aggressive
Packet Count    : 7656
```

Releases 3.1 or later

show tam samplers

Displays details for all samplers, or for a specific sampler.

Command show tam samplers [*name*]

Options *name* — (Optional) Sampler name

Command mode EXEC

Usage Use this command to view the details for all samplers, or for a specific sampler.

Examples

```
sonic# show tam samplers

Name      Sample Rate
-----  -----
sflow_low   1
aggressive 2000
```

```
sonic# show tam samplers aggressive

Name      : aggressive
Sample Rate : 2000
```

Releases 3.1 or later

show tam switch

Displays the configured TAM device identifier.

Command	show tam switch
Options	None
Command mode	EXEC
Usage	Use this command to display the configured TAM device identification information including Switch ID and Enterprise ID.

Example

```
sonic# show tam switch
TAM Device information
-----
Switch ID      : 23456
Enterprise ID  : 1234
```

Releases	3.1 or later
-----------------	--------------

show tam tail-stamping

Displays the switch-wide attributes in use for tail-stamping.

Command	show tam tail-stamping
Options	None
Command mode	EXEC
Usage	Use this command to view the switch-wide attributes in use for tail-stamping.

Example

```
sonic# show tam tail-stamping
Status          : Active
Switch ID       : 2020
Number of sessions : 0
```

Releases	3.1 or later
-----------------	--------------

show tam tail-stamping sessions

Displays details for all tail-timestamping sessions, or for a specific session.

Command	show tam tail-stamping sessions [name]
Options	name — (Optional) Tail-timestamping session name
Command mode	EXEC
Usage	Only explicitly configured tuples display.

Examples

```
sonic# show tam tail-stamping sessions
Name        Flow Group    Node Type
-----      -----      -----
ss66        f9          IFA
ss99        f10         Normal
```

```
sonic# show tam tail-stamping sessions http_236
Session      : http_236
```

```
Flow Group Name      : tcp_port_236
  Id                : 4025
  Priority          : 100
  SRC IP            : 13.92.96.32
  DST IP            : 7.72.235.82
  DST L4 Port       : 236
  Packet Count      : 7656
```

Releases 3.1 or later

show tech-support

Collects technical support information.

Command show tech-support [since {date time | yesterday}]

Options

- since *date time*—(Optional) Configures the date and time used to start collecting data for technical support. Enter the date in the format *YYYY-MM-DD*, where:
 - *YYYY* is the year, such as 2021
 - *MM* is the number of the month (01 to 12)
 - *DD* is the number of the day (01 to 31)Enter the *since* time in the format *THH:MM:SS[.ddd...]{z | +hh:mm | -hh:mm}*, where:
 - Enter *T* to identify that a time parameter follows.
 - *HH* is the hour (01 to 24)
 - *MM* is the number of minutes (00 to 59)
 - *SS* is the second (01 to 60)
 - *.ddd...* is an optional decimal of the specified second (example, .234)
 - *z* indicates that there is no offset from the specified time
 - *+hh:mm* indicates the hours and minutes to be added to the specified time and date.
 - *-hh:mm* indicates the hours and minutes to be subtracted from the specified time and date.
- since *yesterday*—(Optional) Configures data collection for technical support to start from yesterday.

Modes EXEC

Usage

Use the *since* option to limit the size of the technical support data collected. Use the *show tech-support status* command to verify the status of the technical support collection and to find out the file location once it has been collected.

Example

```
sonic# show tech-support since 2020-03-05T07:10:00Z
```

```
sonic# show tech-support since yesterday
```

Releases 3.0 or later

show tech-support cancel

Cancels technical support collection.

Command show tech-support cancel

Options None

Modes EXEC

Usage Use this command to cancel technical support collection.

Example

```
sonic# show tech-support cancel  
%Info: Tech-support process canceled
```

Releases

4.0 or later

show techsupport-export

Displays technical support export configuration.

Command show techsupport-export**Options** None**Modes** EXEC**Usage** Use this command to view the technical support export configuration.**Example**

```
sonic# show techsupport-export  
=====  
Techsupport Export Configuration  
=====  
Server Name      : 50.0.0.1  
User Name        : dell  
Protocol         : scp  
Interval         : 1000  
Config Mode      : True
```

Releases

4.0 or later

show tech-support status

Displays technical support collection status.

Command show tech-support status**Options** None**Modes** EXEC**Usage** Use this command to view the status of the technical support collection and the file location once it is collected. You could also use dir tech-support:/ to list the collected files.**Example**

```
sonic# show tech-support status  
Status: Completed  
File Name: /var/dump/sonic_dump_sonic_20220321_145328.tar.gz
```

Releases

4.0 or later

show tech-support terminal

Displays the contents of the show tech-support .tar.gz output file on a terminal used to connect to a switch.

Command show tech-support terminal**Options** None**Modes** EXEC**Usage** When you use the show tech-support terminal command, no tar.gz output file created. Using the show tech-support terminal command allows you to log in to a switch and view and capture

technical support output without having to wait for the show tech-support tar.gz to complete and to transfer the tech-support data to a remote device.

Example

```
sonic# show tech-support terminal
*****
***#:sonic::tech-support-terminal:## show clock
Mon 16 Oct 2023 04:54:26 PM UTC
*****
***#:sonic::tech-support-terminal:## show version

Software Version   : rel_dell_sonic_4.x_share.1273-d83912624
Product          : Generic
Distribution       : Debian 10.13
Kernel            : 5.10.0-21-amd64
Config DB Version : version_4_2_1
Build Commit      : d83912624
Build Date        : Thu Oct 12 09:21:41 UTC 2023
Built By          : dngnetbuild.svc@jenkinsworker-eqx-03
Platform          : x86_64-dellemi_s5212f_c3538-r0
HwSKU             : DellEMC-S5212f-P-25G
ASIC              : broadcom
Hardware Version  : A06
Serial Number     : TH0VK93CCET0021800DZ
Uptime             : 16:54:28 up 2 days, 21:39, 2 users, load average: 1.44,
1.83, 1.70
Mfg               : Dell EMC

REPOSITORY        TAG                      IMAGE ID      SIZE
docker-database  latest                   8a121a2081f3  628MB
docker-database  rel_dell_sonic_4.x_share.1273-d83912624 8a121a2081f3  628MB
...
*****
***#:sonic::tech-support-terminal:## show uptime
2 days, 21 hours, 39 minutes
*****
***#:sonic::tech-support-terminal:## show users
admin    pts/0        2023-10-13 19:21 (100.64.53.225)
admin    pts/1        2023-10-16 16:53 (100.64.53.225)
*****
***#:sonic::tech-support-terminal:## show image list
Current: SONiC-OS-rel_dell_sonic_4.x_share.1273-d83912624
Next: SONiC-OS-rel_dell_sonic_4.x_share.1273-d83912624
Available:
SONiC-OS-rel_dell_sonic_4.1.x_share.236-a56ad2029
SONiC-OS-rel_dell_sonic_4.x_share.1273-d83912624
*****
***#:sonic::tech-support-terminal:## show image patch list
-----
-----  
Id      Tag                  Date      DependsOn
-----  
-----  
*****  
***#:sonic::tech-support-terminal:## show image status
-----  
Global operation status : GLOBAL_STATE_IDLE
-----  
*****  
***#:sonic::tech-support-terminal:## show system status detail
System is ready
Service-Name  Service-Status  App-Ready-Status  Down-Reason  Status-
UpdateTime
...
...
```

Releases

4.2.0 or later

show threshold breaches

Displays information about threshold breach events recorded by the system.

Command	show threshold breaches
Options	None
Modes	EXEC

Usage	Use the <code>clear threshold breach</code> to clear the threshold breach events.
Example	<pre>sonic# show threshold breaches ----- Event-id Buffer Type Port Index Breach Value(%) Time-stamp ----- 2 priority-group shared Ethernet0 7 77 2020-04-14-11:35:20 3 queue unicast Ethernet0 5 45 2020-04-17-11:30:20</pre>
Releases	3.1 or later

show threshold buffer-pool

Displays buffer-pool threshold configuration.

Command	<code>show threshold buffer-pool</code>
Options	None
Modes	EXEC
Usage	Use this command to view buffer-pool threshold configuration.
Example	<pre>sonic# show threshold buffer-pool ----- pool_name type threshold ----- egress_lossless_pool multicast 2</pre>
Releases	3.1 or later

show threshold device

Displays device buffer threshold configuration.

Command	<code>show threshold device</code>
Options	None
Modes	EXEC
Usage	Use this command to view the device buffer threshold configuration.
Examples	<pre>sonic# show threshold device Threshold: 80</pre>
Releases	4.0 or later

show threshold priority-group

Displays priority-group threshold configuration for all priority groups in all interfaces.

Command	<code>show threshold priority-group {headroom shared}</code>
Options	<ul style="list-style-type: none"> • <code>headroom</code>—Displays the headroom buffer. • <code>shared</code>—Displays the shared buffer.
Modes	EXEC
Usage	Use this command to view the priority-group threshold configuration for all priority groups in all interfaces.

Examples

```
sonic# show threshold priority-group
  headroom  choose headroom as threshold buffer type
  shared     choose shared as threshold buffer type

z9264f-01# show threshold priority-group headroom
-----
Port          PG0   PG1   PG2   PG3   PG4   PG5   PG6   PG7
-----
Ethernet0      0     0     0     0     0     0     0     0
Ethernet4      0     0     0     0     0     0     0     0
Ethernet8      0     0     0     0     0     0     0     0
Ethernet12     0     0     0     0     0     0     0     0
Ethernet16     0     0     0     0     0     0     0     0
Ethernet20     0     0     0     0     0     0     0     0
Ethernet24     0     0     0     0     0     0     0     0
Ethernet28     0     0     0     0     0     0     0     0
Ethernet32     0     0     0     0     0     0     0     0
Ethernet36     0     0     0     0     0     0     0     0
Ethernet40     0     0     0     0     0     0     0     0
Ethernet44     0     0     0     0     0     0     0     0
Ethernet48     0     0     0     0     0     0     0     0
Ethernet52     0     0     0     0     0     0     0     0
Ethernet56     0     0     0     0     0     0     0     0
Ethernet57     0     0     0     0     0     0     0     0
Ethernet58     0     0     0     0     0     0     0     0
Ethernet59     0     0     0     0     0     0     0     0
Ethernet60     0     0     0     0     0     0     0     0
Ethernet64     0     0     0     0     0     0     0     0
Ethernet65     0     0     0     0     0     0     0     0
--more--
```

```
sonic# show threshold priority-group shared
-----
Port          PG0   PG1   PG2   PG3   PG4   PG5   PG6   PG7
-----
Ethernet0      0     0     0     0     0     0     0     0
Ethernet4      0     0     0     0     0     0     0     0
Ethernet8      0     0     0     0     0     0     0     0
Ethernet12     0     0     0     0     0     0     0     0
Ethernet16     0     0     0     0     0     0     0     0
Ethernet20     0     0     0     0     0     0     0     0
Ethernet24     0     0     0     0     0     0     0     0
Ethernet28     0     0     0     0     0     0     0     0
Ethernet32     0     0     0     0     0     0     0     0
Ethernet36     0     0     0     0     0     0     0     0
Ethernet40     0     0     0     0     0     0     0     0
Ethernet44     0     0     0     0     0     0     0     0
Ethernet48     0     0     0     0     0     0     0     0
Ethernet52     0     0     0     0     0     0     0     0
Ethernet56     0     0     0     0     0     0     0     0
Ethernet57     0     0     0     0     0     0     0     0
Ethernet58     0     0     0     0     0     0     0     0
Ethernet59     0     0     0     0     0     0     0     0
Ethernet60     0     0     0     0     0     0     0     0
Ethernet64     0     0     0     0     0     0     0     0
Ethernet65     0     0     0     0     0     0     0     0
--more--
```

Releases

3.1 or later

show threshold queue

Displays queue threshold configuration.

Command `show threshold queue {CPU | multicast | unicast}`

Options • CPU—Displays the threshold CPU queue.

- **multicast**—Displays the multicast as `queue_buffer_type`.
- **unicast**—Displays unicast as `queue_buffer_type`.

Modes

EXEC

Usage

Use this command to view the queue threshold configuration for CPU and Ethernet interfaces.

Examples

```
sonic# show threshold queue CPU
-----
      Queue          Percent
-----
CPU:0           0
CPU:1           0
CPU:2           0
CPU:3           0
CPU:4           0
CPU:5           0
CPU:6           0
CPU:7           0
CPU:8           0
CPU:9           0
CPU:10          0
CPU:11          0
CPU:12          0
CPU:13          0
CPU:14          0
CPU:15          0
CPU:16          0
CPU:17          0
CPU:18          0
CPU:19          0
CPU:20          0
--more--
```

```
sonic# show threshold queue multicast
-----
```

Port	MC0	MC1	MC2	MC3	MC4	MC5	MC6	MC7
Ethernet0	0	0	0	0	0	0	0	0
Ethernet4	0	0	0	0	0	0	0	0
Ethernet8	0	0	0	0	0	0	0	0
Ethernet12	0	0	0	0	0	0	0	0
Ethernet16	0	0	0	0	0	0	0	0
Ethernet20	0	0	0	0	0	0	0	0
Ethernet24	0	0	0	0	0	0	0	0
Ethernet28	0	0	0	0	0	0	0	0
Ethernet32	0	0	0	0	0	0	0	0
Ethernet36	0	0	0	0	0	0	0	0
Ethernet40	0	0	0	0	0	0	0	0
Ethernet44	0	0	0	0	0	0	0	0
Ethernet48	0	0	0	0	0	0	0	0
Ethernet52	0	0	0	0	0	0	0	0
Ethernet56	0	0	0	0	0	0	0	0
Ethernet57	0	0	0	0	0	0	0	0
Ethernet58	0	0	0	0	0	0	0	0
Ethernet59	0	0	0	0	0	0	0	0
Ethernet60	0	0	0	0	0	0	0	0
Ethernet64	0	0	0	0	0	0	0	0
Ethernet65	0	0	0	0	0	0	0	0

```
--more--
```

```
sonic# show threshold queue unicast
-----
```

Port	UC0	UC1	UC2	UC3	UC4	UC5	UC6	UC7
Ethernet0	0	0	0	0	0	0	0	0
Ethernet4	0	0	0	0	0	0	0	0
Ethernet8	0	0	0	0	0	0	0	0
Ethernet12	0	0	0	0	0	0	0	0
Ethernet16	0	0	0	0	0	0	0	0

Ethernet20	0	0	0	0	0	0	0	0
Ethernet24	0	0	0	0	0	0	0	0
Ethernet28	0	0	0	0	0	0	0	0
Ethernet32	0	0	0	0	0	0	0	0
Ethernet36	0	0	0	0	0	0	0	0
Ethernet40	0	0	0	0	0	0	0	0
Ethernet44	0	0	0	0	0	0	0	0
Ethernet48	0	0	0	0	0	0	0	0
Ethernet52	0	0	0	0	0	0	0	0
Ethernet56	0	0	0	0	0	0	0	0
Ethernet57	0	0	0	0	0	0	0	0
Ethernet58	0	0	0	0	0	0	0	0
Ethernet59	0	0	0	0	0	0	0	0
Ethernet60	0	0	0	0	0	0	0	0
Ethernet64	0	0	0	0	0	0	0	0
Ethernet65	0	0	0	0	0	0	0	0

--more--

Releases 3.1 or later

show tpcm list

View the third-party containers installed on the switch.

Command show tpcm list

Options None

Modes EXEC

Usage Information on each TPC image, VRF in which the container is running, and current status is displayed.

Example

```
sonic# show tpcm list
CONTAINER NAME IMAGE TAG VRF CONFIGURED/RUNNING STATUS
TEST mydocker:latest default/default Up 8 seconds
```

Releases 4.1.0 or later

show tpcm name

Displays the third-party containers installed on the switch.

Command show tpcm name *name*

Options *name*—Name of the container

Modes EXEC

Usage Use this command to display the third-party containers installed on the switch based on the container name.

Examples

```
sonic# show tpcm name telegraf
TPC docker args:
--network=host -v /etc/sonic/frr:/etc/sonic/frr -v /etc/resolv.conf:/etc/
resolv.conf --hostname=sonic
TPC container CMD:

TPC configs      :
--cpu-period=100000 --cpu-quota=20000 --cpu-shares=0 --cpus=0 --
memory=618m --memory-swap=618m
--memory-reservation=0
TPC service file:
```

```

[Unit]
Description=telegraf docker
After=docker.service

[Service]
ExecStartPre=/usr/local/bin/tpc.sh start telegraf telegraf:37141b42
ExecStart=/usr/local/bin/tpc.sh wait telegraf telegraf:37141b42
ExecStop=/usr/local/bin/tpc.sh stop telegraf telegraf:37141b42
StandardOutput=syslog
StandardError=syslog
Restart=on-failure
RestartSec=60

[Install]
WantedBy=tpcm.service
WantedBy=tpcm-user.target

TPC service drop in file:
[Unit]
After=systemready.service

TPC VRF name      :
default

```

Releases 4.1.0 or later

show udld global

Displays global-level unidirectional link detection protocol (UDLD) information.

Command	show udld global
Options	None
Modes	EXEC
Usage	After enabling UDLD at a global-level or modifying UDLD attributes, use this command to check global-level UDLD information.

Example

```

sonic# show udld global
UDLD Global Information
  Admin State      : UDLD Enabled
  Mode             : Normal
  UDLD Message Time : 1 seconds
  UDLD Multiplier   : 3

```

Releases 3.0 or later

show udld interface

Displays unidirectional link detection protocol (UDLD) information and neighbors detail for a specific interface.

Command	show udld interface <i>interface-name</i>
Options	<i>interface-name</i> — Name of interface to display UDLD information

Modes	EXEC
Usage	After enabling UDLD at an interface-level, use this command to view UDLD information and neighbors attached to this interface.
Example	<pre>sonic# show udld interface Ethernet28 UDLD information for Ethernet28 UDLD Admin State: Enabled Mode: Normal Status: Bidirectional Local device id: 3c2c.992d.8201 Local port id : Ethernet28 Local device name: Sonic Message time: 1 Timeout interval: 3 Neighbor Entry 1 ----- Neighbor device id: 3c2c.992d.8235 Neighbor port id: Ethernet28 Neighbor device name: Sonic Neighbor message time: 1 Neighbor timeout interval: 3</pre>
Releases	3.0 or later

show udld neighbors

Displays unidirectional link detection protocol (UDLD) neighbors information

Command	show udld neighbors
Options	None
Modes	EXEC
Usage	After enabling UDLD at global and interface levels, use this command to view all UDLD neighbors information.
Example	<pre>sonic# show udld neighbors Port Device Name Device ID Port ID Neighbor State ----- ----- Ethernet1 Sonic 3c2c.992d.8201 Ethernet0 Bidirectional Ethernet28 Sonic 3c2c.992d.8201 Ethernet29 Bidirectional</pre>
Releases	3.0 or later

show udld statistics

Displays unidirectional link detection protocol (UDLD) statistics for all interfaces.

Command	show udld statistics
Options	None
Modes	EXEC
Usage	Use this command to view the UDLD statistics for all interfaces.
Example	<pre>sonic# show udld statistics UDLD Interface statistics for Ethernet0 Frames transmitted: 10 Frames received: 9 Frames with error: 0 UDLD Interface statistics for Ethernet1</pre>

```
Frames transmitted:      5
Frames received:        8
Frames with error:      0
```

Releases 3.0 or later

show udld statistics interface

Displays unidirectional link detection protocol (UDLD) statistics for a specific interface.

Command	<code>show udld statistics interface <i>interface-name</i></code>
Options	<code>interface <i>interface-name</i></code> —Interface name to view UDLD statistics
Modes	EXEC
Usage	Use this command to view the UDLD statistics for a specific interface.
Example	<pre>sonic# show udld statistics interface Ethernet0 UDLD Interface statistics for Ethernet0 Frames transmitted: 10 Frames received: 9 Frames with error: 0</pre>

Releases 3.0 or later

show uptime

Displays system uptime information.

Command	<code>show uptime</code>
Options	None
Modes	EXEC
Usage	Use this command to view the information about how long the system has been running.
Example	<pre>sonic# show uptime 0 days, 16 hours, 55 minutes</pre>

Releases 3.1 or later

show users

Displays information about the active users who are logged in to the switch, such as role, connected terminal, idle time, and so on.

Command	<code>show users [all configured]</code>
Options	<ul style="list-style-type: none"><code>all</code>—Displays all usernames and their roles.<code>configured</code>—Displays usernames and their roles that are configured locally.
Modes	EXEC
Usage	The <code>show users</code> output displays the users who logged on locally to the switch and users who accessed the switch through a remote login; for example, using RADIUS or TACACS authentication. Description about the attributes in the command output: <ul style="list-style-type: none"><code>LINE</code>—The terminal that is associated with the user.<code>USER</code>—The username.

- **ROLE**—The user roles that are configured for the user.
- **APPLICATION**—Displays which application the user uses to log in to Enterprise SONiC.
- **IDLE**—The idle time of the user. If the user idle time exceeds one hour, the idle time is displayed in HH:MM:SS format. If the user idle time is less than one hour, the idle time is displayed in MM:SS format.
- **LOGIN-TIME**—Displays the user login time.
- **LOCATION**—The host details of the console or SSH user such as the IP address.

Example

```
sonic# show users
INDEX LINE      USER     ROLE      APPLICATION    IDLE    LOGIN-TIME
LOCATION
1       pts/0     admin    admin     bash           2.00s   13-12-2023
08:04:20.855559 10.107.106.113 [ssh]
2       ttys0     admin    admin     bash           04:57   13-12-2023
08:14:11.298683 console
```

Releases

3.1 or later

show users configured

Displays information on the locally configured users who are logged in to the switch.

Command `show users configured`

Options None

Modes EXEC

Usage In Release 4.1.0 and later, users who are locally configured with the `username password role` command are not displayed in `show running-configuration | grep user` output and in the config_db.json file. To monitor the locally configured users who are logged in to the switch, you must use the `show users configured` command.

Example

```
sonic# show users configured
-----
User                      Role(s)
-----
JustAnything              operator
Kenna                     operator
admin                     admin
babuji                    admin
dellradius15              secadmin,operator
isg-admin                 operator
ldapuser                  admin
localprocessdmzscan       operator
processdmzscan            operator
t088788                  admin
t098888                  admin
tacacsadmin               operator
tacacsuser                operator
```

Releases

4.1.0 or later

show version

Displays software version information.

Command `show version`

Options None

Modes EXEC

Usage

Use this command to view the software version that is being installed on the switch, the type of ASIC, the uptime, and the hardware version information.

Example

```
sonic# show version

Software Version : 4.4.0-Cloud_Premium_Build106
Product          : Enterprise SONiC Distribution by Dell Technologies
Distribution     : Debian 11.9
Kernel           : 5.10.0-21-amd64
Config DB Version: version 4_3_1
Build Commit     : 8595cec683
Build Date       : Sun Jul  7 14:06:57 UTC 2024
Built By         : sonicbld@bld-lvn-csg-10
Platform         : x86_64-dell_z9864f-r0
HwSKU            : Dell-z9864f-064
ASIC             : broadcom
Serial Number    :
Uptime           : 20:24:24 up 0 min, 1 user, load average: 4.37, 1.08, 0.36

REPOSITORY          TAG      IMAGE ID   SIZE
docker-database    4.4.0-Cloud_Premium_Build106 6daaca363758
400MB
docker-database    latest    6daaca363758
400MB
docker-dhcp-relay-cloud-advanced 4.4.0-Cloud_Premium_Build106 d0f2d9bb80bc
452MB
docker-dhcp-relay-cloud-advanced latest    d0f2d9bb80bc
452MB
docker-eventd      4.4.0-Cloud_Premium_Build106 5fe29840d970
402MB
docker-eventd      latest    5fe29840d970
402MB
docker-fpm-frr     4.4.0-Cloud_Premium_Build106 31e8678ad6fb
484MB
docker-fpm-frr     latest    31e8678ad6fb
484MB
docker-gbsyncd-brcm 4.4.0-Cloud_Premium_Build106 76fbf6736e48
932MB
docker-gbsyncd-brcm latest    76fbf6736e48
932MB
docker-iccpd       4.4.0-Cloud_Premium_Build106 e9c10f757c3f
451MB
docker-iccpd       latest    e9c10f757c3f
451MB
docker-lldp        4.4.0-Cloud_Premium_Build106 d0445105f4ec
490MB
docker-lldp        latest    d0445105f4ec
490MB
docker-nat         4.4.0-Cloud_Premium_Build106 3e3aebf63cc4
450MB
docker-nat         latest    3e3aebf63cc4
450MB
docker-platform-monitor 4.4.0-Cloud_Premium_Build106 a224dc75f700
576MB
docker-platform-monitor latest    a224dc75f700
576MB
docker-router-advertiser 4.4.0-Cloud_Premium_Build106 10b1f3000ed3
400MB
docker-router-advertiser latest    10b1f3000ed3
400MB
docker-sflow        4.4.0-Cloud_Premium_Build106 3e6be54cc324
450MB
docker-sflow        latest    3e6be54cc324
450MB
docker-snmp         4.4.0-Cloud_Premium_Build106 fde213b4beab
429MB
docker-snmp         latest    fde213b4beab
429MB
docker-sonic-mgmt-framework 4.4.0-Cloud_Premium_Build106 2c98e0666f39
656MB
docker-sonic-mgmt-framework latest    2c98e0666f39
656MB
docker-sonic-telemetry 4.4.0-Cloud_Premium_Build106 f2a373ebbfbe
582MB
docker-sonic-telemetry latest    f2a373ebbfbe
582MB
docker-swss-brcm-cld-advanced 4.4.0-Cloud_Premium_Build106 653b62b7dff0
445MB
docker-swss-brcm-cld-advanced latest    653b62b7dff0
```

445MB			
docker-syncd-brcm-cld-advanced	4.4.0-Cloud_Premium_Build106	cb5194da67e5	
900MB	latest	cb5194da67e5	
docker-syncd-brcm-cld-advanced			
900MB			
docker-tam	4.4.0-Cloud_Premium_Build106	00ee9a02af1b	
442MB	latest	00ee9a02af1b	
docker-tam			
442MB			
docker-teamd	4.4.0-Cloud_Premium_Build106	9dfb60527c59	
448MB	latest	9dfb60527c59	
docker-teamd			
448MB			
docker-udld	4.4.0-Cloud_Premium_Build106	20a37f2744c9	
454MB	latest	20a37f2744c9	
docker-udld			
454MB			
docker-vrrp	4.4.0-Cloud_Premium_Build106	0758a10afa8b	
456MB	latest	0758a10afa8b	
docker-vrrp			
456MB			

Releases 3.0 or later

show Vlan

Displays the current VLAN configuration.

Command show Vlan [id]

Options Vlan id — (Optional) VLAN ID (1 to 4094)

Command mode EXEC

Usage Use this command to view the current VLAN configuration, or for a specific VLAN interface.

Examples

```
sonic# show Vlan
Q: A - Access (Untagged), T - Tagged
NUM      Status      Q Ports          Autostate   Dynamic
100     Inactive    T Ethernet4      Enable       No
                    T Ethernet32
                    A Ethernet8
```

Releases 3.0 or later

show vrrp

Displays IPv4 VRRP instance information.

Command show vrrp [interface {ifname {vrid id}}]

- **interface ifname**—(Optional) Interface name (up to 63 characters)
- **vrid id**—(Optional) VRID identifier

Modes EXEC

Usage Use this command to view the IPv4 VRRP instance information.

Examples

```
sonic# show vrrp
      Interface_Name  VRID  State      VIP          Cfg_Prio  Curr_Prio
      Ethernet4        1    Master    40.0.0.5      120        120
      Ethernet8        2    Backup    80.0.0.5      100        100
```

```
sonic# show vrrp interface Ethernet4 vrid 1
      Ethernet4, VRID 1
      Version is 2
      State is Master
      Virtual IP address:
```

```

40.0.0.5
Virtual MAC address is 0000.5e00.0101
Track interface:
None
Configured Priority is 100, Current Priority is 100
Advertisement interval is 1 sec
Preemption is enabled

```

Releases

3.1 or later

show vrrp6

Displays IPv6 VRRP instance information.

Command show vrrp6 [interface (ifname {vrid id})]

- Options**
- **interface ifname**—(Optional) Interface name (up to 63 characters)
 - **vrid id**—(Optional) VRID identifier

Modes EXEC

Usage

Use this command to view the IPv6 VRRP instance information.

Examples

```

sonic# show vrrp6
      Interface_Name    VRID    State      VIP      Cfg_Prio Curr_Prio
      Ethernet4          1       Master    40::5    120        120
      Ethernet8          2       Backup   80::5    100        100

```

```

sonic# show vrrp6 interface Ethernet4 vrid 1
      Ethernet4, VRID 1
      Version is 3
      State is Master
      Virtual IP address:
      40::5
      Virtual MAC address is 0000.5e00.0201
      Track interface:
      None
      Configured Priority is 100, Current Priority is 100
      Advertisement interval is 1 sec
      Preemption is enabled

```

Releases

3.1 or later

show vxlan counters

Displays VXLAN tunnel counters per remote VTEP or all remote VTEPs.

Command show vxlan counters [vtep-ip]

Options vtep-ip—(Optional) Remote VTEP IP address

Modes EXEC

Usage

Use this command to view the packet statistics on VXLAN tunnels.

Example

For all:

```

sonic# show vxlan counters
Polling Rate      : 5 seconds
-----
Interface      RX_BYTES_OK RX_OK      RX_BPS  RX_PPS  TX_BYTES_OK TX_OK    TX_BPS  TX_PPS
-----
EVPN_1.1.1.1    224452400   1122262   105349   527     14670      112      0       0
EVPN_1.1.1.2    112226200   561131     0         0       14670      112      0       0

```

For specific VXLAN tunnel:

```
sonic# show vxlan counters 1.1.1.1
Polling Rate      : 5 seconds
-----
Interface      RX_BYTES_OK RX_OK      RX_BPS   RX_PPS TX_BYTES_OK  TX_OK    TX_BPS   TX_PPS
-----
-----
```

Interface	RX_BYTES_OK	RX_OK	RX_BPS	RX_PPS	TX_BYTES_OK	TX_OK	TX_BPS	TX_PPS
EVPN_1.1.1.1	224452400	1122262	105349	527	14670	112	0	0

Releases 4.0 or later

show vxlan interface

Displays the VXLAN interface configuration.

Command show vxlan interface

Options None

Modes EXEC

Usage Use this command to view the VXLAN interface configuration.

Example

```
sonic# show vxlan interface

VTEP Name      : vtep1
VTEP Source IP : 1.1.1.1
VTEP Primary IP : 2.2.2.2
VTEP External IP : 10.10.10.10
EVPN NVO Name  : nvol
EVPN VTEP      : vtep1
Source Interface : Loopback10
Primary IP interface : Loopback20
External IP interface: Loopback30
```

Releases 3.0 or later

show vxlan remote mac

Displays the tenant MAC addresses and tenant VLANs learned from a specified, or all VXLAN tunnel source IP addresses.

Command show vxlan remote mac [remote_ip_addr]

Options remote mac *remote_ip_addr*—(Optional) Remote IP address in A.B.C.D format

Modes EXEC

Usage Use this command to view the tenant MAC addresses and tenant VLANs learned from a specified, or all VXLAN tunnel source IP addresses.

Examples

```
leaf1# show vxlan remote mac
      Vlan          Mac           Type     Tunnel/Intf      Group      VNI
      ===          ===           ===      =====      =====      ===
      Vlan1        00:44:b2:11:00:01    dynamic      5.5.5.5      internal
      100001
      Vlan1        00:44:b2:11:00:02    dynamic      6.6.6.6      5.5.5.5      internal
      100001
                                         6.6.6.6
```

```

Vlan1    00:44:b2:11:00:03    dynamic    5.5.5.5    internal
100001

sonic# show vxlan remote mac 3.3.3.3
Vlan      Mac          Type     Tunnel   Group   VNI
=====  ======  =====  ======  =====  =====
===== 
Vlan1003  00:c0:05:31:00:01  dynamic   3.3.3.3  external  10003
Vlan1003  00:c0:05:31:00:02  dynamic   3.3.3.3  external  10003
Total count : 2

```

Releases 3.0 or later

show vxlan remote mac count

Displays the number of remote MACs available.

Command show vxlan remote mac count [*remote_ip_addr*]
Options *remote_ip_addr*—(Optional) Remote IP address in A.B.C.D format
Modes EXEC
Usage Use this command to view the number of remote MACs available.
Example

```

sonic# show vxlan remote mac count
Total Count: 5876

```

Releases 3.1 or later

show vxlan remote nexthop-group

Displays the remote IP addresses in the next-hop group (NHG) for a VTEP.

Command show vxlan remote nexthop-group
Options None
Modes EXEC
Usage Multihomed VTEPs display the port channel for their Ethernet segment in the Local Members column.
Examples

```

sonic# show vxlan remote nexthop-group
      NHG      Rmote VTEPs      Local Members
      ===      ======  =====
      536870913  2.2.2.2
                  3.3.3.3
                  4.4.4.4

      536870914  3.3.3.3
                  4.4.4.4
                  5.5.5.5
                  6.6.6.6

      536870916  5.5.5.5
                  6.6.6.6

```

Releases 4.2.0 or later

show vxlan remote vni

Displays all VLANs learned from the specified remote IP or all remote IPs.

Command	show vxlan remote vni [remote_ip_addr]
Options	vni remote_ip_addr—(Optional) Remote IP address in A.B.C.D format
Modes	EXEC
Usage	Use this command to retrieve the list of VNIs mapped to VLANs from all remote VTEPs or the specified remote VTEP.

Examples

```
sonic# show vxlan remote vni
Vlan      Tunnel      Group      VNI
=====  ======  ======  =====
Vlan1001  1.0.3.255  internal   1001
Vlan1001  1.0.5.1    external   100001
Vlan1002  1.0.3.255  internal   1002
Vlan1002  1.0.5.1    external   100002
```

```
sonic# show vxlan remote vni 3.3.3.3
Vlan      Tunnel      Group      VNI
=====  ======  ======  =====
Vlan1001  3.3.3.3    internal   1001
Total count : 1
```

Releases	3.0 or later
-----------------	--------------

show vxlan remote vni count

Displays the number of VLANs extended to remote VTEPs.

Command	show vxlan remote vni count [remote_ip_addr]
Options	remote_ip_addr—(Optional) Remote IP address in A.B.C.D format
Modes	EXEC
Usage	Use this command to view the number of VLANs extended to remote VTEPs.
Example	<pre>sonic# show vxlan remote vni count Total Count: 650</pre>

Releases	3.1 or later
-----------------	--------------

show vxlan tunnel

Displays all discovered tunnels.

Command	show vxlan tunnel
Options	None
Modes	EXEC
Usage	Use this command to retrieve the VXLAN tunnel information and its status.
Example	<pre>show vxlan tunnel Name SIP DIP source Group DVNI operstatus ===== ====== ====== ====== ====== ===== ===== EVPN_1.0.1.1 1.0.1.255 1.0.1.1 EVPN external yes oper_up</pre>

EVPN_1.0.3.1	1.0.1.255	1.0.3.1	EVPN	external	yes	oper_up
EVPN_1.0.3.255	1.0.1.255	1.0.3.255	EVPN	internal	no	oper_up
EVPN_1.0.4.1	1.0.1.255	1.0.4.1	EVPN	external	yes	oper_up
EVPN_1.0.5.1	1.0.1.255	1.0.5.1	EVPN	external	yes	oper_up

Releases 3.0 or later

show vxlan tunnel count

Displays the number of remote VTEPs.

Command show vxlan tunnel count

Options None

Modes EXEC

Usage Use this command to view the number of remote VTEPs.

Example

```
sonic# show vxlan tunnel count
Total Count: 52
```

Releases 3.1 or later

show vxlan vlanvnimap

Displays all VLAN VNI mappings.

Command show vxlan vlanvnimap

Options None

Modes EXEC

Usage Use this command to retrieve the VLAN VNI map configurations of the local VTEPs.

Example

```
sonic# show vxlan vlanvnimap
      VLAN      VNI
      ===      ===
      Vlan1    100001
      Vlan2    100002
      Vlan3    100003
      Vlan4    100004
      Vlan5    100005
      Vlan6    100006
      Vlan7    100007
      Vlan8    100008
      Vlan9    100009
      Vlan10   100010
      Vlan11   100011
      Vlan12   100012
      Vlan13   100013
      Vlan14   100014
      Vlan15   100015
      Vlan16   100016
      Vlan17   100017
      Vlan18   100018
      Vlan19   100019
      Vlan20   100020
      Vlan21   100021
      Vlan22   100022
```

Releases 3.0 or later

show vxlan vlanvnimap count

Displays the number of VLAN VNI mappings.

Command show vxlan vlanvnimap count

Options None

Modes EXEC

Usage Use this command to view the number of VLAN VNI mappings.

Example

```
sonic# show vxlan vlanvnimap count
Total Count: 457
```

Releases 3.1 or later

show vxlan vrfvnimap

Displays all VRF VNI mappings.

Command show vxlan vrfvnimap

Options None

Modes EXEC

Usage Use this command to display the VRF VNI map configurations.

Example

```
leaf1# show vxlan vrfvnimap

      VRF          VNI
      =====        =====
Vrf001        1103001
Vrf002        1103002
Vrf003        1103003
Vrf004        1103004
Vrf005        1103005
Vrf006        1103006
Vrf007        1103007
Vrf008        1103008
Vrf009        1103009
Vrf010        1103010
Vrf011        1103011
Vrf012        1103012
Vrf013        1103013
Vrf014        1103014
Vrf015        1103015
Vrf016        1103016
Vrf017        1103017
Vrf018        1103018
Vrf019        1103019
Vrf020        1103020
Vrf021        1103021
Vrf022        1103022
```

Releases 3.0 or later

show vxlan vrfvnimap count

Displays the number of VRF VNI mappings.

Command show vxlan vrfvnimap count

Options	None
Modes	EXEC
Usage	Use this command to view the number of VRF VNI mappings.
Example	<pre>sonic# show vxlan vrfvnimap count Total Count: 1</pre>
Releases	3.1 or later

show warm-restart

Displays the current warm restart information.

Command	show warm-restart [check config system]
Options	<ul style="list-style-type: none"> • check— Displays if there are any pending entries. • config— Displays warm restart configuration information. • system— Displays warm restart system state information.
Modes	EXEC
Usage	Use the <code>show warm-restart</code> command to check the status of a warm restart.
Example	The following information is displayed after a reconciliation:

```
sonic# show warm-restart
-----
Module          Restore_count   Status
-----
aclsvcd        1               reconciled
bgp            1               reconciled
fdbsyncd       1               reconciled
gearsyncd      1
intfmgrd       1               reconciled
iphelpermgr    1
l2mcmgrd       2
loopbackmgrd   1               reconciled
natsyncd       1               reconciled
nbrmrgd        1
neighsyncd     1               reconciled
nhg            1               reconciled
orchagent      1               reconciled
portmrgd       1
portsyncd      1
resrcmrgd      0
stpmrgd        2
switchmrgd    1
syncd          1
system         1               reconciled
teammrgd       1
teamsyncd      1               reconciled
udldmrgd       1
vlanmrgd       1               reconciled
vrfmrgd        1               reconciled
vrrpmrgd       1
vrrpsyncd      1               reconciled
vxlanmrgd      1               reconciled
warm-shutdown  0               pre-shutdown-succeeded
xcvrd          0
```

The `show warm-restart check` output shows if there are any pending entries:

```
sonic# show warm-restart check
No pending entries
```

The `show warm-restart system` output displays the system status.

```
sonic# show warm-restart system
-----
Module           Restore_count   Status
-----
system          1                reconciled
```

The `show warm-restart config` output displays the warm-restart configuration if it is enabled.

```
sonic# show warm-restart config
-----
-----
Module      Enable      Timer Name      Timer Duration      End-of-
Initial Update (EOIU)                                Duration
-----
bgp        False       bgp_timer        240                  False
```

Releases 4.2.0 or later

show watermark interval

Displays the configured watermark snapshot interval.

Command `show watermark interval`

Options None

Modes EXEC

Usage Use this command to view the configured watermark snapshot interval.

Example

```
sonic# show watermark interval
Snapshot interval : 220 seconds
```

Releases 3.1 or later

show watermark telemetry

Displays the configured watermark telemetry interval.

Command `show watermark telemetry interval`

Options None

Modes EXEC

Usage Use this command to view the configured watermark telemetry interval.

Example

```
sonic# show watermark telemetry interval
interval : 220 seconds
```

Releases 3.1 or later

show ztp-status

Displays the current zero-touch provisioning (ZTP) status.

Command `show ztp-status`

Options	None
Mode	EXEC
Usage	<ul style="list-style-type: none"> • ZTP Admin Mode—Displays if ZTP is administratively enabled or disabled (True or False). • ZTP Service—Displays ZTP status. <ul style="list-style-type: none"> ◦ Active Discovery—ZTP is operational and performing DHCP discovery to learn the switch provisioning. ◦ Processing—ZTP has discovered the switch provisioning information and is processing it. • ZTP Status—Displays the current state and results of ZTP sessions. <ul style="list-style-type: none"> ◦ IN-PROGRESS—ZTP is processing switch configuration information. ◦ SUCCESS—ZTP has successfully processed the switch configuration information. ◦ FAILED—ZTP failed to process the switch configuration information. ◦ Not Started—ZTP has not started processing the discovered switch configuration information. • ZTP Source—Displays the DHCP option and interface name from which the switch configuration information originated. • Runtime—Displays the time that is taken for the ZTP process to complete; for individual configuration, it indicates the time that is taken to process the associated configuration. • Timestamp—Displays the date and time stamp when the status field last changed. • ZTP JSON Version—Version of the ZTP JSON file used for processing switch configuration. • Status—Displays the current state and result of processing a ZTP JSON file. <ul style="list-style-type: none"> ◦ IN-PROGRESS—Configuration currently in-progress. ◦ SUCCESS—Configuration was processed successfully. ◦ FAILED—Configuration failed to run successfully. ◦ Not Started—ZTP has not started processing the configuration. ◦ DISABLED—Configuration has been marked as disabled and cannot be processed. • Exit Codes—Displays the program exit code of the configuration that was processed; a nonzero exit code indicates that the configuration failed to run successfully. • Ignore Results—True indicates that the result of processing a configuration section is ignored and not used to evaluate the overall ZTP result. • Activity String—Displays the current activity string, including the current action that is performed by ZTP, and how long it has been performing the activity.

Example

```
sonic# show ztp-status
=====
ZTP
=====
ZTP Admin Mode : True
ZTP Service    : Inactive
ZTP Status     : SUCCESS
ZTP Source     : dhcp-opt67 (Management0)
Runtime        : 05m 31s
Timestamp      : 2020-09-11 19:12:16 UTC
ZTP JSON Version : 1.0

ZTP Service is not running

-----
01-configdb-json
-----
Status        : SUCCESS
Runtime       : 02m 48s
Timestamp    : 2020-09-11 19:11:55 UTC
Exit Code    : 0
Ignore Result : False

-----
02-connectivity-check
-----
Status        : SUCCESS
Runtime       : 04s
Timestamp    : 2020-09-11 19:12:16 UTC
```

```
Exit Code      : 0
Ignore Result  : False
```

Releases 3.0 or later

shutdown

Administratively shuts down an interface, or a BGP/BFD peer or neighbor.

Command shutdown

Options None

- Modes**
- INTERFACE
 - BGP-PEER
 - BGP-NEIGHBOR
 - BGP-PEER-GROUP
 - BFD

Usage Use this command to mark a physical interface or BGP peer or neighbor as unavailable for traffic. Disabling a VLAN or a port channel interface causes different behavior. When you disable a VLAN, the L3 functions within that VLAN are disabled, and L2 traffic continues to flow. Use this command on a port channel interface to disable all traffic on that interface, and the individual interfaces. The shutdown and description commands are the only commands that you can configure on an interface that is a port channel member. This command also changes the BFD session state to DOWN, disables the interface, and administratively shuts down a BGP neighbor or peer-group sessions. Use the no form of this command to enable the interface, or the BGP/BFD peer or neighbor.

Examples

```
sonic(config)# bfd
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0
sonic(config-bfd-peer)# shutdown
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# shutdown
```

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# shutdown
```

```
sonic(config-bfd-peer)# no shutdown
sonic(config-router-bgp-neighbor)# no shutdown
sonic(config-router-bgp-pg)# no shutdown
```

```
sonic(config)# interface Vlan 100
sonic(config-if-Vlan100)# shutdown
```

```
sonic(config)# interface range Vlan 1-100
sonic(config-if-range-vl**)# no shutdown
```

```
sonic(config)# interface Loopback 10
sonic(config-if-lo10)# [no] shutdown
```

Releases 3.0 or later

snmp-server agentaddress

Configures one or more SNMP agent addresses.

Command `snmp-server agentaddress host-addr {{ [port udp-port]} {[interface ifname]}}`

- Options**
- *host_addr*—Host IP address in A.B.C.D or A:B:C:D:E:F:G:H format
 - *udp_port*—(Optional) UDP port number; default 161
 - *ifname*—(Optional) Interface name (up to 32 characters)

Modes CONFIGURATION

Usage Use this command to configure an SNMP agent address and UDP port number. You can also set the UDP port number on which the SNMP server listens for requests, and the interface used by the Management port to access SNMP. Use the `no snmp-server agent-address host-addr` command to remove the SNMP agent address configuration.

Examples

```
sonic(config)# snmp-server agentaddress 1.2.3.4  
  
sonic(config)# snmp-server agentaddress 1.2.3.4 port 1024  
  
sonic(config)# snmp-server agentaddress 1.2.3.5 port 1024 interface Ethernet10  
  
sonic(config)# no snmp-server agentaddress 1.2.3.4  
sonic(config)# no snmp-server agentaddress 1.2.3.4 port 1024  
sonic(config)# no snmp-server agentaddress 1.2.3.5 port 1024 interface Ethernet10
```

Releases 3.0 or later

snmp-server community

Configures an SNMP user community.

Command `snmp-server community community-name [group group-name]`

- Options**
- *community_name*—Community name string that acts as a password for SNMP server access (up to 255 characters). A minimum of four characters is required. Using # as the first character in a community string (for example, `snmp-server community #public`) is not supported.
 - *group_name*—(Optional) Group name string for SNMP server access (up to 32 characters)

Modes CONFIGURATION

Usage Configure one or more SNMP communities and optionally associate them with a group. SNMP uses community strings, which function as passwords to allow user access to a managed switch. Community strings are sent with Get requests to retrieve information from the local SNMP agent on a switch. Use `no` form of this command to remove SNMP user community configuration. The SNMP community name should not contain any spaces, commas, or '@' symbols.

Example

```
sonic(config)# snmp-server community comm1  
  
sonic(config)# snmp-server community comm1 group group-lab  
  
sonic(config)# no snmp-server community comm1
```

Releases 3.0 or later

snmp-server contact

Configures the contact information for the organization responsible for the switch.

Command	<code>snmp-server contact <i>contact_name</i></code>
Options	<code><i>contact_name</i></code> —Specify the contact information (1 to 255 characters)
Modes	CONFIGURATION
Usage	Use this command to configure contact information (for example, phone number, email, tech support name) and the physical location (campus building, floor, room) of the local SNMP agent. Enclose each text in double quotes ("").
Examples	<pre>sonic(config)# snmp-server contact "Dell Support"</pre> <pre>sonic(config)# no snmp-server contact</pre>
Releases	3.0 or later

snmp-server enable trap

Enables all or selected SNMP traps on switch interfaces.

Command	<code>snmp-server enable trap [auth-fail bgp config-change link-down link-up ospf]</code>
Options	<ul style="list-style-type: none">• <code>auth-fail</code>—Enable SNMP authentication failure traps.• <code>bgp</code>—Enable SNMP BGP traps.• <code>config-change</code>—Enable SNMP configuration-change traps.• <code>link-down</code>—Enable SNMP link-down traps.• <code>link-up</code>—Enable SNMP link-up traps.• <code>ospf</code>—Enable SNMP OSPF traps.
Modes	CONFIGURATION
Usage	This command is disabled by default. Use the <code>snmp-server enable trap</code> basic command to enable all SNMP traps. To enable individual types of SNMP traps, re-enter the command.
Examples	<pre>sonic(config)# snmp-server enable trap</pre> <pre>sonic(config)# no snmp-server enable trap</pre> <pre>sonic(config)# snmp-server trap enable auth-fail</pre> <pre>sonic(config)# snmp-server trap enable link-down</pre> <pre>sonic(config)# snmp-server trap enable ospf</pre>
Releases	3.0 or later

snmp-server engine

Configures the SNMP engine ID.

Command	<code>snmp-server engine <i>engineID</i></code>
Options	<code><i>engineID</i></code> — Engine ID to identify the local SNMP agent on the switch as an octet colon-separated number (5 to 32 octets)
Modes	CONFIGURATION

Usage Use this command to configure the SNMP engine ID used for localizing configuration. The engine ID generates the localized keys for the authentication and privilege passwords. These passwords authenticate SNMP users and encrypt SNMP messages. If you reconfigure the engine ID, the localized keys also change, and the existing values are no longer valid. You must reconfigure SNMP users with new localized password keys. The default engine ID is derived from the device MAC address of the Management interface.

Examples

```
sonic(config)# snmp-server engine 80:00:02:b8:04:61:62:63  
sonic(config)# no snmp-server engine
```

Releases 3.0 or later

snmp-server group

Configures the views allowed for SNMP group users.

Command `snmp-server group group_name {{any | v2c | {v3 {noauth | auth | priv}}}} {[read] view_name} {[write] view_name} {[notify] view_name}`

Options

- *group_name* — Name of the group (up to 32 characters)
- any — Use any authentication method on the group
- v2c — Use no user authentication or privacy protection on the group
- v3 — Use optional user authentication and encryption for SNMP messages on the group
- auth — Authenticate group users in SNMP messages
- noauth — Do not authenticate group users or encrypt SNMP messages
- priv — Authenticate group users and encrypt or decrypt SNMP messages
- read *view_name* — Name of a read-only view (up to 32 characters)
- write *view_name* — Name of a write-only view (up to 32 characters)
- notify *view_name* — Name of a notification view (up to 32 characters)

Modes CONFIGURATION

Usage Use this command to set up the access privileges for a group of SNMP users. Configure the security level for receiving SNMP messages. Specify read-view, write-only, and/or notification access to the SNMP agent. To configure an SNMPv3 user's authentication and privacy settings, use [snmp-server user](#).

Examples

```
sonic(config)# snmp-server group group1 v2c  
sonic(config)# snmp-server group group1 v2c notify no_view  
sonic(config)# snmp-server group group-floor2 v3 priv  
sonic(config)# snmp-server group group-floor2 v3 priv read r_view write w_view notify n_view  
sonic(config)# no snmp-server group group1 v2c
```

Releases 3.0 or later

snmp-server host

Configures a host to receive SNMP notifications.

Command `snmp-server host host-addr {{community {community-name {[traps v2c]} | {[informs {[timeout time-out] {[retries retry]}}}]} {[interface ifname] | {[port udpPort]}} | {user {username {[traps {noauth | auth | priv}]}}`

```
| {[informs {noauth | auth | priv} {[timeout time-out]} {[retries  
retry]}]}]} {[interface ifname]} {| Vrf vrf-name} {[port udpPort]}}}
```

Options

- *host-addr*—IPv4 or IPv6 of the SNMP host in A.B.C.D or A:B:C:D:E:F:G:H format
- *community_name*—Community string name ((4-32 characters: Except space, comma and @))
- *time-out*—(Optional) Timeout value in seconds
- *retry*—(Optional) Retry value in seconds
- *ifname*—(Optional) Interface name
- *udpPort*—(Optional) UDP port number
- *username*—(Optional) User name (up to 32 characters)

Modes

CONFIGURATION

Usage

Use this command to configure an SNMP agent to send SNMP notifications, traps, and inform SNMP managers configured as host receivers. You can configure multiple host receivers. An SNMP host does not acknowledge the trap messages and notifications received from an SNMP agent. Set the timeout and number of retries for the inform messages sent to an SNMP host. Timeout indicates the number of seconds before the informs time out when sending to a host. Retries indicate the number of times the informs are sent after timing out.

Examples

```
sonic(config)# snmp-server host 1.2.3.4 community comm1 traps v2c  
  
sonic(config)# snmp-server host 1.2.3.5 user user1 informs noauth timeout 200 retries 10  
  
sonic(config)# snmp-server host 2001::1 community comm2 informs timeout 150 retries 5  
  
sonic(config)# snmp-server host 3001::1 user u1 traps priv  
  
sonic(config)# no snmp-server host 3001::1
```

Releases

3.0 or later

snmp-server location

Configures the location of the SNMP server.

Command

```
snmp-server location location_name
```

Options

location_name—Location name in alphanumeric string (up to 255 characters)

Modes

CONFIGURATION

Usage

If the location consists of more than one word, enclose the name in quotes.

Examples

```
sonic(config)# snmp-server location "Lab1, Rack-10"  
  
sonic(config)# no snmp-server location
```

Releases

3.0 or later

snmp-server user

Configures user access to the SNMP agent on the switch using group membership.

Command

```
snmp-server user username {[group] group-name} {[encrypted] {auth {{md5  
{auth-password {authpassword {[priv] {{des {priv-password privpassword}  
| {aes-128 {priv-password privpassword}}}}}}}} | {sha {auth-password  
{authpassword {[priv] {{des {priv-password privpassword} | {aes-128 {priv-  
password privpassword}}}}}}}}}} | {[auth] {noauth | {md5 {auth-password
```

```
{authpassword {[priv] {{des {priv-password privpassword}} | {aes-128  
{priv-password privpassword}}}}} | {sha {auth-password {authpassword  
|[priv] {{des {priv-password privpassword}} | {aes-128 {priv-password  
privpassword}}}}}}}}
```

Options

- *username* — SNMP username (up to 32 characters)
- *group-name* — (Optional) SNMP group-name (up to 32 characters)
- *authpassword* — (Optional) Authentication password
- *privpassword* — (Optional) Privacy password

Modes

CONFIGURATION

Usage

Use this command to assign each user to a group and configure SNMPv3-specific authentication and encryption settings. Authentication passwords can be encrypted. If password encryption is desired, it must be specified prior to setting the authentication type.

Examples

```
sonic(config)# snmp-server user user1  
  
sonic(config)# snmp-server user user1 group group-lab auth md5  
auth-password pwd priv aes-128 priv-password pwd  
  
sonic(config)# snmp-server user snmpuser group snmpgroup  
auth sha auth-password snmpauthpassword priv des priv-password snmpprivpassword  
  
sonic(config)# no snmp-server user user1
```

Releases

3.0 or later

snmp-server view

Configures one or more SNMP views and set the OID tree to include or exclude from the view.

Command

```
snmp-server view view-name {oid-tree {included | excluded}}
```

Options

- *view-name* — View name (up to 32 characters)
- *oid-tree* — OID tree name (up to 255 characters)
- *included* — Included in the SNMP views
- *excluded* — Excluded from the SNMP views

Modes

CONFIGURATION

Usage

Use this command to configure a SNMP view. SNMP views are used by the groups for the GET/SET requests and to send traps.

Examples

```
sonic(config)# snmp-server view view2 1.2.3.4.5.6.7.8.9.2 excluded  
  
sonic(config)# no snmp-server view view2 1.2.3.4.5.6.7.8.9.2
```

Releases

3.0 or later

snmp trap enable

Disables or re-enables sending linkup and linkdown traps that are generated on an interface.

Command

```
snmp trap enable
```

Options

None

Modes

INTERFACE

Usage

By default, linkup and linkdown traps are enabled on all physical port interfaces. To view the SNMP trap status on switch interfaces, use the [show snmp-server interface-traps](#) command.

Examples

```
sonic(config)# interface Eth1/1
sonic(config-if-Eth1/1)# no snmp trap enable

sonic(config)# interface Eth1/1
sonic(config-if-Eth1/1)# snmp trap enable
```

Releases

4.1.0 or later

soft-reconfiguration

Enables soft-reconfiguration for a BGP neighbor.

Command

soft-reconfiguration inbound

Options

None

Modes

- NEIGHBOR-ADDRESS-FAMILY
- PEER-GROUP-ADDRESS-FAMILY

Usage

Use this command to store routes received (RIB-In) from a BGP neighbor. This command is not supported on a peer-group level. To enable soft-reconfiguration for peers in a peer-group, you must enable this command at a per-peer level. With soft-reconfiguration inbound, all updates that are received from this neighbor are stored unmodified, regardless of the inbound policy. When inbound soft-reconfiguration is performed later, the stored information generates a new set of inbound updates. These stored routes could be used to refresh the Loc-RIB in future as needed. If inbound policy changes, these stored routes will be used to generate LocRIB after applying the modified inbound policy.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 20.20.20.2
sonic(config-router-bgp-neighbor)# remote-as 300
sonic(config-router-bgp-neighbor)# address-family ipv4 unicast
sonic(config-router-bgp-neighbor-af)# soft-reconfiguration inbound

sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Int
sonic(config-router-bgp-pg)# address-family ipv4 unicast
sonic(config-router-bgp-pg-af)# soft-reconfiguration inbound

sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 20.20.20.2
sonic(config-router-bgp-neighbor)# remote-as 300
sonic(config-router-bgp-neighbor)# address-family 12vpn evpn
sonic(config-router-bgp-neighbor-af)# soft-reconfiguration inbound

sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Int
sonic(config-router-bgp-pg)# address-family 12vpn evpn
sonic(config-router-bgp-pg-af)# soft-reconfiguration inbound

sonic(config-router-bgp-neighbor-af)# no soft-reconfiguration
sonic(config-router-bgp-pg-af)# no soft-reconfiguration
sonic(config-router-bgp-neighbor-af)# no soft-reconfiguration inbound
```

Releases

3.0 or later

solo

Configures neighbor as solo peer.

Command	<code>solo</code>
Options	None
Modes	<ul style="list-style-type: none">• NEIGHBOR• PEER-GROUP
Usage	Use this command to configure the capability that prevents routes advertised by the specified neighbor from being reflected back to the neighbor. Use this command only if there is a single peer that is defined in the peer group.
Examples	<pre>sonic(config) # router bgp 100 sonic(config-router-bgp) # neighbor 30.30.30.3 sonic(config-router-bgp-neighbor) # solo</pre> <pre>sonic(config) # router bgp 100 sonic(config-router-bgp) # peer-group PG_Ext sonic(config-router-bgp-pg) # solo</pre> <pre>sonic(config-router-bgp-neighbor) # no solo sonic(config-router-bgp-pg) # no solo</pre>
Releases	3.0 or later

source-address

Configures the source address for ICMP or TCP IP SLA.

Command	<code>source-address <i>ip-address</i></code>
Options	<i>ip-address</i> —Source IP address for ICMP and TCP IP SLA.
Modes	<ul style="list-style-type: none">• IP-SLA-ICMP• IP-SLA-TCP
Usage	This command configures a source IP address for ICMP and TCP IP SLA.
Examples	<pre>sonic(config-ipsla-10) # icmp-echo 10.30.1.2 sonic(config-ipsla-10-icmp) # source-address 10.30.1.1</pre> <pre>sonic(config-ip-sla-20) # tcp-connect 10.30.1.2 22 sonic(config-ip-sla-20-tcp) # source-address 10.30.1.1</pre> <pre>sonic(config-ipsla-10-icmp) # no source-address</pre>
Releases	3.1 or later

source-interface

Configures a source interface for ICMP or TCP IP SLA.

Command	<code>source-interface <i>interface</i></code>
Options	<i>interface</i> — A Layer 3 egress interface.
Modes	<ul style="list-style-type: none">• IP-SLA-ICMP

- IP-SLA-TCP

Usage

This command configures a source Layer 3 egress interface for ICMP and TCP IP SLA.

Examples

```
sonic(config)# ip sla 10
sonic(config-ipsla-10)# icmp-echo 30.30.1.2
sonic(config-ipsla-10-icmp)# source-interface Eth 1/3
```

```
sonic(config-ip-sla-20)# tcp-connect 10.30.1.2 22
sonic(config-ip-sla-20-tcp)# source-interface Eth 1/3
```

```
sonic(config-ipsla-10-icmp)# no source-interface
```

Releases

3.1 or later

source-ip

Configures the source IPv4 address on a VXLAN VTEP or an MCLAG peer.

Command

```
source-ip {ipv4-address | Loopback number}
```

Options

- *ipv4-address* — Enter an IPv4 address in A.B.C.D format. An IPv6 address is not supported as a source IP address for VXLAN and MCLAG.
- *Loopback number* — Enter a loopback ID number (0 - 16383). The loopback interface must be configured with an IPv4 address.

Modes

- INTERFACE-VXLAN-VTEP
- MCLAG-DOMAIN

Usage

A source IP address is required when you configure a VXLAN VTEP, a border leaf VTEP in multisite DCI, or an MCLAG peer. In VXLAN, a source IP is required before you create VLAN-VNI mappings. In a multisite DCI installation, configure a separate source and external IP address on each border leaf VTEP to distinguish between internal and external VXLAN tunnels. In MCLAG, configure the same source and external IP address for remote site connections on each MCLAG peer.

(i) NOTE: If you specify a loopback number, the loopback interface must be configured with an IPv4 address. You cannot reconfigure or delete a loopback IP address if it is being used as the source IP address on a VXLAN VTEP. In asymmetric and symmetric IRB, you can reconfigure a VTEP source IP address "on the fly" after you map L2 host VLANs to VNIs and L3 VNIs to VRFs. However, you cannot delete a VTEP source IP address if VLAN- or VRF-to-VNI mapping is configured.

Examples

On a VXLAN VTEP:

```
sonic(config)# interface Loopback 2
sonic(config-if-lo2)# ip address 10.10.10.25/32
sonic(config-if-lo2)# exit
sonic(config)# interface vxlan vtep1
sonic(config-if-vxlan-vtep1)# source-ip Loopback 2

sonic(config-if-vxlan-vtep1)# no source-ip
```

On an MCLAG peer :

```
sonic(config)# mclag domain 1
sonic(config-mclag-domain-1)# source-ip 192.168.100.2
```

Releases

3.0 or later

source-port

Configures a source port for an IP SLA TCP instance.

Command `source-port port-number`

Options `port` — Port number

Modes TCP-CONNECT

Usage Use this command to specify a source port for an TCP SLA instance.

Examples

```
sonic(config-ipsla-20) # tcp-connect 40.40.1.2  
sonic(config-ipsla-20-tcp) # source-port 200
```

```
sonic(config) # no source-port
```

Releases 3.1 or later

source-vrf

Configures the ICMP or TCP source VRF for IP SLA.

Command `source-vrf vrf-name`

Options `vrf-name`—VRF name prefixed by Vrf (up to 15 characters)

Modes

- ICMP-ECHO
- TCP-CONNECT

Usage Use this command to specify a source VRF for an SLA instance.

Examples

```
sonic(config-ipsla-10) # icmp-echo 30.30.1.2  
sonic(config-ipsla-10-icmp) # source-vrf VrfRed
```

```
sonic(config-ipsla-10-icmp) # no source-vrf
```

Releases 3.1 or later

spanning-tree bpdufilter

Enables or disables BPDU filtering on an interface.

Command `spanning-tree bpdufilter {enable | disable}`

Options

- `enable` — Enables the BPDU filter on an interface
- `disable` — Disables the BPDU filter on an interface

Modes INTERFACE

Usage Use this command to enable or disable bridge protocol data unit (BPDU) filtering.

Examples

```
sonic(config-if-Ethernet28)# spanning-tree bpdufilter enable  
  
sonic(config-if-Ethernet28)# spanning-tree bpdufilter disable  
  
sonic(config-if-Ethernet28)# no spanning-tree bpdufilter  
  
sonic(config-if-pol1)# spanning-tree bpdufilter enable  
  
sonic(config-if-pol1)# spanning-tree bpdufilter disable  
  
sonic(config-if-pol1)# no spanning-tree bpdufilter
```

Releases

3.0 or later

spanning-tree bpduguard

Enables or disables the BPDU guard on an interface.

Command

```
spanning-tree bpduguard [port-shutdown]
```

Options

- port-shutdown — (Optional) Shuts down the port when a BPDU is received

Modes

INTERFACE

Usage

Use this command to shut down an interface when it receives a bridge protocol data unit (BPDU). If the port receives a BPDU, it is placed in the error-disabled state. BPDU guard can be enabled when the spanning-tree is enabled which is useful when the port is in portfast mode (see [spanning-tree portfast](#)) or disabled.

Examples

```
sonic(config)# interface PortChannel 1  
sonic(config-if-pol1)# spanning-tree bpduguard port-shutdown  
  
sonic(config-if-pol1)# no spanning-tree bpduguard
```

Releases

3.0 or later

spanning-tree cost

Configures the spanning-tree cost on an interface.

Command

```
spanning-tree [mst inst-id/range] cost value
```

Options

- mst *inst-id/range* — (Optional) MST instance ID or range
- value* — Specify the port path cost (1 to 200000000)

Modes

INTERFACE

Usage

The default path cost is determined by the port speed. When this command is configured without the MST instance, cost value is applied to all the MST instances on the port. When configured with MST instance, the cost value is applied only to the instance specified in the configuration.

Examples

```
sonic(config) # interface PortChannel 1  
sonic(config-if-pol) # spanning-tree cost 100000
```

```
sonic(config) # interface PortChannel 1  
sonic(config-if-pol) # spanning-tree mst 2 cost 100000
```

```
sonic(config-if-pol) # no spanning-tree cost
```

Releases

3.0 or later

spanning-tree edge-port

Configures a spanning-tree BPDU filter on all edge ports.

Command

```
spanning-tree edge-port bpdufilter default
```

Options

None

Modes

CONFIGURATION

Usage

Use this command to enable the configuration of the BPDU filter at a global level. However, it can only be applied if the port is operating in edge port mode. When the global BPDU filter is activated, approximately 10 BPDUs are transmitted when the link is up, after which the port ceases BPDU transmissions. If BPDUs are received, the port transitions from an edge port to a normal STP port, and the filtering is disabled, allowing the port to function as a standard STP port.

Examples

```
sonic(config) # spanning-tree edge-port bpdufilter default
```

```
sonic(config) # no spanning-tree edge-port bpdufilter default
```

Releases

3.0 or later

spanning-tree enable

Enables spanning-tree on an interface.

Command

```
spanning-tree enable
```

Options

None

Modes

INTERFACE

Usage

Spanning-tree is enabled by default on Layer 2 interfaces if global STP mode is configured.

Example

```
sonic(config) # interface PortChannel 1  
sonic(config-if-pol) # spanning-tree enable
```

```
sonic(config-if-pol) # no spanning-tree enable
```

Releases

3.0 or later

spanning-tree forward-time

Configures the spanning-tree forward delay time in seconds.

Command

```
spanning-tree forward-time seconds
```

Options	forward time <i>seconds</i> — Specifies the spanning-tree forward delay time in seconds (4 to 30; default 15)
Modes	CONFIGURATION
Usage	Spanning-tree forward-time is the amount of time a port remains in listening and learning states before entering the forwarding state. When configuring the forwarding time, this relationship should be maintained: $2 * (\text{forward-time} - 1) \geq \text{max-age} \geq 2 * (\text{hello-time} + 1)$.
	(i) NOTE: This command is not supported in MST mode.
Examples	<pre>sonic(config) # spanning-tree forward-time 25</pre> <pre>sonic(config) # no spanning-tree forward-time</pre>
Releases	3.0 or later

spanning-tree guard

Enables root guard on all spanning-tree instances on an interface.

Command	spanning-tree guard root {timeout <i>seconds</i> }
Options	<i>seconds</i> — Timeout value (5 to 600; default 30)
Modes	CONFIGURATION
Usage	Root guard prevents the interface from becoming the root port of the device. Root guard can be enabled when the device operates in any mode. When root guard is enabled, the port changes to blocking or discarding state if the spanning-tree calculations select the port as the root port.
Examples	<pre>sonic(config) # spanning-tree guard root timeout 10</pre> <pre>sonic(config-if-Ethernet28) # spanning-tree guard root timeout 10</pre> <pre>sonic(config) # no spanning-tree guard root timeout</pre> <pre>sonic(config-if-Ethernet28) # no spanning-tree guard root timeout</pre>
Releases	3.0 or later

spanning-tree guard

Configures loop guard or root guard on an interface.

Command	spanning-tree guard {loop root none}
Options	<ul style="list-style-type: none"> • loop — Configures loop guard on the interface • root — Configures root guard on the interface • none — Disable both loop guard and root guard on the interface
Modes	INTERFACE
Usage	By default, both loop guard and root guard are disabled on an interface. Root guard enforces the root bridge placement in the network and allows STP to interoperate with network bridges while maintaining the bridged network topology. When BPDUs are received on a root guard-enabled port, the STP state is moved to root inconsistent state. Once the port stops receiving superior BPDUs, root guard automatically sets the port back to a forwarding state after the timer is expired.
	(i) NOTE: By default, when spanning-tree stops receiving the BPDUs on a blocking port, it transitions to forwarding state which can result in a loop. The Loop guard feature when enabled, avoids

this transition of non-designated ports to forwarding state and instead moves the port to a loop inconsistent state where the port continues to block the traffic to avoid the loop.

Examples

```
sonic(config-if-Ethernet28) # spanning-tree guard root
```

```
sonic(config-if-Ethernet28) # spanning-tree guard loop
```

```
sonic(config-if-Ethernet28) # no spanning-tree guard
```

Releases

3.0 or later

spanning-tree hello-time

Configures the spanning-tree hello time value for transmission of BPDUs.

Command `spanning-tree hello-time seconds`

Options `seconds` — Specifies the spanning-tree hello time in seconds (1 to 10; default 2)

Modes CONFIGURATION

Usage This command configures how often the switch broadcasts hello messages to other devices. When configuring the hello time, this relationship should be maintained: `max-age >= 2 * (hello-time + 1)`.

 **NOTE:** This command is not supported in MST mode.

Examples

```
sonic(config) # spanning-tree hello-time 3
```

```
sonic(config) # no spanning-tree hello-time
```

Releases

3.0 or later

spanning-tree link-type

Sets spanning-tree link-type as point-to-point or shared.

Command `spanning-tree link-type {point-to-point | shared}`

- `point-to-point` — Specifies that the interface is a point-to-point or full-duplex link (default)
- `shared` — Specifies that the interface is a half-duplex link

Modes INTERFACE

 **NOTE:** Do not configure shared media such as hubs as point-to-point links.

Examples

```
sonic(config) # interface PortChannel 1  
sonic(config-if-pol) # spanning-tree link-type point-to-point
```

```
sonic(config-if-pol) # no spanning-tree link-type
```

Releases

3.0 or later

spanning-tree loopguard

Configures spanning-tree loop guard.

Command	<code>spanning-tree loopguard default</code>
Options	None
Modes	CONFIGURATION
Usage	This command enables loop guard globally on all ports. When loop guard is enabled and if BPDU are not received on a nondesignated port, that port is moved into the STP loop-inconsistent blocking state, instead of the listening/learning/forwarding state.
Examples	<pre>sonic(config) # spanning-tree loopguard default</pre> <pre>sonic(config) # no spanning-tree loopguard default</pre>
Releases	3.1 or later

spanning-tree max-age

Configures the spanning-tree max-age timeout value.

Command	<code>spanning-tree max-age <i>seconds</i></code>
Options	<i>seconds</i> — Specifies the spanning-tree maximum time to listen for the root bridge in seconds (6 to 40; default 20)
Modes	CONFIGURATION
Usage	Use this command to configure the spanning-tree maximum age. When configuring the maximum age, this relationship should be maintained: $2 * (\text{forward-time} - 1) \geq \text{max-age}$.
	(i) NOTE: This command is not supported in MST mode.
Examples	<pre>sonic(config) # spanning-tree max-age 10</pre> <pre>sonic(config) # no spanning-tree max-age</pre>
Releases	3.0 or later

spanning-tree mode

Configures global spanning-tree mode for the device.

Command	<code>spanning-tree mode {pvst rapid-pvst mst}</code>
Options	<ul style="list-style-type: none"><code>pvst</code> — Enable PVST+ (based on IEEE 802.1W)<code>rapid-pvst</code> — Enable rapid PVST+ (based on IEEE 802.1D)<code>mst</code> — Enables MST (based on IEEE 802.1Q)
Modes	CONFIGURATION
Usage	Use the <code>spanning-tree mode</code> command to select which spanning-tree protocol to run. When global PVST or RPVST mode is enabled, by default spanning-tree is enabled on the first 255 VLANs. If spanning-tree instances are configured first followed by VLANs, configuration order is used to count the first 255 spanning-tree instances. If VLANs are configured first followed by spanning-tree instances, VLANs are sorted by VLAN ID, and first 255 VLAN IDs are used. Only one mode can be enabled at a time. Use the <code>no</code> form of the command to disable the spanning-tree protocol.

Examples

```
sonic(config) # spanning-tree mode pvst
```

```
sonic(config) # no spanning-tree mode
```

Releases

3.0 or later

spanning-tree mst configuration

Enter MST Configuration mode.

Command spanning-tree mst configuration

Options None

Modes CONFIGURATION

Usage This mode allows configuring the MST name, revision number, and VLAN to instance mapping. The no form of this command removes the configuration and sets to the default values.

(i) NOTE: This command is supported only in MST mode.

Examples

```
sonic(config) # spanning-tree mst configuration  
sonic(config-mst) #
```

```
sonic(config) # no spanning-tree mst configuration
```

Releases

4.0 or later

spanning-tree mst forward-time

Configures the forward delay time for MSTP.

Command spanning-tree mst forward-time *seconds*

Options *seconds* — MST forward-time in seconds (4 to 30; default is 15)

Modes CONFIGURATION

(i) NOTE: This command is supported only in MST mode.

Examples

```
sonic(config) # spanning-tree mst forward-time 20
```

```
sonic(config) # no spanning-tree mst forward-time 20
```

Releases

4.0 or later

spanning-tree mst hello-time

Configures the hello time value for MSTP.

Command spanning-tree mst hello-time *seconds*

Options *seconds* — Hello time interval (in seconds) for transmitting BPDUs (1 to 10; default is 2)

Modes CONFIGURATION

(i) NOTE: This command is supported only in MST mode.

Examples

```
sonic(config) # spanning-tree mst hello-time 3
```

```
sonic(config) # no spanning-tree mst hello-time 3
```

Releases

4.0 or later

spanning-tree mst max-age

Configures the max-age time value for MSTP.

Command

```
spanning-tree mst max-age seconds
```

Options

seconds — Maximum time in seconds (6 to 40; default is 20)

Modes

CONFIGURATION

Usage

Use this command to configure the maximum time to listen for root bridge.

 **NOTE:** This command is supported only in MST mode.

Examples

```
sonic(config) # spanning-tree mst max-age 22
```

```
sonic(config) # no spanning-tree mst max-age 22
```

Releases

4.0 or later

spanning-tree mst max-hops

Configures the max-hop value for MSTP.

Command

```
spanning-tree mst max-hops hop-count
```

Options

hop-count — Maximum hop-count number for the MST (1 to 40; default is 20)

Modes

CONFIGURATION

Usage

In MSTP, max-hops value specifies the number of hops in a region before the BPDU is discarded and the information is aged out.

 **NOTE:** This command is supported only in MST mode.

Examples

```
sonic(config) # spanning-tree mst max-hops 10
```

```
sonic(config) # no spanning-tree mst max-hops 10
```

Releases

4.0 or later

spanning-tree mst priority

Configures the bridge priority for the MST instance.

Command

```
spanning-tree [mst inst-id/range] priority value
```

Options

- *mst inst-id/range*—(Optional) MST instance ID or instance range (0 to 4094)
- *value*—Priority value in multiples of 4096 (0 to 61440; default is 32768)

Modes

CONFIGURATION

Usage	When MST instance ID or range is specified, the priority value is applied only to those specific MST instances. i NOTE: This command is supported only in MST mode.
--------------	---

Examples	<pre>sonic(config)# spanning-tree mst 1 priority 4096</pre> <pre>sonic(config)# spanning-tree priority 4096</pre> <pre>sonic(config)# no spanning-tree mst 1 priority 4096</pre>
-----------------	--

Releases	4.0 or later
-----------------	--------------

spanning-tree port

Sets the edge-port type to an interface.

Command	<code>spanning-tree port type edge</code>
Options	None
Modes	INTERFACE
Usage	When you configure an EdgePort on a device running STP, the port immediately transitions to the forwarding state. Only configured ports connected to end hosts act as EdgePorts. i NOTE: This command is not supported in PVST mode.

Examples	<pre>sonic(config-if-pol1)# spanning-tree port type edge</pre> <pre>sonic(config-if-pol1)# no spanning-tree port</pre>
-----------------	---

Releases	3.1 or later
-----------------	--------------

spanning-tree portfast

Enables spanning-tree portfast mode on an interface.

Command	<code>spanning-tree portfast default</code>
Options	None
Modes	<ul style="list-style-type: none"> • CONFIGURATION • INTERFACE
Usage	Use this command to enable portfast mode on an interface. Portfast allows edge ports to move to a forwarding state quickly when the connected device is not participating in spanning-tree. The default option is only used in CONFIGURATION mode. i NOTE: This command is only supported in PVST mode.

Examples	<pre>sonic(config)# interface PortChannel 1</pre> <pre>sonic(config-if-pol1)# spanning-tree portfast default</pre> <pre>sonic(config)# spanning-tree portfast default</pre> <pre>sonic(config-if-pol1)# no spanning-tree portfast</pre>
-----------------	---

Releases	3.2 or later
-----------------	--------------

spanning-tree port-priority

Configures the port-level priority value for a port.

Command	<code>spanning-tree [mst <i>inst-id/range</i>] port-priority <i>value</i></code>
Options	<ul style="list-style-type: none">• <i>mst inst-id/range</i> — (Optional) MST instance ID or range (1 to 4094)• <i>value</i> — Priority value (0 to 240 in multiples of 16; default 128)
Modes	INTERFACE
Usage	When this command is configured without the MST instance, port priority value is applied to all the MST instances on the port. If the MST instance is specified when configuring this command, the port priority value is applied only to the instance specified in the configuration.
Examples	<pre>sonic(config)# interface PortChannel 1 sonic(config-if-pol)# spanning-tree port-priority 96 sonic(config-if-pol)#spanning-tree mst 1 priority 4096 sonic(config-if-pol)# no spanning-tree port-priority</pre>
Releases	3.0 or later

spanning-tree priority

Configures the global-level spanning-tree bridge priority value.

Command	<code>spanning-tree priority <i>priority</i></code>
Options	<i>priority</i> — Bridge priority value in increments of 4096 (0 to 61440; default 32768)
Modes	CONFIGURATION
Usage	Use this command to configure the device spanning-tree priority which is used to determine which bridge is selected as the root bridge. The switch with the lowest priority is the root of the spanning-tree. When more than one switch has the lowest priority, the switch with the lowest MAC address is selected as the root.  NOTE: This command is not supported in MST mode.
Examples	<pre>sonic(config)# spanning-tree priority 12288 sonic(config)# no spanning-tree priority</pre>
Releases	3.0 or later

spanning-tree uplinkfast

Configures spanning-tree uplink fast on an interface.

Command	<code>spanning-tree uplinkfast</code>
Options	None
Modes	INTERFACE
Usage	Uplink fast enhances STP performance for switches with redundant uplinks. Using the default value for the standard STP forward delay, convergence following a transition from an active link to a redundant link can take 30 seconds (15 seconds for listening and an additional 15 seconds for learning). When uplink fast is configured on the redundant uplinks, it reduces the convergence time to just one second by moving to

forwarding state (bypassing listening and learning modes) in just once second when the active link goes down.

i|NOTE: This command is only supported in PVST mode.

Examples

```
sonic(config)# interface PortChannel 1  
sonic(config-if-pol1)# spanning-tree uplinkfast
```

```
sonic(config-if-pol1)# no spanning-tree uplinkfast
```

Releases

3.0 or later

spanning-tree vlan

Configures interface and spanning-tree parameters on a per VLAN-basis.

Command `spanning-tree vlan vlan-range {{[forward-time seconds]}} | {[hello-time seconds]}} | {[max-age seconds]}} | {[priority value]}}`

Options

- *vlan-range* — VLAN ID (1 to 4094)
- *forward-time seconds* — Forward-time interval in seconds (4 to 30; default 15)
- *hello-time seconds* — Hello-time interval in seconds (1 to 10; default 2)
- *max-age seconds* — Max-age time interval in seconds (6 to 40; default 20)
- *priority value* — Priority value (0 to 61440; default 32768)

Modes

CONFIGURATION

Usage

This command is similar to the global-level commands but allows configuring spanning-tree parameters on per VLAN basis. You can specify a single VLAN ID, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

i|NOTE: This command is not supported in MST mode.

Examples

```
sonic(config)# spanning-tree vlan 100  
sonic(config)# spanning-tree vlan 100 forward-time 11  
sonic(config)# spanning-tree vlan 100 hello-time 3  
sonic(config)# spanning-tree vlan 100 max-age 22  
sonic(config)# spanning-tree vlan 100 priority 4096
```

```
sonic(config)# no spanning-tree vlan 100  
sonic(config)# no spanning-tree vlan 100 forward-time  
sonic(config)# no spanning-tree vlan 100 hello-time  
sonic(config)# no spanning-tree vlan 100 max-age  
sonic(config)# no spanning-tree vlan 100 priority
```

Releases

3.2 or later

spanning-tree vlan

Configures interface and spanning-tree parameters on a per VLAN-basis.

Command `spanning-tree vlan vlan-range {{cost value} | {port-priority value}}`

Options

- *vlan-range* — VLAN ID (1 to 4094)
- *cost value* — Cost value (1 to 200000000; higher values mean higher costs)

Table 15. Cost values

Link speed	Default path cost values	Path cost range
< 100 kilo bits per second	200,000,000	20,000,000 to 200,000,000
1 Megabit per second	20,000,000	2,000,000 to 200,000,000
10 Megabits per second	2,000,000	200,000 to 200,000,000
100 Megabits per second	200,000	20,000 to 200,000,000
1 Gigabit per second	20,000	2,000 to 200,000,000
10 Gigabits per second	2,000	200 to 20,000
100 Gigabits per second	200	20 to 2,000
1 Terabits per second	20	2 to 200
10 Terabits per second	2	1 to 20

- `port-priority value` — Priority value (0 to 61440; default 32768)

Modes

INTERFACE

Usage

This command is similar to the global-level commands but allows configuring spanning-tree parameters on per VLAN basis. You can specify a single VLAN ID, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

 **NOTE:** This command is not supported in MST mode.

Examples

```
sonic(config)# interface Ethernet 28
sonic(config-if-Ethernet28)# spanning-tree vlan 100 cost 1000
sonic(config-if-Ethernet28)# spanning-tree vlan 100 port-priority 16

sonic(config)# interface PortChannel 1
sonic(config-if-pol1)# spanning-tree vlan 100 cost 1000
sonic(config-if-pol1)# spanning-tree vlan 100 port-priority 16

sonic(config-if-pol1)# no spanning-tree vlan 100 cost 1000
sonic(config-if-pol1)# no spanning-tree vlan 100 port-priority 16
```

Releases

3.2 or later

speed

Configures the transmission speed of the Management and other Ethernet interfaces.

Command `speed {10 | 100 | 1000 | 2500 | 5000 | 10000 | 20000 | 25000 | 40000 | 50000 | 100000 | 200000 | 400000 | 800000 | auto}`

Options

- 10—10M
- 100—100M
- 1000—1G (default)
- 2500—2.5G
- 5000—5G
- 10000—10G
- 25000—25G
- 40000—40G
- 50000—50G
- 100000—100G
- 200000—200G
- 400000—400G

- 800000—800G
- auto—Enable autonegotiation

Modes

INTERFACE

Usage

- On a Management interface, the supported transmission speeds are {10 | 100 | 1000 | auto}. On other Ethernet interfaces, the supported transmission speeds {10 | 100 | 1000 | 2500 | 5000 | 10000 | 20000 | 25000 | 40000 | 50000 | 100000 | 200000 | 400000 | 800000 | auto}.
- Separate advertised speeds with a comma; for example, speed 25000,10000,1000.
- Enter speed auto to enable autonegotiation and advertise all supported speeds. When you enable autonegotiation, you can specify the speeds to advertise to connecting devices; for example, speed auto 25000. Dell Technologies recommends that you advertise the native speed of the cable that is used in the port.

i **NOTE:** If autonegotiation is off, you must set the interface speed.

i **NOTE:** On platforms with 1G Base-T and 10G Base-T RJ45 interfaces, ensure that the auto option is enabled.

Examples

```
sonic(config)# interface Management 0
sonic(config-if-Management0)# speed ?
<10/100/1000/auto> Speed config of the interface
```

```
sonic(config)# interface Eth 1/1
sonic(config-if-Eth1/1)# speed ?
<10/100/1000/2500/5000/10000/20000/25000
/40000/50000/100000/200000/400000/800000> Speed config of the interface
auto
```

Enable auto-negotiation

Releases

3.0 or later

speed auto

Enables autonegotiation and advertises all the speeds supported in the hardware.

Command `speed auto [admin_advertise]`

Options `admin_advertise` — (Optional) Administration advertise

Modes

- INTERFACE
- INTERFACE RANGE

Usage

Autonegotiation and link training are not supported on the 10G SFP+ ports of Z9664F-ON, Z9432F-ON, Z9332F-ON, Z9264F-ON, S5448F-ON, and S5232F-ON switches. For all other types of ports that support 10G SFP+ connections (for example, SFP28), do not enable autonegotiation for 10G SFP+ links.

Examples

```
sonic(config)# interface Ethernet 0
sonic(config-if-Ethernet0)# speed auto 400000
```

```
sonic(config)# interface Ethernet 0
sonic(config-if-Ethernet0)# speed auto
```

```
sonic(config-if-Ethernet0)# no speed auto
```

Releases

4.0 or later

ssh-server vrf

Enables the SSH server on a specific VRF.

Command	<code>ssh-server vrf <i>vrf-name</i></code>
Options	<i>vrf-name</i> —VRF name prefixed by Vrf (up to 15 characters)
Modes	CONFIGURATION
Usage	Use this command to enable the SSH server on a specific VRF.
Examples	<pre>sonic(config) # ssh-server vrf Vrf2</pre> <pre>sonic(config) # no ssh-server vrf Vrf2</pre>

Releases	3.1 or later
-----------------	--------------

standalone-link-training

Enables stand-alone link-training regardless of the auto negotiation state.

Command	<code>standalone-link-training</code>
Options	None
Modes	<ul style="list-style-type: none">• INTERFACE• INTERFACE RANGE
Usage	Use this command to enable or disable stand-alone link-training for the port. Stand-alone link-training is used when full auto negotiation is not required on an Ethernet link but link training is needed. Stand-alone link-training is ignored when auto negotiation is enabled. i NOTE: Autonegotiation and link training are not supported on the 10G SFP+ ports of Z9664F-ON, Z9432F-ON, Z9332F-ON, Z9264F-ON, S5448F-ON, and S5232F-ON switches. For all other types of ports that support 10G SFP+ connections (for example, SFP28), do not enable autonegotiation for 10G SFP+ links.
Examples	<pre>sonic# configure terminal</pre> <pre>sonic(config) # interface Ethernet 1</pre> <pre>sonic(config-if-Ethernet1) # standalone-link-training</pre> <pre>sonic(config-if-Ethernet1) # no standalone-link-training</pre> <pre>sonic# configure terminal</pre> <pre>sonic(config) # interface range Ethernet 0-16</pre> <pre>%Info: Configuring only existing interfaces in range</pre> <pre>sonic(config-if-range-eth**) # standalone-link-training</pre>

Releases	4.0 or later
-----------------	--------------

startup-delay

Configures a startup delay to avoid traffic loss during the bootup of a multihomed VTEP.

Command	<code>startup-delay <i>seconds</i></code>
Options	<i>seconds</i> — Startup-delay timer in seconds (0-3600; default 300).
Modes	EVPN-ESI-MULTIHOMING

Usage

During VTEP bootup, the EVPN multihoming interfaces are kept in an administrative-down state until the startup-delay timer expires. As a result, traffic from a multihomed tenant device is not load-balanced to the VTEP until the VTEP starts up and is ready. To view the configured startup-delay value, use the [show evpn es startup-delay](#) command.

i | NOTE: In order for the startup delay timer to take effect, interface tracking on uplinks must be configured (see [link state track](#)).

Examples

```
sonic(config) # evpn esi-meshing  
sonic(config-evpn-esi-mh) # startup-delay 300
```

Releases

4.2.0 or later

static

Adds a static NAT entry based on all ports, or global or local IP addresses.

Command

```
static {all | {basic global-ip local-ip [natType] {[twice-nat-id] twice-nat-id-value}} | {natPortType global-ip global-port local-ip local-port [natType] {[twice-nat-id] twice-nat-id-value}}}}
```

Options

- *global-ip*—Global IP in A.B.C.D format
- *local-ip*—Local IP in A.B.C.D format
- *natType*—NAT authentication type; snat or dnat
- *twice-nat-id-value*—NAT ID
- *natPortType*—Port type; tcp or udp
- *global-port*—Global port ID
- *local-port*—Local port ID

Modes

NAT

Usage

Use this command to add a static NAT entry based on all ports, or global or local IP addresses.

Examples

```
sonic(config-nat) # static all  
  
sonic(config-nat) # static basic 1.1.1.1 2.2.2.2  
  
sonic(config-nat) # static tcp 2.2.2.2 3000 3.3.3.3 4000  
  
sonic(config-nat) # no static all
```

Releases

3.0 or later

storm-control broadcast

Configures storm-control broadcast in kbps.

Command

```
storm-control broadcast kpbs
```

Options

kpbs — Storm-control broadcast value

Modes

INTERFACE

Usage

This command allows the broadcast traffic with the configured rate, excess traffic is dropped.

Examples

```
sonic(config) # interface Ethernet 0
sonic(config-if-Ethernet0) # storm-control broadcast 10000

sonic(config-if-Ethernet0) # no storm-control broadcast
```

Releases

3.1 or later

storm-control unknown-multicast

Configures storm-control unknown multicast in kbps.

Command `storm-control unknown-multicast kbps`

Options *kbps*—Storm-control unknown-multicast value

Modes INTERFACE

Usage Use this command to configure storm-control unknown multicast in kbps. Unknown-multicast traffic consists of all multicast traffic that does not match any of the statically configured or dynamically learned multicast groups.

Examples

```
sonic(config) # interface Ethernet 0
sonic(config-if-Ethernet0) # storm-control unknown-multicast 30000

sonic(config-if-Ethernet0) # no storm-control unknown-multicast
```

Releases

3.1 or later

storm-control unknown-unicast

Configures storm-control unknown unicast in kbps.

Command `storm-control unknown-unicast kbps`

Options *kbps*—Storm-control unknown unicast value

Modes INTERFACE

Usage Use this command to configure the storm-control unknown unicast on a port interface. Traffic that exceeds the configured rate is dropped.

Examples

```
sonic(config) # interface Ethernet 0
sonic(config-if-Ethernet0) # storm-control unknown-unicast 20000

sonic(config-if-Ethernet0) # no storm-control unknown-unicast
```

Releases

3.1 or later

strict-capability-match

Configures a BGP neighbor or peer-group to strictly compare remote capabilities and local capabilities.

Command `strict-capability-match`

Options None

Modes • BGP-NEIGHBOR
 • PEER-GROUP

Usage If remote and local capabilities are different, this command sends an unsupported capability error then resets the connection.

Examples

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # neighbor 30.30.30.3
sonic(config-router-bgp-neighbor) # strict-capability-match
```

```
sonic(config) # router bgp 100
sonic(config-router-bgp) # peer-group PG_Ext
sonic(config-router-bgp-pg) # strict-capability-match
```

```
sonic(config-router-bgp-neighbor) # no strict-capability-match
sonic(config-router-bgp-pg) # no strict-capability-match
```

Releases 3.0 or later

switch-id

Configures a 32-bit identifier that uniquely identifies the switch, and is used in telemetry reports.

Command `switch-id id`

Options *id* — Switch ID (1 to 4294967295)

Modes TAM

Usage Use [show tam switch](#) to view the configured switch ID.

Examples

```
sonic(config-tam) # switch-id 1234
```

```
sonic(config-tam) # no switch-id
```

Releases 3.1 or later

switch-resource

Configures switch resources.

Command `switch-resource`

Options None

Modes CONFIGURATION

Usage Use this command to enter switch resource mode to enable different route-scale profiles and enable switch resources for multihoming, VLAN stacking, and drop monitor.

Example

```
sonic(config) # switch-resource
sonic(config-switch-resource) #
```

Releases 3.1 or later

switching-mode cut-through

Enables cut-through switching mode on a switch.

Command `switching-mode cut-through`

Options None

Modes	CONFIGURATION
Usage	The default switching mode is store-and-forward. To enable cut-through switching mode, use the <code>switching-mode cut-through</code> command. To disable cut-through switching and return the switch to the default store-and-forward mode, enter the <code>no switching-mode cut-through</code> command.
Examples	<pre>sonic(config) # switching-mode cut-through</pre>
Releases	4.2.0 or later

switchport access

Assigns access VLAN membership to a port in L2 Access or Trunk mode.

Command	<code>switchport access Vlan <i>vlan-id</i></code>
Options	<i>vlan-id</i> —VLAN ID (1 to 4094)
Modes	INTERFACE
Usage	By default, an Ethernet or port-channel interface is not in L2 mode. You must configure the interface to operate either as an access (untagged traffic) or trunk (tagged traffic) port (see switchport trunk). An access port sends and receives untagged frames from connected L2 devices.
Examples	<pre>sonic(config) # interface Ethernet 28 sonic(config-if-Ethernet28) # switchport access Vlan 5</pre> <pre>sonic(config) # interface PortChannel 4 sonic(config-if-po4) # switchport access Vlan 5</pre> <pre>sonic(config-if-Ethernet28) # no switchport access Vlan sonic(config-if-po4) # no switchport access Vlan</pre>
Releases	3.0 or later

switchport trunk

Configures the tagged VLAN traffic that an L2 trunk interface can carry.

Command	<code>switchport trunk allowed Vlan {<i>vlanid_list</i> add <i>vlanid_list</i> all except <i>vlanid_list</i> none remove <i>vlanid_list</i>}</code>
Options	<ul style="list-style-type: none"> • <i>vlan-id_list</i>—VLAN numbers of the tagged traffic that the L2 trunk port can carry; comma-separated and hyphenated VLAN number ranges are supported. • <code>add <i>vlan-id_list</i></code>—Append the list of VLANs to the existing configuration. • <code>all</code>—Add all VLANs. • <code>except <i>vlan-id_list</i></code>—Add all VLANs except the list of VLANs specified. • <code>none</code>—Remove all VLANs (remove the trunk configuration). • <code>remove <i>vlan-id_list</i></code>—Removes the list of VLANs from the existing configuration.
Mode	INTERFACE
Usage	By default, an Ethernet or PortChannel interface is not in L2 mode. You must configure the interface to operate either as a trunk (tagged traffic) or access (untagged traffic) port (see switchport access). A trunk port sends and receives tagged frames from multiple VLANs and untagged frames from the access VLAN.
Examples	<pre>sonic(config) # interface Ethernet 4 sonic(config-if-Ethernet4) # switchport trunk allowed Vlan add 100-103,110</pre>

```

sonic(config-if-Ethernet4)# switchport access Vlan 105
sonic(config-if-Ethernet4)# switchport trunk allowed Vlan remove 101

sonic(config)# interface PortChannel 1
sonic(config-if-pol1)# switchport trunk allowed Vlan add 100-103
sonic(config-if-pol1)# switchport access Vlan 105

sonic(config-if-Ethernet28)# no switchport trunk allowed Vlan 100-103,110
sonic(config-if-po4)# no switchport trunk allowed Vlan 105

```

Releases	3.0 or later
-----------------	--------------

switchport vlan-mapping

Configures Q-in-Q VLAN tunneling or VLAN translation for transmitting customer VLAN traffic over a service provider network.

Command	<ul style="list-style-type: none"> Q-in-Q VLAN tunneling: <code>switchport vlan-mapping {cvlan-list {add remove} cvlan-list} dot1q-tunnel svlan-id [priority priority-bits] [multi-tag]</code> VLAN translation: <code>switchport vlan-mapping cvlan-id [inner inner-cvlan-id] svlan-id [priority priority-bits] [multi-tag]</code>
Q-in-Q options	<ul style="list-style-type: none"> <code>cvlan-list</code> — Enter the customer VLAN IDs to be mapped to an SVLAN, or to be added or removed from the list of CVLANs already mapped to the SVLAN. Enter a single CVLAN ID or a range with a hyphen (-); for example, 10-21. Separate CVLAN IDs and ranges using a comma (,); for example, 10,15-18,21. <code>{add remove} cvlan-list</code> — Specify the customer VLAN IDs to be added or removed from the list of CVLAN traffic that is mapped to the specified SVLAN. <code>svlan-id</code> — Specifies the service-provider VLAN ID used to transmit CVLAN traffic (1-4094). <code>priority priority-bits</code> — (Optional) Sets the priority bits in the SVLAN tag (0-7). <code>multi-tag</code> — (Optional) Allows unknown customer VLAN tags to be sent as a payload across a VxLAN network. An unknown customer VLAN tag can be part of a traffic flow for single- or double-tagged CVLAN-to-SVLAN translation. The <code>multi-tag</code> option is only supported on flows that are configured for VXLAN.
VLAN translation options	<ul style="list-style-type: none"> <code>cvlan-id</code> — Matches a customer VLAN ID (1-4094). <code>cvlan-id</code> is a mandatory parameter for both single- and double-tagged VLAN packets. <code>inner cvlan-id</code> — Matches a customer VLAN ID (1-4094) in double-tagged packets. The outer VLAN tag is identified by the preceding <code>cvlan-id</code> parameter. <code>svlan-id</code> — Specifies the service-provider VLAN ID used to transmit CVLAN traffic (1-4094). <code>priority priority-bits</code> — (Optional) Sets the priority bits in the SVLAN tag (0-7). <code>multi-tag</code> — (Optional) Allows unknown customer VLAN tags to be sent as a payload across a VxLAN network. An unknown customer VLAN tag can be part of a traffic flow for single- or double-tagged CVLAN-to-SVLAN translation. The <code>multi-tag</code> option is only supported on flows configured for VXLAN.
Mode	INTERFACE
Usage	<p>Q-in-Q VLAN tunneling and VLAN translation for provider networks are supported on Ethernet and port-channel interfaces. Use Q-in-Q VLAN tunneling to separate VLAN traffic from different customers in a service provider network by tunneling multiple VLANs from one customer (CVLANs) in a single, customer-specific service-provider VLAN (SVLAN). The encapsulated packet consists of an inner CVLAN tag of the private customer network and an outer SVLAN tag of the public provider network. In VLAN translation, single- or double-tagged CVLAN IDs are swapped with an SVLAN at the ingress provider edge device. Customer traffic is then forwarded based on the SVLAN ID in the provider network. The CVLANs are lost in the translation.</p> <ul style="list-style-type: none"> You cannot configure the same SVLAN ID for both a Q-in-Q VLAN tunnel and a CVLAN to SVLAN translation. If you configure a multi-tag CVLAN-to-SVLAN mapping, all flows on the SVLAN must be either all single-tagged or all double-tagged CVLANs. Only L2 traffic is supported on an SVLAN; L3 configuration settings are not supported.

- To remove a Q-in-Q VLAN tunnel configuration a VLAN translation, enter the `no switchport vlan-mapping svlan-id` command.
- To remove the priority bit configuration for the SVLAN tag in both Q-in-Q VLANs and VLAN translation, use the `no switchport vlan-mapping svlan-id priority` command.

Examples: VLAN translation

```
sonic(config-if-Eth1/1)# switchport vlan-mapping 100 200
sonic(config-if-Eth1/1)# switchport vlan-mapping 101 inner 111 200
priority 4
sonic(config-if-Eth1/1)# switchport vlan-mapping 150 350 priority 3
multi-tag
sonic(config-if-Eth1/1)# switchport vlan-mapping 360 inner 160 460
priority 2 multi-tag
```

Examples: Q-in-Q VLAN tunneling

```
sonic(config-if-Eth1/1)# switchport vlan-mapping 20,30 dot1q-tunnel 100
sonic(config-if-Eth1/1)# switchport vlan-mapping add 30-40 dot1q-tunnel
100
```

Releases

4.1.0 or later

system-mac

Configures a system MAC address that is used to bring up a port channel that connects multihomed VTEPs.

Command

`system-mac XX:XX:XX:XX:XX:XX`

Options

`XX:XX:XX:XX:XX:XX`—MAC address used to calculate the ES-ID for a multihomed VTEP port channel.

Modes

PORT CHANNEL

Usage

You configure a System MAC address in Port-Channel mode when you specify the Type-0, Type-1, or Type-3 Ethernet segment type. To remove a system MAC address, enter the `no system-mac XX:XX:XX:XX:XX:XX` command.

Examples

```
sonic(config)# interface PortChannel1
sonic(config-if-pol1)# system-mac 00:00:00:0a:00:01
sonic(config-if-pol1)# evpn ethernet-segment auto-system-mac
```

Releases

4.2.0 or later

system resource-stats-polling-interval

Configures a polling interval to retrieve system resource utilization metrics.

Command

`system resource-stats-polling-interval polling-interval`

Options

`polling-interval`—Enter the polling interval in seconds (120 to 3600; default is 120).

Modes

CONFIGURATION

Usage

This command configures the polling interval to retrieve system resource utilization metrics, such as CPU and memory.

Examples

```
sonic# configure terminal
sonic(config)# system resource-stats-polling-interval 300
```

```
sonic(config)# no system resource-stats-polling-interval
```

Releases	4.2.0 or later
-----------------	----------------

system vlan

Configures reserve contiguous 128 VLANs.

Command	system vlan <i>vlan-id</i> reserve
----------------	------------------------------------

Options	<i>vlan-id</i> —Starting VLAN ID of 128 VLANs to be reserved
----------------	--

Modes	CONFIGURATION
--------------	---------------

Usage	This command reserves 128 contiguous VLANs. The no form of this command would change the reserved VLAN range to default. The default reserved VLAN range is 3967 to 4094.
--------------	---

Examples	
-----------------	--

```
sonic# configure terminal  
sonic(config)# system vlan 600 reserve
```

```
sonic(config)# no system vlan 600 reserve
```

Releases	4.0 or later
-----------------	--------------

T, U, V, W, and Z commands

Topics:

- table-map
- tacacs-server auth-type
- tacacs-server host
- tacacs-server key
- tacacs-server source-interface
- tacacs-server timeout
- tail-stamping
- tam
- tcam
- tcp-connect
- tcp-timeout
- techsupport-export enable
- techsupport-export interval
- techsupport-export remote-server
- terminal length
- terminal timeout
- test cable-diagnostics
- threshold
- threshold (IP SLA)
- threshold buffer-pool
- threshold device
- threshold priority-group
- threshold queue
- timeout
- timeout (IP-SLA)
- timeout (NAT)
- timers
- timers
- tos
- tpcm install
- tpcm uninstall
- tpcm update
- tpcm update disk-limit
- tpcm upgrade
- traceroute
- traceroute6
- track-interface
- traffic-class
- transmit-interval
- ttl
- ttl-security hops
- type
- udld aggressive
- udld enable
- udld message-time
- udld multiplier
- udp-timeout

- unreliable-ls
- unsuppress-map
- update-delay
- update-source
- usb enable
- usb mount
- username password role
- use-v2-checksum
- v6only
- version
- vip
- vlan-stacking
- vni
- vni-downstream
- voice
- voice-signaling
- vrrp
- warm-reboot
- warm-restart bgp
- watermark interval
- watermark telemetry
- weight
- write memory
- write erase
- write erase boot
- write erase install
- write-multiplier
- write-quanta
- ztp enable

table-map

Applies a BGP table to RIB manager route download filter.

Command	<code>table-map <i>rtmap</i></code>
Options	<code><i>rtmap</i></code> — Route-map name
Modes	ADDRESS-FAMILY
Usage	This command enables route-map on route updates from BGP to Zebra (RIB manager). All applicable match operations are allowed, including match on prefix, next-hop, communities, and so on. Set operations for this attach-point are limited to metric and next-hop only. Any operation does not affect BGPs internal RIB.
Examples	<pre>sonic(config-router-bgp) # address-family ipv4 unicast sonic(config-router-bgp-af) # table-map rmap_block_private</pre> <pre>sonic(config-router-bgp-af) # no table-map rmap_block_private</pre>
Releases	3.0 or later

tacacs-server auth-type

Configures the global TACACS+ server authentication type that is used for remote access.

Command	<code>tacacs-server auth-type [pap chap mschap login]</code>
----------------	--

Options	<ul style="list-style-type: none"> • <code>chap</code> — Enables challenge handshake authentication protocol • <code>pap</code> — Enables password authentication protocol (default) • <code>mschap</code> — Enables Microsoft challenge handshake authentication protocol • <code>login</code> — Enables Microsoft challenge handshake authentication protocol
Modes	CONFIGURATION
Usage	<p>The authentication type is used to encrypt or decrypt data that is sent and received between the switch and the TACACS+ server. If you do not specify an authentication type using tacacs-server host, <code>pap</code> is used as the default value. Different authentication types use different access-request and access-challenge messages. If you have not configured a server-specific authentication type, this global value is used for that server. To view the configured TACACS+ authentication types, use show tacacs-server host.</p>
Examples	<pre>sonic(config)# tacacs-server auth-type chap</pre> <pre>sonic(config)# no tacacs-server auth-type</pre>
Releases	3.0 or later

tacacs-server host

Configures a TACACS+ server and the key used to authenticate the switch on the server.

Command	<code>tacacs-server host <i>host</i> [port <i>port-val</i>] [timeout <i>timeout-val</i>] [key <i>key-val</i>] [<i>type type-val</i>] [<i>priority priority-val</i>] [<i>vrf {mgmt}</i>]</code>
Options	<ul style="list-style-type: none"> • <code>host</code> — IPv4 or IPv6 host address in A.B.C.D or A::B format • <code>port_val</code> — TCP port number on the server (1 to 65535; default 49) • <code>timeout-val</code> — Transmission timeout in seconds (1 to 60; default 5) • <code>key-val</code> — Secret key that is shared between a TACACS+ server and the switch (up to 32 characters) • <code>type-val</code> — Authentication type; the authentication algorithm is used to encrypt/decrypt data that is sent and received between the switch and the TACACS+ server <ul style="list-style-type: none"> ◦ <code>chap</code> — Challenge handshake authentication protocol ◦ <code>pap</code> — Password authentication protocol (default) ◦ <code>mschap</code> — Microsoft challenge handshake authentication protocol • <code>priority-val</code> — Priority used to access multiple TACACS+ servers to authenticate users (1 highest priority to 64; default 1)
Mode	CONFIGURATION
Usage	<p>You can configure up to seven TACACS+ servers for remote user authentication. The configured TACACS+ server addresses are updated in the <code>/etc/pam.d/common-auth-sonic</code> configuration file that is used by the TACACS service. The authentication key must match the key configured on the TACACS+ server, and you cannot enter spaces in the key. You can configure the global timeout allowed for authentication requests on TACACS+ servers using radius-server timeout. To view the configured TACACS+ servers, use show tacacs-server host.</p>
Examples	<pre>sonic(config)# tacacs-server host 1.1.1.1 port 11 timeout 10 key mykey type pap priority 11</pre> <pre>sonic(config)# no tacacs-server host 1.1.1.1</pre>
Releases	3.0 or later

tacacs-server key

Configures the global shared secret authentication key for the TACACS+ server.

Command	<code>tacacs-server key <i>secret-key</i></code>
Options	<code><i>secret-key</i></code> — Authentication key (up to 32 characters)
Modes	CONFIGURATION
Usage	Use this command to configure a global shared secret key that is used by the switch as a TACACS+ client to authenticate itself on a TACACS+ server. Valid characters are 0 to 9, A to Z, and a to z. The authentication key can include all printable ASCII characters with a few exceptions (#, SPACE, and COMMA). The global shared key is used only on TACACS+ authentication servers configured without a key secret value using tacacs-server host . To view the configured TACACS+ server keys, use show tacacs-server host .

Examples	<pre>sonic(config)# tacacs-server key testing123</pre> <pre>sonic(config)# no tacacs-server key</pre>
-----------------	--

Releases	3.0 or later
-----------------	--------------

tacacs-server source-interface

Configures the global IPv4 or IPv6 TACACS+ server address.

Command	<code>tacacs-server source-interface {Ethernet <i>port</i>[.<i>subport</i>] Loopback <i>loopback-id</i> Management <i>mgmt-id</i> PortChannel <i>portch-id</i> Vlan <i>vlan-id</i>}</code>
Options	<ul style="list-style-type: none">• <code><i>port</i>[.<i>subport</i>]</code>—Ethernet interface or sub-interface• <code><i>loopback-id</i></code>—Loopback interface• <code><i>mgmt-id</i></code>—Management interface (0)• <code><i>portch-id</i></code>—PortChannel interface or sub-interface• <code><i>vlan-id</i></code>—VLAN interface
Modes	CONFIGURATION
Usage	Use this command to configure the source interface used by the switch to communicate with TACACS+ servers. By default, no source interface is configured. To view the configured TACACS+ server information, use show tacacs-server host .
Examples	<pre>sonic(config)# tacacs-server source-interface Ethernet 10.1.1.1</pre> <pre>sonic(config)# no tacacs-server source-interface</pre>
Releases	3.1 or later

tacacs-server timeout

Configures the global timeout used for authentication attempts on TACACS+ servers.

Command	<code>tacacs-server timeout <i>seconds</i></code>
Options	<code><i>seconds</i></code> — Timeout period to wait for an authentication response from a TACACS+ server (1 to 60 seconds; default 5)
Modes	CONFIGURATION

Usage Use this command to configure a global timeout value for all TACACS+ servers used for remote authentication. The global timeout is used only on TACACS+ authentication servers configured without a specified timeout using [tacacs-server host](#). If you have not configured a server-specific timeout, this global value is used for that TACACS+ server. To view the configured TACACS+ server information, use [show tacacs-server host](#).

Examples

```
sonic(config)# tacacs-server timeout 60
```

```
sonic(config)# no tacacs-server timeout
```

Releases 3.0 or later

tail-stamping

Configures tail-stamping.

Command tail-stamping
Options None
Modes TAM
Usage Use this command to enter the mode to configure tail-stamping.
Example

```
tor1(config)# tam
tor1(config-tam)# tail-stamping
tor1(config-tam-ts) #
```

Releases 3.1 or later

tam

Enters telemetry and monitoring (TAM) device configuration mode.

Command tam
Options None
Modes CONFIGURATION
Usage Use this command to enter the TAM configuration mode.
Example

```
sonic(config)# tam
sonic(config-tam) #
```

Releases 3.0 or later

tcam

Configures TCAM Key-profile parameters.

Command tcam
Options None
Modes HARDWARE
Usage Use this command to enter the hardware TCAM mode to configure TCAM key profile parameters for forwarding flow-based services, monitoring flow-based services, and QoS flow-based services.

Examples

```
sonic# configure terminal  
sonic(config)# hardware  
sonic(config-hardware)# tcam  
sonic(config-hardware-tcam)#[/pre>
```

Releases

4.0 or later

tcp-connect

Configures the operation type as TCP, the target IP address, and the destination port for an IP SLA instance.

Command `tcp-connect addr port-number port-number`**Options** • *addr*—IP address in A.B.C.D format• *port-number*—The destination TCP port number.**Mode** IP-SLA**Usage** The command enables TCP-based IP SLA for tracking a destination.**Examples**

```
sonic(config)# ip sla 1  
sonic(config-ipsla-1)# tcp-connect 1.1.1.1 port 100  
sonic(config-ipsla-1-tcp)#[/pre>
```

```
sonic# no tcp-connect
```

Releases

3.1 or later

tcp-timeout

Configures the TCP NAT entry aging timeout in seconds.

Command `tcp-timeout tcp-timeout-value`**Options** *tcp-timeout-value*—NAT entry aging timeout in seconds (300 to 432000; default is 86400)**Modes** NAT**Usage** Use this command to change the TCP entry aging timeout for address translation.**Examples**

```
sonic(config-nat)# tcp-timeout 500
```

```
sonic(config-nat)# no tcp-timeout
```

Releases

3.0 or later

techsupport-export enable

Enables periodic export of technical support to a remote server.

Command `techsupport-export enable {on | off}`**Options** • *on*—Enable technical support export.
• *off*—Disable technical support export.**Modes** CONFIGURATION**Usage** Use `techsupport-export remote-server` to configure the remote server to which the tech-support has to be exported.

Examples

```
sonic# configure terminal  
sonic(config)# techsupport-export enable on
```

Releases

4.0 or later

techsupport-export interval

Configures the periodic export interval of technical support in minutes.

Command `techsupport-export interval interval`**Options** *interval*—Interval in minutes (30 to 1440; default is 30)**Modes** CONFIGURATION**Usage** Use this command to set the interval of technical support periodic export to a remote server.**Examples**

```
sonic# configure terminal  
sonic(config)# techsupport-export interval 600
```

Releases

4.0 or later

techsupport-export remote-server

Configures technical support export remote server.

Command `techsupport-export remote-server {ip-address | ipv6-address | host-name} {destdir dir-string} {username username} {password pwd} {protocol {scp | sftp}}`**Options**

- *host-address*—hostname
- *ip-address*—IP address
- *ipv6-address*—IPv6 address
- *dir-string*—remote directory
- *username*—username
- *pwd*—password
- *scp*—SCP protocol
- *sftp*—SFTP protocol

Modes CONFIGURATION**Usage** Use this command to configure the details of the remote SCP or SFTP server to which technical support has to be exported.**Examples**

```
sonic# configure terminal  
sonic(config)# techsupport-export remote-server 100.1.1.10 destdir tmp  
username  
admin password ***** protocol scp
```

Releases

4.0 or later

terminal length

Configures the number of lines to display on the terminal.

Command `terminal length length-value`**Options** *length-value* — Number of lines to display (0 to 512; default 24)

Modes	EXEC
Usage	Enter zero (0) for the terminal to display without pausing.
Example	<pre>sonic# terminal length 30</pre>
Releases	3.0 or later

terminal timeout

Configures the terminal timeout.

Command	<code>terminal timeout <i>timeout-value</i></code>
Options	<i>timeout-value</i> — CLI terminal session timeout value in seconds (0 to 3600; default 605)
Modes	EXEC
Usage	Enter zero (0) to disable the session timeout.
Example	<pre>sonic# terminal timeout 1200</pre>
Releases	4.0 or later

test cable-diagnostics

Run a cable diagnostics test.

Command	<code>test cable-diagnostics [Ethernet <i>if-id</i>]</code>
Options	<i>if-id</i> —(Optional) Ethernet interface ID
Modes	EXEC
Usage	Use this command to check the cable issues on RJ45 ports.
Examples	<pre>sonic# test cable-diagnostics !!WARNING!! This operation may cause disruption of traffic, continue? [y/N]:n</pre> <pre>sonic# test cable-diagnostics Ethernet 1 !!WARNING!! This operation may cause disruption of traffic, continue? [y/N]:</pre>
Releases	4.0 or later

threshold

Configures the threshold number of probes to be successful or lost before an uplink tracking session is brought up or down.

Command	<code>threshold {{type percentage {[up threshold-up]} {[down threshold-down]}}} {up threshold-up {[down threshold-down]}} {down threshold-down}</code>
Options	<ul style="list-style-type: none"> • <i>threshold-up</i>—Threshold up value. • <i>threshold-down</i>—Threshold down value.
Modes	LINK-STATE-TRACK
Usage	The threshold up value must be higher than the threshold down value. If the threshold up is not configured, it is assumed that all upstream interfaces are online to bring up downstream interfaces. If

the threshold down is not configured, it is assumed that all upstream interfaces are offline to shut down downstream interfaces.

Examples

```
sonic(config-link-track) # threshold type percentage up 70 down 40  
  
sonic(config-link-track) # threshold up 80  
  
sonic(config-link-track) # threshold down 20  
  
sonic(config-link-track) # no threshold down
```

Releases

3.1 or later

threshold (IP SLA)

Timeout in seconds to wait before declaring loss of probe.

Command

`threshold threshold-value`

Options

threshold-value—Threshold value in seconds. The range is from 1 to 300.

Modes

IP-SLA

Usage

Configure the number of probes to be successful or lost before an IP SLA session is brought up or down.

Examples

```
sonic(config-link-track) # threshold 50
```

Releases

3.1 or later

threshold buffer-pool

Configures the buffer pool threshold on ingress or egress buffers pools-lossy or lossless.

Command

`threshold buffer-pool buffer_pool_name {multicast | shared} threshold_value`

Options

- *buffer_pool_name*—Buffer pool name
- *threshold_value*—Threshold value in percentage (1 to 100)

Modes

CONFIGURATION

Usage

Use this command to configure the threshold used for ingress and egress buffers in the switch-level buffer pool or a specified port-level buffer pool. Buffer pools are used on ingress and egress interfaces for lossy or lossless traffic. To display a list of buffer-pool names, use the `show buffer pool` command.

Examples

```
sonic(config) # threshold buffer-pool ingress_lossless_pool shared 1
```

```
sonic(config) # threshold buffer-pool egress_lossless_pool shared 50
```

```
sonic(config) # no threshold buffer-pool ingress_lossless_pool shared
```

Releases

3.1 or later

threshold device

Configures device threshold buffer.

Command	threshold device <i>threshold_value</i>
Options	<i>threshold_value</i> —Threshold value (1 to 100)
Modes	CONFIGURATION
Usage	Use this command to configure the threshold used for the global switch-level buffer pool. To remove the threshold configured for the global switch-level buffer pool, enter the no threshold device command.
Examples	<pre>sonic(config)# threshold device 77</pre>
Releases	4.0 or later

threshold priority-group

Configures a threshold for a specific priority group that is shared or headroom buffer of an interface.

Command	threshold priority-group <i>priority-group-index</i> {headroom shared} <i>threshold_value</i>
Options	<ul style="list-style-type: none">• <i>priority-group-index</i>—Specify the priority group index (0 to 7).• <i>threshold_value</i>—Specify the threshold value in percentage (1 to 100).• <i>shared</i>—Specifies the threshold for shared memory buffer usage for a priority group.• <i>headroom</i>—Specifies the additional buffer limit that can be used to when the shared buffer is exhausted, such as when flow control is enabled.
Modes	INTERFACE
Usage	Configure the threshold for priority-group traffic in the shared or headroom buffer on an ingress port interface. To remove the threshold that is configured for a shared or headroom priority-group buffer on an ingress port interface, enter the no form of this command.
Examples	<pre>sonic(config-if-Eth1/28)# threshold priority-group 5 headroom 57</pre> <pre>sonic(config-if-Eth1/28)# threshold priority-group 7 shared 78</pre> <pre>sonic(config-if-Eth1/28)# no threshold priority-group</pre>
Releases	3.1 or later

threshold queue

Configures a threshold for a specific unicast or multicast queue of an interface.

Command	threshold queue <i>queue_index</i> {unicast multicast} <i>threshold_value</i>
Options	<ul style="list-style-type: none">• <i>queue_index</i>—Queue index (0 to 7)• <i>unicast</i>—Unicast• <i>multicast</i>—Multicast• <i>threshold_value</i>—Threshold value in percentage (1 to 100)
Modes	INTERFACE
Usage	Re-enter this command to configure additional unicast or multicast queue thresholds on the interface.

Examples

```
sonic(config-if-Ethernet28)# threshold queue 4 unicast 47  
sonic(config-if-Ethernet28)# threshold queue 2 multicast 67  
sonic(config-if-Ethernet28)# no threshold queue
```

Releases

3.1 or later

timeout

Configures the aging timeout in seconds for link state tracking.

Command `timeout timeout-value`**Options** `timeout-value`—Aging timeout in seconds (1 to 1800).**Modes** LINK-TRACK**Usage** Use this command to configure the aging timeout to wait before bringing up a downstream interface after one or more uplink interfaces come up.**Examples**

```
sonic(config)# link state track trackGrp  
sonic(config-link-track)# timeout 300  
  
sonic(config-link-track)# no timeout
```

Releases

3.0 or later

timeout (IP-SLA)

Configures the timeout value in seconds for IP-SLA.

Command `timeout timeout-value`**Options** `timeout-value`—Aging timeout in seconds (1 to 300; default is 3)**Modes** IP-SLA**Usage** Use this command to configure the timeout value to wait before declaring the loss of probe.**Examples**

```
sonic(config-ip-sla)# timeout 25
```

Releases

3.1 or later

timeout (NAT)

Configures the timeout value in seconds for NAT.

Command `timeout timeout-value`**Options** `timeout-value`—Aging timeout in seconds ((300 to 432000)**Modes** NAT**Usage** By default, dynamic address translation configurations are set to timeout after 10 minutes (600 seconds) of inactivity. However, static NAT entries do not have a timeout.

Examples

```
sonic(config) # ip sla sla-id  
sonic(config-ip-sla) # timeout 400
```

Releases

3.1 or later

timers

Adjusts BGP keepalive and hold time intervals.

Command

```
timers {keepalive-intvl hold-time} [ {connect connect-time} ]
```

Options

- *keepalive-intvl*—Keepalive time interval, in seconds, between keepalive messages sent to the neighbor routers (1 to 3600; default 60)
- *hold-time*—Hold time interval, in seconds, between the last keepalive message and declaring a router dead (1 to 3600; default 180)
- *connect-time*—(Optional) Connect time interval in seconds (1-65535)

Modes

- ROUTER-BGP
- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage

Use this command to configure keepalive, hold timer, and connect neighbor and peer-group interval values for an instance of BGP. The configured timer value becomes effective after a BGP hard restart. The timer values negotiate from peers. The `connect` option only applies to BGP-NEIGHBOR and BGP-PEER-GROUP modes.

Examples

```
sonic(config) # router bgp 65300  
sonic(config-router-bgp) # timers 10 30
```

```
sonic(config) # router bgp 100  
sonic(config-router-bgp) # neighbor 30.30.30.3  
sonic(config-router-bgp-neighbor) # timers 3 9
```

```
sonic(config) # router bgp 100  
sonic(config-router-bgp) # peer-group PG_Ext  
sonic(config-router-bgp-pg) # timers 3 9
```

```
sonic(config-router-bgp) # no timers
```

Releases

3.0 or later

timers

Configures OSPFv2 LSA and SPF intervals.

Command

```
timers {{lsa {min-arrival minarrivaltimer}} | {throttle {{lsa {all  
lsadelaytimer}} | {spf spfdelaytime spfinitialholdtime spfmaxholdtime}}}}
```

Options

- *minarrivaltimer*—Minimum arrival timer in milliseconds (0 to 600000)
- *lsadelaytimer*—LSA delay timer in milliseconds (0 to 5000)
- *spfdelaytime*—SPF delay time in milliseconds (0 to 600000)
- *spfinitialholdtime*—SPF initial hold time in milliseconds (0 to 600000)
- *spfmaxholdtime*—SPF maximum hold time in milliseconds (0 to 600000)

Modes

ROUTER-OSPF

Usage

Use this command to configure OSPFv2 LSA refresh interval, minimum interval, and throttle timer. OSPFv2 SPF algorithm throttle timers set initial-delay, the initial-hold-time, and the maximum-hold-time between when SPF is calculated and the event which triggered the calculation.

Examples

```
sonic(config)# router ospf  
sonic(config-router-ospf)# timers lsa min-arrival 30  
sonic(config-router-ospf)# timers throttle lsa all 150
```

```
sonic(config)# router ospf  
sonic(config-router-ospf)# timers throttle spf 200 400 10000
```

Releases

3.2 or later

tos

Defines the type of service (ToS) byte for ICMP and TCP IP SLA.

Command

`tos tos-value`

Options

`tos-value`—TOS type byte in the IPv4 header (1 to 255).

Modes

- IP-SLA-ICMP
- IP-SLA-TCP

Usage

Use this command to set the ToS value for ICMP-ECHO and TCP-CONNECT under IP-SLA.

Examples

```
sonic(config)# ip sla 10  
sonic(config-ipsla-10)# icmp-echo 10.30.1.2  
sonic(config-ipsla-10-icmp)# tos 4
```

```
sonic(config)# ip sla 20  
sonic(config-ipsla-20)# tcp-connect 1.1.1.1 port 100  
sonic(config-ipsla-20-tcp)# tos 4
```

```
sonic(config-ipsla-10-icmp)# no tos
```

Releases

3.1 or later

tpcm install

Install a TPC image file.

Command

- From an external HTTP/HTTPS server: `tpcm install name tpc-container-name url url [vrf-name vrf-name] [args docker-arguments] [cargs container-arguments] [start-after-system-ready {True | False}]`
- From an external server using SCP or SFTP: `tpcm install name tpc-container-name {scp | sftp} server-name username password password filename tpc-image-path [vrf-name vrf-name] [args docker-arguments] [cargs container-arguments] [start-after-system-ready {True | False}]`
- From a local media path: `tpcm install name tpc-container-name file tpc-image-path [vrf-name vrf-name] [args docker-arguments] [cargs container-arguments] [start-after-system-ready {True | False}]`
- From an external Docker repository: `tpcm install name tpc-container-name pull image-name [:tag-name] [vrf-name vrf-name] [args docker-arguments] [cargs container-arguments] [start-after-system-ready {True | False}]`
- From an existing Docker image: `tpcm install name tpc-container-name image image-name [:tag-name] [vrf-name vrf-name] [args docker-arguments] [cargs container-arguments] [start-after-system-ready {True | False}]`

Options

- `name tpc-container-name` — Enter the name of the container (255 characters maximum).
- `url url` — Enter the URL of the server where the TPC image is stored.

- `{scp | sftp} server-name username username password password filename tpc-image-path` — Enter the SCP or SFTP server name, login credentials, and TCP image file path.
- `file tpc-image-path` — Enter the path on the local installed media where the TPC image is stored.
- `pull image-name [:tag-name]` — Enter the name of a TPC image in a Docker repository.
- `image image-name [:tag-name]` — Enter the name of an existing Docker image.
- `vrf-name vrf-name` — (Optional) Enter the name of the VRF in which the container runs (15 characters maximum in the format: `Vrfname`); by default, a TPC uses the default VRF.
- `args docker-arguments` — (Optional) Enter standard docker arguments.
- `cargs container-arguments` — (Optional) Enter container arguments to specify additional arguments for a container's init process or a script; for example, “`-path.rootfs=/host`”.
- `start-after-system-ready {True | False}` — (Optional) Specify whether to bring up the container after system startup. Default: True.

Modes

EXEC

Usage

Use this command to install a TPC image from one of the following sources: HTTP server, SCP path, SFTP server, local media folder, Docker hub, or an existing Docker image. You can install one or more TPC images on the system.

Example

From an external HTTP/HTTPS server:

```
sonic# tpcm install name mydocker url http://myserver/path/
mydocker.tar.gz args " -e TESTENV=TESTVALUE"
```

From an external server using SCP or SFTP:

```
sonic# tpcm install name mydocker scp myserver username myuser password
passwd filename /path/mydocker.tar.gz
```

From a local media path:

```
sonic# tpcm install name mydocker url http://myserver/path/
mydocker.tar.gz args " -e TESTENV=TESTVALUE"
```

From an external Docker repository:

```
sonic# tpcm install name mydocker pull ubuntu:latest
```

From an existing Docker image:

```
sonic# tpcm install name mydocker image ubuntu:latest
```

Releases

4.1.0 or later

tpcm uninstall

Uninstall a third-party container.

Command

`tpcm uninstall name tpc-container-name [clean-data {Yes | No}]`

Options

- `name tpc-container-name` — Enter the name of the container.
- `clean-data {Yes | No}` — (Optional) Specify whether to remove container data (Yes) or to leave it in the system (No). Default: No.

Modes

EXEC

Usage

Use this command to uninstall a TPC container. After a third-party container and its associated service are removed, the removed TPC services do not automatically start at the next system reboot.

Example

```
sonic# tpcm uninstall name mydocker clean-data Yes
```

Releases	4.1.0 or later
-----------------	----------------

tpcm update

Update the configuration settings of an installed TPC image.

Command	<code>tpcm update name <i>tpc-container-name</i> [memory <i>memory-value</i>] [vrf-name <i>vrf-name</i>] [start-after-system-ready {True False}]</code>
Options	<ul style="list-style-type: none"> • <i>name tpc-container-name</i>—Enter the name of the container (255 characters maximum). • <i>memory memory-value</i>—Enter the memory that is allocated to a TPC with one of the b k m g characters or a KB, MB, or GB value; or a K, M, or G value; or enter a memory unit without any postfix character to be considered as a simple byte value. Default: The overall memory limit for a TPC is 20% of the total system memory. • <i>vrf-name vrf-name</i>—(Optional) Enter the name of the VRF in which the container runs (15 characters maximum in the format: <i>Vrfname</i>); by default, a TPC uses the default VRF. • <i>start-after-system-ready {True False}</i>—(Optional) Specify whether to bring up the container after system startup. Default: True.
Modes	EXEC
Usage	<p>Use this command to update any of the following configuration settings of an installed TPC image:</p> <ul style="list-style-type: none"> • VRF in which the TPC runs and restarts the TPC. • start-after-system-ready setting—Brings up the container after system startup. • Memory capacity of the TPC—Reconfigures the memory limit and does not restart the TPC. <p>To reconfigure the memory limit for all TPCs installed on the switch, use the <code>tpcm update disk-limit</code> command.</p>
Example	<pre>sonic# tpcm update name TEST memory 200M vrf-name "mgmt" start-after-system-ready False sonic# tpcm update name TPC2 memory 1G vrf-name "mgmt" start-aftersystem-ready False sonic# tpcm update name TPC3 memory 500M vrf-name "mgmt" start-aftersystem-ready False</pre>

Releases	4.1.0 or later
-----------------	----------------

tpcm update disk-limit

Update the overall disk limit for all third-party containers installed on the switch.

Command	<code>tpcm update disk-limit <i>disk-value</i></code>
Options	<i>disk-value</i> —Enter a value to be used to set the maximum disk space allowed for all TPCs on the switch. The disk-value must be a unit with one of the postfix characters: G M K g m k. The disk-value cannot be a single decimal number.
Modes	EXEC
Usage	Use this command to update the overall disk limit for all installed third-party containers.
Examples	<pre>sonic# tpcm update disk-limit 8G sonic# tpcm update disk-limit 4000M</pre>

Releases	4.1.0 or later
-----------------	----------------

tpcm upgrade

Upgrade a TPC image file and its configuration.

Command `tpcm upgrade name tpc-container-name [url url] [{scp | sftp} server-name username username password password filename tpc-image-path] [args docker-arguments] [cargs container-arguments] [skip-data-migration {Yes | No}]`

- Options**
- *name tpc-container-name* — Enter the name of the container (255 characters maximum).
 - *url url* — (Optional) Enter the URL of the server where the TPC image is stored.
 - *{scp | sftp} server-name username password password filename tpc-image-path* — (Optional) Enter the SCP or SFTP server name, login credentials, and TCP image file path.
 - *args docker-arguments* — (Optional) Enter standard docker arguments.
 - *cargs container-arguments* — (Optional) Enter container arguments to specify additional arguments for a container's init process or a script; for example, “*-path.rootfs=/host*”.
 - *skip-data-migration {Yes | No}* — (Optional) Specify whether to migrate and retain container data (No) or to not migrate the data (Yes). Default: No.

Modes EXEC

Usage Use this command to upgrade a TPC image and one or more of its configuration settings. The TPC settings which you can upgrade with the image are:

- Skip-data-migration — Brings up the container after system startup.
- Docker arguments, such as `--privileged`, `--network`, `--memory`
- Container arguments, such as `"-path.rootfs=/host"`

Example

```
sonic# tpcm upgrade name mydocker image ubuntu:latest
```

```
sonic# tpcm upgrade name mydocker sftp myserver username myuser password  
passwd filename mydocker.tar.gz skip_data_migration yes  
args "--memory=500M" args " -e TESTENV=TESTVALUE"
```

Releases 4.1.0 or later

traceroute

Traces route packets to the host.

Command `traceroute [vrf {mgmt | vrf-name}]`

Options *vrf {mgmt | vrf-name}*—(Optional) Traces the route to an IPv4/IPv6 address in the management or a specified VRF instance.

Modes EXEC

Usage Use this command to display the routes that packets take to a destination IPv4 address.

i **NOTE:** The syntaxes for this command contain the most commonly used options. For a complete parameter list, see the Linux man page of the traceroute command.

Example

```
sonic# traceroute -I 1.1.1.1  
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets  
1 10.11.90.254 (10.11.90.254) 0.978 ms 1.010 ms 1.050 ms  
2 10.11.3.253 (10.11.3.253) 0.657 ms 0.694 ms 0.779 ms  
3 10.11.27.254 (10.11.27.254) 0.499 ms 0.478 ms 0.447 ms  
4 * 63.80.56.65 (63.80.56.65) 0.871 ms *  
5 * * *  
6 * * *  
7 * * *  
8 * * *  
9 * * *
```

```
10 * * *
11 * *
12 1.1.1.1 (1.1.1.1) 2.194 ms 2.186 ms 2.181 ms
```

Releases	3.1 or later
-----------------	--------------

traceroute6

Traces route packets to the IPv6 host.

Command	<code>traceroute6 [vrf {mgmt vrf-name}]</code>
Options	<code>vrf {mgmt vrf-name}</code> —(Optional) Traces the route to an IPv4/IPv6 address in the management or a specified VRF instance.
Modes	EXEC
Usage	Use this command to display the routes that packets take to a destination IPv6 address. i NOTE: The syntaxes for this command contain the most commonly used options. For a complete parameter list, see the Linux man page of the <code>traceroute6</code> command.

Example
<pre>sonic# traceroute6 20::1 traceroute to 20::1 (20::1), 30 hops max, 80 byte packets 1 20::1 (20::1) 2.622 ms 2.649 ms 2.964 ms</pre>

Releases	3.1 or later
-----------------	--------------

track-interface

Configures VRRP track interface for priority values.

Command	<code>track-interface interface-name {weight wt_value}</code>
Options	<ul style="list-style-type: none">• <code>interface-name</code>—Interface name. Ethernet, Loopback, or a VLAN interface• <code>wt_value</code>—Weight value (1 to 254)
Modes	VRRP
Usage	Use this command to increase the effective priority by weight value if the track interface is up.
Examples	<pre>sonic(config-if-Eth1/4)# vrrp 1 address-family ipv4 sonic(config-if-Eth1/4-vrrp-ipv4-1)# track-interface Ethernet12 weight 10 sonic(config-if-Eth1/4)# vrrp 1 address-family ipv6 sonic(config-if-Eth1/4-vrrp-ipv6-1)# track-interface Ethernet24 weight 10 sonic(config-if-Eth1/4-vrrp-ipv4-1)# no track-interface Ethernet12 sonic(config-if-Eth1/4-vrrp-ipv6-1)# no track-interface Ethernet24</pre>

Releases	3.1 or later
-----------------	--------------

traffic-class

Adds an entry to map traffic class to queue.

Command	<code>traffic-class tc {dot1p dot1p-val dscp dscp-val priority-group pg queue qid}</code>
----------------	---

- Options**
- *tc*—Traffic class (0 to 7)
 - *dot1p-val*—dot1p value (0 to 7)
 - *dscp-val*—DSCP value (0 to 63)
 - *pg*—Priority group value (0 to 7)
 - *qid*—Queue ID (0 to 7)

- Modes**
- QOS MAP TC-DOT1P
 - QOS MAP TC-DSCP
 - QOS MAP TC-PG
 - QOS MAP TC-QUEUE

Usage

Use this command to add an entry to map traffic class to a queue.

Examples

```
sonic(config)# qos map tc-dot1p tc_dot1p
sonic(config-tc-dot1p-map-tc_dot1p)# traffic-class 0 dot1p 0
sonic(config-tc-dot1p-map-tc_dot1p)# traffic-class 1 dot1p 1
sonic(config-tc-dot1p-map-tc_dot1p)# traffic-class 3 dot1p 2
```

```
sonic(config)# qos map tc-dscp tc_dscp
sonic(config-tc-dscp-map-tc_dscp)# traffic-class 0 dscp 0
sonic(config-tc-dscp-map-tc_dscp)# traffic-class 1 dscp 10
sonic(config-tc-dscp-map-tc_dscp)# traffic-class 3 dscp 29
```

```
sonic(config-tc-dot1p-map-tc_dot1p)# no traffic-class 3
sonic(config-tc-dscp-map-tc_dscp)# no traffic-class 3
```

Releases

3.1 or later

transmit-interval

Configures the minimum interval to transmit BFD packets.

Command

`transmit-interval transmit_interval`

Options

transmit_interval—Peer transmit interval in milliseconds (10 to 60000; default is 300)

- Modes**
- PEER
 - BFD PROFILE

Usage

Use this command to configure the minimum transmission interval during which the system can send BFD control packets.

Example

```
sonic# configure terminal
sonic(config)# bfd
sonic(config-bfd)# peer 192.168.0.5 interface Ethernet0
sonic(config-bfd-peer)# transmit-interval 11
```

Example for PROFILE mode:

```
sonic# configure terminal
sonic(config)# bfd
sonic(config-bfd)# profile fast
sonic(config-bfd-profile)# transmit-interval 11
```

Releases

3.0 or later

ttl

Configures the maximum hop count for ICMP and TCP with IP SLA.

Command `ttl ttl-value`

Options `ttl-value`—The maximum hop count (1 to 255) .

- Modes**
- IP-SLA-ICMP
 - IP-SLA-TCP

Usage This command configures the TTL value or hop count for an ICMP echo request packet or a TCP connection request.

Examples

```
sonic(config-ipsla-10)# icmp-echo 30.30.1.2  
sonic(config-ipsla-10-icmp)# ttl 16
```

```
sonic(config-ipsla-20)# tcp-connect 10.30.1.2 22  
sonic(config-ipsla-20-tcp)# ttl 12
```

```
sonic(config-ipsla-10-icmp)# no ttl
```

Releases 3.1 or later

ttl-security hops

Configures the number of hops for a neighbor, and only those neighbors that are within the specified number of hops are permitted to become neighbors.

Command `ttl-security hops nhops`

Options `nhops`—Specified number of hops to be allowed to become a neighbor (1 to 254)

- Modes**
- BGP-NEIGHBOR
 - PEER-GROUP

Usage This command is mutually exclusive with [ebgp-multihop](#).

Examples

```
sonic(config)# router bgp 100  
sonic(config-router-bgp)# neighbor 30.30.30.3  
sonic(config-router-bgp-neighbor)# ttl-security hops 6
```

```
sonic(config)# router bgp 100  
sonic(config-router-bgp)# peer-group PG_Ext  
sonic(config-router-bgp-pg)# ttl-security hops 8
```

```
sonic(config-router-bgp-neighbor)# no ttl-security hops  
sonic(config-router-bgp-pg)# no ttl-security hops
```

Releases 3.0 or later

type

Configures the scheduler type.

Command `type type`

Options `type`—Scheduler type

- `dwrr`—Deficit Weighted Round Robin

- `wrr`—Weighted Round Robin
- `strict`—Strict

Modes

QOS SCHEDULER-POLICY

Usage

Use this command to schedule each egress queue of an interface using DWRR, WRR, or by strict priority. These types are mutually exclusive.

Examples

```
sonic(config) # qos scheduler-policy scheduler_policy
sonic(config-sched-policy-scheduler_policy)# queue 0
sonic(config-scheduler-scheduler_policy-queue-0) # type dwrr
sonic(config-scheduler-scheduler_policy-queue-0) # exit
sonic(config-sched-policy-scheduler_policy)# queue 6
sonic(config-scheduler-scheduler_policy-queue-6) # type strict
sonic(config-scheduler-scheduler_policy-queue-6) #
```

Releases

3.1 or later

udld aggressive

Configures unidirectional link detection protocol (UDLD) mode to aggressive on an interface-level or globally.

Command `udld aggressive`

Options None

- Modes**
- CONFIGURATION
 - INTERFACE

Usage

By default all ports operate in normal mode. When global aggressive mode is enabled, all ports operate in aggressive mode.

Examples

```
sonic(config) # udld enable
sonic(config) # udld aggressive
```

```
sonic(config-if-Ethernet0) # udld enable
sonic(config-if-Ethernet0) # udld aggressive
```

```
sonic(config-if-Ethernet0) # no udld aggressive
```

Releases

3.0 or later

udld enable

Enables unidirectional link detection protocol (UDLD) at an interface-level or globally.

Command `udld enable`

Options None

- Modes**
- CONFIGURATION
 - INTERFACE

Usage

Use this command to enable UDLD globally or at an interface-level.

Examples

```
sonic(config) # udld enable
```

```
sonic(config) # no udld enable
```

Releases

3.0 or later

udld message-time

Configures the unidirectional link detection protocol (UDLD) message time interval at which periodic hellos are exchanged.

Command `udld message-time msg-time`

Options *msg-time*—Time interval period in seconds (1 to 30; default 1)

Modes CONFIGURATION

Usage Use this command to configure the unidirectional link detection protocol (UDLD) message time interval at which periodic hellos are exchanged.

Examples

```
sonic(config)# udld enable  
sonic(config)# udld message-time 3
```

```
sonic(config)# no udld message-time
```

Releases 3.0 or later

udld multiplier

Configures the unidirectional link detection protocol (UDLD) multiplier value.

Command `udld multiplier multiplier`

Options *multiplier*—UDLD multiplier value (3 to 10; default 3)

Modes CONFIGURATION

Usage This multiplier value is used to determine the timeout interval (message-time x the multiplier value) after which UDLD declares the link as unidirectional.

Examples

```
sonic(config)# udld enable  
sonic(config)# udld multiplier 8
```

```
sonic(config)# no udld multiplier
```

Releases 3.0 or later

udp-timeout

Configures UDP NAT entry aging timeout.

Command `udp-timeout udp-timeout-value`

Options *udp-timeout-value*—UDP timeout value in seconds (120 to 600; default is 300)

Modes NAT

Usage Use this command to change the UDP timeout for dynamic address translation.

Examples

```
sonic(config-nat)# udp-timeout 200
```

```
sonic(config-nat)# no udp-timeout
```

Releases 3.0 or later

unreliable-los

Configures unreliable Loss of Signal (LOS).

Command	<code>unreliable-los {auto on off}</code>
Options	<ul style="list-style-type: none">• <code>auto</code> — Automatically enables or disables unreliable LOS based on the transceiver that is detected on a port (default).• <code>on</code> — Enables LOS detection.• <code>off</code> — Disables LOS detection.
Modes	INTERFACE
Usage	Use unreliable LOS to avoid mistuned signal issues with installed transceivers. Automatic LOS detection is enabled by default.
	<p> NOTE: The no unreliable-los command does not remove the configuration from the interface. To reset unreliable LOS operation to the default <code>auto</code> mode, enter the <code>unreliable-los auto</code> command.</p>
Examples	<pre>sonic(config)# interface Eth1/2 sonic(config-if-Eth1/2)# unreliable-los {auto on off}</pre>
Releases	4.1.0 or later

unsuppress-map

Configures a route policy using a route-map to unsuppress suppressed routes.

Command	<code>unsuppress-map map</code>
Options	<code>map</code> —Route-map name
Modes	<ul style="list-style-type: none">• ADDRESS-FAMILY• PEER-GROUP
Usage	Use this command to configure a route policy using a route-map to unsuppress suppressed routes.
Examples	<pre>sonic(config)# router bgp 100 sonic(config-router-bgp)# neighbor 20.20.20.2 sonic(config-router-bgp-neighbor)# remote-as 300 sonic(config-router-bgp-neighbor)# address-family ipv4 unicast sonic(config-router-bgp-neighbor-af)# unsuppress-map rm_unsup_ext_rt sonic(config)# router bgp 100 sonic(config-router-bgp)# peer-group PG_Int sonic(config-router-bgp-pg)# address-family ipv4 unicast sonic(config-router-bgp-pg-af)# unsuppress-map rm_unsup_ext_rt sonic(config-router-bgp-neighbor-af)# no unsuppress-map rm_unsup_ext_rt sonic(config-router-bgp-pg-af)# no unsuppress-map rm_unsup_ext_rt</pre>
Releases	3.0 or later

update-delay

Sets the update delay which controls how long to wait before running best-path selection after graceful restart.

Command	<code>update-delay time [maxmedval]</code>
Options	<ul style="list-style-type: none">• <code>time</code>—Maximum delay for best path calculation in seconds (0 to 3600).

- *maxmedval*—Maximum delay for the first BGP peer to reach Established status (1-3600; default is 0).

Modes

Usage

This command is used to enable read-only mode on BGP process restart or when BGP process is cleared using `clear ip bgp`. Read-only mode begins when the first peer reaches the established status, and a timer for max-delay seconds is started. During this mode, BGP does not run any best-path or generate any updates to its peers. This mode continues until all the configured peers (except the shutdown peers) have sent an explicit EOR (End-Of-RIB) or an implicit-EOR. The first keep-alive established after BGP has reached is considered an implicit-EOR. If the establish-wait optional value is given, BGP waits for peers to reach established from the beginning of the update-delay until the establish-wait period is over (the minimum set of established peers for which EOR is expected would be peers established during the establish-wait window), not necessarily all the configured neighbors and max-delay period is over. On encountering any of the above two conditions, BGP resumes the decision process and generates updates to its peers. The default maximum delay is 0 (the feature is off by default). When configuring both delay timers, the maximum delay time for the best path calculation should be configured longer than the delay timer for the first BGP peer to reach establishment.

Examples

```
sonic(config)# router bgp 65300
sonic(config-router-bgp)# update-delay 120 60

sonic(config-router-bgp)# no update-delay
```

Releases

3.0 or later

update-source

Specifies the IPv4 or IPv6 source address to use for the BGP session or peer-group.

Command

`update-source {ip | {interface {Ethernet | PortChannel | Vlan | Loopback}}}`

Options

- *ip*—IPv4 or IPv6 address in A.B.C.D or A::B format
- *interface*—Interface type

Modes

- BGP-NEIGHBOR
- BGP-PEER-GROUP

Usage

Use this command to configure the source interface for a BGP neighbor session or peer-group. The source address may be specified as either an IPv4/IPv6 address directly or as an interface name. The interface name could be router port, PortChannel, Loopback, or VLAN interface configure with IPv4/IPv6 address.

Examples

```
sonic(config)# router bgp 100
sonic(config-router-bgp)# neighbor 30.30.30.3
sonic(config-router-bgp-neighbor)# update-source 10.0.0.1

sonic(config)# router bgp 100
sonic(config-router-bgp)# peer-group PG_Ext
sonic(config-router-bgp-pg)# update-source interface Eth1/16

sonic(config-router-bgp-neighbor)# no update-source 10.0.0.1
sonic(config-router-bgp-pg)# no update-source interface Eth1/16
```

Releases

3.0 or later

usb enable

Enable auto-detection of a USB storage device.

Command	usb enable
Options	None
Modes	CONFIGURATION
Usage	Use the <code>usb enable</code> command to enable the auto-detection of USB media and automatically mount all USB partitions which have a supported file system. To disable USB auto-detection and unmount all USB partitions, enter the <code>no usb enable</code> command.
Example	<pre>sonic# configure terminal sonic(config)# usb enable</pre>
Releases	4.2.0 or later

usb mount

Mount USB partitions

Command	usb {mount un-mount}
Options	<ul style="list-style-type: none">• <code>mount</code>—Mount all available USB partitions• <code>un-mount</code>—Un-mount all available USB partitions
Modes	EXEC
Usage	Use the <code>usb mount</code> command to manually mount all available USB partitions with a supported file system to the corresponding mount points in the <code>/media</code> directory. To unmount all USB mount points, enter the <code>usb un-mount</code> command.
Note	<p>(i) NOTE: You must first enter the <code>usb enable</code> command before you can mount USB partitions using the <code>usb mount</code> command.</p>
Example	<pre>sonic# usb mount</pre>
Releases	4.2.0 or later

username password role

Adds a user.

Command	username <i>username</i> password <i>passwd</i> role <i>role</i>
Options	<ul style="list-style-type: none">• <code>username</code>—Enter a text string (up to 32 alphanumeric characters; minimum is one character). Username must be in UTF-8 characters.• <code>passwd</code>—Enter a text string (up to 32 alphanumeric characters; minimum is one character)• <code>role</code>—Enter a user role:<ul style="list-style-type: none">◦ <code>admin</code>—Full access to all commands in the system, exclusive access to commands that change the file system, and access to the system shell. An administrator can create user IDs and assign roles.◦ <code>operator</code>—Access to EXEC mode to view the current configuration. An operator cannot modify configuration settings on a switch.◦ <code>secadmin</code>—Access to all security-related commands in the system. A <code>secadmin</code> user can view, change, and run commands specific to security features. Also the user is allowed to access system-level information.

- `netadmin`—Access to the configuration commands that manage traffic flowing through the switch.

Modes

CONFIGURATION

Usage

To create, delete, and modify user roles, you must log in with the `admin` role.

i **NOTE:** During an Enterprise SONiC upgrade/downgrade, locally configured users and their passwords/roles are properly migrated when installing a SONiC image using the `image install` command. The configuration migration scripts automatically migrate the `config_db.json`, `/etc/passwd`, `/etc/group`, `/etc/shadow`, `/etc/gshadow`, `/home/*`, and `/etc/sonic/cert/` directories, and `/var/spool/mail` files. However, if you reinstall Enterprise SONiC from ONIE, and manually migrate a configuration from one switch to another by copying and restoring a `config_db.json` file or by provisioning Enterprise SONiC using custom ZTP scripts, you must do one of the following:

- Manually reconfigure the local users using the `username password role` command or programmatic interfaces.
- Restore the `/etc/passwd`, `/etc/shadow`, and `/etc/group` files in addition to the `config_db.json` file. Remotely authenticated users whose credentials are authenticated by RADIUS, TACACS+, or LDAP are not affected.

i **NOTE:** When you run the `username password role` command on the switch, the configuration is directly written into the kernel. As a result, the `write memory` command is not required to keep it after a reboot.

i **NOTE:** When upgrading Enterprise SONiC from any older version to 4.4.1, ensure that all existing usernames for switch access are in UTF-8 format. To change the existing non-UTF-8-formatted usernames to UTF-formatted usernames, follow these steps in the legacy SONiC CLI:

- Use the `sudo cat /etc/passwd` command to view the list of existing usernames.
- If any usernames are not in UTF-8 format, delete them using the `sudo userdel <username>` command.
- When copying and pasting usernames, ensure that the names are in UTF-8 format.

If an existing username is not in the UTF-8 format, do not use the MF-CLI until you change the formatting of the username.

Examples

```
sonic(config)# username tango password charlie role operator
sonic(config)# username tangol password charlie2 role secadmin,operator
sonic(config)# no username tango
```

Releases

3.0 or later

use-v2-checksum

Configures checksum capability for a VRRP instance.

Command `use-v2-checksum`

Options None

Modes CONFIGURATION

Usage Use this command to enable compatibility with third-party network devices which uses v2 checksum for VRRPv3.

Examples

```
sonic(config-if-Eth1/4)# vrrp 1 address-family ipv4  
sonic(config-if-Eth1/4-vrrp-ipv4-1)# use-v2-checksum
```

```
sonic(config-if-Eth1/4-vrrp-ipv4-1)# no use-v2-checksum
```

Releases

3.1 or later

v6only

Enables BGP with v6 link-local only.

Command v6only**Options** None**Modes** BGP-NEIGHBOR**Usage** Use this command to enable BGP session with only v6 link-local on an interface neighbor.**Example**

```
sonic# configure terminal  
sonic(config)# router bgp 100  
sonic(config-router-bgp)# neighbor interface Ethernet 0  
sonic(config-router-bgp-neighbor)# v6only
```

```
sonic(config-router-bgp-neighbor)# no v6only
```

Releases

4.0 or later

version

Configures version 2 or 3.

Command version ver**Options** ver—Version (default is 2)**Modes** VRRP**Usage** Use this command to configure the VRRP version.**Examples**

```
sonic(config-if-Ethernet4)# vrrp 1 address-family ipv4  
sonic(config-if-Ethernet4-vrrp-ipv4-1)# version 3
```

```
sonic(config-if-Ethernet4-vrrp-ipv4-1)# no version
```

Releases

3.1 or later

vip

Configures a virtual IP address for an IPv4 or IPv6 VRRP instance.

Command vip *vip_addr***Options** *vip_addr*—IP address in A.B.C.D or A::B format**Modes** VRRP**Usage** Use this command to configure a virtual IP address for an IPv4 or IPv6 VRRP instance.

Examples

```
sonic(config-if-Eth1/4)# vrrp 1 address-family ipv4  
sonic(config-if-Eth1/4-vrrp-ipv4-1)# vip 10.0.0.5
```

```
sonic(config-if-Eth1/4)# vrrp 1 address-family ipv6  
sonic(config-if-Eth1/4-vrrp-ipv6-1)# vip 2001::5
```

```
sonic(config-if-Eth1/4-vrrp-ipv4-1)# no vip
```

```
sonic(config-if-Eth1/4-vrrp-ipv6-1)# no vip
```

Releases

3.1 or later

vlan-stacking

Enables VLAN stacking on Z9432F-ON and S5448F-ON switches.

Command `vlan-stacking`

Options None

Mode SWITCH-RESOURCE

Usage By default, VLAN stacking features are not enabled on Z9432F-ON and S5448F-ON switches. You must enable this feature from the switch-resource command tree before you can configure Q-in-Q VLAN tunneling and VLAN translation. Then save the configuration and reload the switch. To disable VLAN stacking on the specified switches, enter the `no vlan-stacking` command. Then save and reload the switch.

Example To enable VLAN stacking:

```
sonic(config)# switch-resource  
sonic(config-switch-resource)# vlan-stacking  
Config save and reboot is required for this change to take effect  
sonic(config-switch-resource)# exit  
sonic# write memory  
sonic# reload
```

After reboot:

```
sonic# show switch-resource vlan-stacking  
Configured : enabled  
Operational : enabled
```

To disable VLAN stacking:

```
sonic(config)# switch-resource  
sonic(config-switch-resource)# no vlan-stacking  
Config save and reboot is required for this change to take effect  
sonic(config-switch-resource)# exit  
sonic# write memory  
sonic# reload
```

After reboot:

```
sonic# show switch-resource vlan-stacking  
Configured : disabled  
Operational : disabled
```

Releases

4.1.0 or later

vni

Enables configuration of per-VNI EVPN parameters.

Command	vni <i>vnum</i>
Options	<i>vnum</i> —Specify the VNI number.
Modes	ROUTER-BGP
Usage	Use this command to enter per-VNI configuration mode for L2 VNIs and configure manual route targets and manual route distinguisher.

Examples	<pre>sonic(config-router-bgp) # address-family l2vpn evpn sonic(config-router-bgp-af) # vni 100 sonic(config-router-bgp-af-vni) #</pre>
	<pre>sonic(config-router-bgp-af) # no vni 100</pre>

Releases	3.0 or later
-----------------	--------------

vni-downstream

Enables or disables the downstream VNI configuration.

Command	vni-downstream { <i>remoteip</i> external}
Options	<i>remoteip</i> —Remote IP address in A.B.C.D format.
Modes	INTERFACE
Usage	Use this command if a remote site border leaf has different VNI assignment in multisite configurations. Use external option to enable downstream VNI for all remote sites. This command is applicable only for VXLAN interfaces.

Examples	<pre>sonic(config) # interface vxlan vtep1 sonic(config-if-vxlan-vtep1) # vni-downstream 1.1.1.2 sonic(config-if-vxlan-vtep1) # vni-downstream external</pre>
	<pre>sonic(config) # interface vxlan vtep1 sonic(config-if-vxlan-vtep1) # no vni-downstream 1.1.1.2 sonic(config-if-vxlan-vtep1) # no vni-downstream external</pre>

Releases	4.0 or later
-----------------	--------------

voice

Configure the voice application type and its attributes.

Command	voice vlan { <i>vlan-id</i> [untagged] dot1p] [[cos <i>cos-val</i>] [dscp <i>dscp-val</i>]]
Options	<ul style="list-style-type: none">• <i>vlan-id</i>—VLAN ID (1 to 4094)• <i>cos-val</i>—(Optional) Cost value (0 to 7)• <i>dscp-val</i>—(Optional) DSCP value (0 to 63)
Modes	NETWORK POLICY
Usage	Use this command to configure voice VLAN with tagging, cost, and DSCP values.

Examples

```
sonic(config) # network-policy profile 1  
sonic(config-network-policy-1)# voice vlan 100 cos 4 dscp 20  
  
sonic(config-network-policy-1)# no voice vlan 100 cos 4 dscp 20
```

Releases

4.0 or later

voice-signaling

Configure the voice-signaling application type and its attributes.

Command

```
voice-signaling vlan {vlan-id [untagged] | dot1p} [[cos cos-val] [dscp dscp-val]]
```

Options

- *vlan-id*—VLAN ID (1 to 4094)
- *cos-val*—Cost value (0 to 7)
- *dscp-val*—DSCP value (0 to 63)

Modes

NETWORK POLICY

Usage

Use this command to configure a voice-signaling VLAN with tagging, cost, and DSCP values.

Examples

```
sonic(config) # network-policy profile 1  
sonic(config-network-policy-1)# voice-signaling vlan dot1p cos 3 dscp 10  
  
sonic(config-network-policy-1)# no voice-signaling vlan dot1p cos 3 dscp 10
```

Releases

4.0 or later

vrrp

Configures virtual router redundancy protocol (VRRP).

Command

```
vrrp vrrp-id address-family {ipv4 | ipv6}
```

Options

- *vrrp-id*—VRRP ID (1 to 255)
- *address-family*—Address-family name

Modes

INTERFACE

Usage

Use this command to configure VRRP on an Ethernet, PortChannel, or VLAN interface.

Examples

```
sonic(config-if-Ethernet4)# vrrp 1 address-family ipv4  
sonic(config-if-Ethernet4-vrrp-ipv4-1)#  
  
sonic(config-if-Ethernet4)# vrrp 1 address-family ipv6  
sonic(config-if-Ethernet4-vrrp-ipv6-1)#  
  
sonic(config-if-Ethernet4)# no vrrp 1 address-family ipv4  
  
sonic(config-if-Ethernet4)# no vrrp 1 address-family ipv6
```

Releases

3.1 or later

warm-reboot

Initiates warm reboot on the switch.

Command	warm-reboot
Options	None
Modes	EXEC
Usage	Use the <code>warm-reboot</code> command to perform a warm reboot on Enterprise SONiC software during maintenance or upgrade without impacting the data plane.
Examples	<pre>sonic# warm-reboot warm-reboot in process</pre>
Releases	4.2.0 or later

warm-restart bgp

Configures the timer value for warm restart of the BGP service.

Command	<code>warm-restart bgp timer value</code>
Options	<code>timer value</code> —Timer value in seconds (1 to 3600; default is 120).
Modes	CONFIGURATION
Usage	Use the <code>warm-restart bgp timer</code> command to configure the timer value for a warm restart of the BGP service. The software performs reconciliation after this timer expires and removes stale entries. In scaled configurations, set this value to a higher number matching with the BGP graceful restart timer. (i) NOTE: You must enter the full command syntax because it is a hidden command.
Examples	<pre>sonic(config)# warm-restart bgp timer 60 sonic(config)# no warm-restart bgp timer</pre>
Releases	4.2.0 or later

watermark interval

Configures the snapshot watermark interval.

Command	<code>watermark interval interval_value</code>
Options	<code>interval_value</code> —Interval value (1 to 600)
Modes	CONFIGURATION
Usage	Use this command to configure the interval at which counter data is retrieved from the hardware and stored into the counter database.
Examples	<pre>sonic(config)# watermark interval 77 sonic(config)# no watermark interval</pre>
Releases	3.1 or later

watermark telemetry

Configures the watermark telemetry interval.

Command	<code>watermark telemetry <i>interval_value</i></code>
Options	<code><i>interval_value</i></code> —Interval value (1 to 600)
Modes	CONFIGURATION
Usage	Use this command to configure the interval at which samples are taken from a telemetry data source.
Examples	<pre>sonic(config)# watermark telemetry interval 88</pre> <pre>sonic(config)# no watermark telemetry interval</pre>
Releases	3.1 or later

weight

Assigns a default weight to BGP routes received from neighbor interfaces.

Command	<code>weight <i>val</i></code>
Options	<code><i>val</i></code> — Weight value for routes (1 to 4294967295; default 0)
Modes	ROUTER-BGP
Usage	Use this command to assign a default weight to BGP routes received from this neighbor, or neighbors in a peer-group. Weight parameter is used in BGP route selection process. Configuring weight may influence the outcome of the route selection process.
Examples	<pre>sonic(config-router-bgp)# neighbor 20.20.20.2</pre> <pre>sonic(config-router-bgp-neighbor)# remote-as 300</pre> <pre>sonic(config-router-bgp-neighbor)# address-family ipv4 unicast</pre> <pre>sonic(config-router-bgp-neighbor-af)# weight 4096</pre> <pre>sonic(config-router-bgp-neighbor-af)# no weight</pre>
Releases	3.0 or later

write memory

Saves the current running configuration to the startup configuration file.

Command	<code>write memory</code>
Options	None
Modes	EXEC
Usage	By default, any configuration changes are not automatically saved to the startup configuration. Dell Technologies recommends that you save the configuration changes using the <code>write memory</code> command.
Example	<pre>sonic# write memory</pre>
Releases	3.0 or later

write erase

Erases the existing switch configuration files except the Management interface configuration.

Command	write erase
Options	None
Modes	EXEC
Usage	Use this command to delete the startup configuration JSON file and all application configuration files in the /etc/sonic directory. The Management interface configuration in the startup configuration file is retained so that you can access the switch using the same management address after the switch reboot. For this command to take effect, you must reboot the switch after issuing this command. Use no write erase command to cancel the configuration erase operation.

Examples	<pre>sonic# write erase Existing switch configuration files except management interface configuration will be removed, continue? [y/N]:</pre>
	<pre>sonic# no write erase Switch configuration erase operation will be cancelled, continue? [y/N]:</pre>

Releases	3.0 or later
-----------------	--------------

write erase boot

Erases the configuration files including the Management interface configuration.

Command	write erase boot
Options	None
Modes	CONFIGURATION
Usage	Use this command to delete the startup configuration JSON file, and all application configuration files in the /etc/sonic directory. The Management interface configuration in the startup configuration JSON file is also removed. The SONiC switch boots with a factory default configuration file.
Example	<pre>sonic# write erase boot Existing switch configuration files will be removed, continue? [y/N]:</pre>

Releases	3.0 or later
-----------------	--------------

write erase install

Restores all SONiC switch content to default values, and removes all changes made by the user.

Command	write erase install
Options	None
Modes	CONFIGURATION
Usage	All user installed packages and file changes are removed. It also deletes the startup configuration JSON file and the files in the /etc/sonic directory. The SONiC switch is reverted to the same state as a newly installed image. After the SONiC switch is rebooted, if the ZTP is enabled, the switch starts to discover and download the switch configuration.
Example	<pre>sonic(config)# write erase install All SONiC switch content will be restored to default values, continue? [y/N]:</pre>

Releases	3.0 or later
-----------------	--------------

write-multiplier

Configures the maximum interface write multiplier.

Command	<code>write-multiplier maxinterfacewrite</code>
Options	<code>maxinterfacewrite</code> —Maximum interface write value (1 to 100; default is 20)
Modes	ROUTER-OSPF
Usage	Use this command to tune the amount of work that is done in the packet read and write threads before relinquishing control. The parameter is the number of packets to process before returning. The default value of this parameter is 20.

Examples	<pre>sonic(config) # router ospf sonic(config-router-ospf) # write-multiplier 10</pre>
	<pre>sonic(config-router-ospf) # no write-multiplier</pre>

Releases	3.1 or later
-----------------	--------------

write-quanta

Configures the maximum number of BGP packets to write to, peer socket, in one I/O cycle.

Command	<code>write-quanta wrval</code>
Options	<code>wrval</code> —Write value (1 to 64; default is 64)
Modes	ROUTER-BGP
Usage	The BGP message transmission I/O is vectored which means that multiple packets are written to the peer socket simultaneously on each I/O cycle to minimize system call overhead. This value controls how many are written at a time. Under certain load conditions, reducing this value could make peer traffic less bursty. It is recommended to leave this setting as the default (64).

Examples	<pre>sonic(config) # router bgp 65300 sonic(config-router-bgp) # write-quanta 50</pre>
	<pre>sonic(config) # router bgp 65300 sonic(config-router-bgp) # no write-quanta</pre>

Releases	3.0 or later
-----------------	--------------

ztp enable

Administratively enables or disables zero-touch provisioning (ZTP).

Command	<code>ztp enable</code>
Options	None
Modes	CONFIGURATION
Usage	ZTP is enabled by default when you boot a switch with a factory-installed Enterprise SONiC for the first time, or when you perform an ONIE: OS Install from the ONIE boot menu. To exit ZTP operation and manually configure a switch by entering CLI commands, stop the ZTP process with <code>no ztp enable</code> .

To enable ZTP again, enter `ztp enable` and reboot the switch. When you enable ZTP again, the ZTP process does not start until you reboot the switch.

Examples

```
sonic(config)# ztp enable
```

```
sonic(config)# no ztp enable
```

Releases

3.0 or later