

OS10 Enterprise Edition User Guide

Release 10.4.1.0

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.

Chapter 1: Getting Started.....	20
Supported Hardware.....	20
Download OS10 image and license.....	20
Installation using ONIE.....	22
Automatic installation.....	22
Manual installation.....	23
Log into OS10.....	24
Install OS10 license.....	25
Zero-touch deployment.....	26
ZTD DHCP server configuration.....	28
ZTD provisioning script.....	28
ZTD CLI batch file.....	29
Post-ZTD script.....	29
ZTD commands.....	30
Remote access.....	31
Configure Management IP address.....	32
Management Route Configuration.....	32
Configure user name and password.....	33
Upgrade OS10.....	33
CLI Basics.....	33
CLI command categories.....	35
CONFIGURATION Mode.....	35
Command help.....	35
Check device status.....	37
Candidate configuration.....	39
Change to transaction-based configuration.....	42
Copy running configuration	42
Restore startup configuration	43
Reload system image.....	43
Filter show commands.....	44
Alias command.....	44
Batch mode.....	48
Linux shell commands.....	48
SSH commands.....	49
OS9 environment commands.....	50
Common commands.....	50
alias.....	50
alias (multi-line).....	51
batch.....	52
boot.....	52
commit.....	53
configure.....	53
copy.....	53
default (alias).....	54
delete.....	55

description (alias).....	55
dir.....	56
discard.....	56
do.....	57
feature config-os9-style.....	57
exit.....	57
license.....	58
line (alias).....	58
lock.....	59
management route.....	59
move.....	60
no.....	60
reload.....	60
show alias.....	61
show boot.....	62
show candidate-configuration.....	62
show environment.....	64
show inventory.....	65
show ip management-route.....	65
show ipv6 management-route.....	66
show license status.....	66
show running-configuration.....	67
show startup-configuration.....	69
show system.....	70
show version.....	72
start.....	72
system.....	72
system identifier.....	73
terminal.....	73
traceroute.....	73
unlock.....	75
write.....	75

Chapter 2: Interfaces..... 76

Ethernet interfaces.....	76
Unified port groups.....	76
L2 mode configuration.....	77
L3 mode configuration.....	78
Fibre Channel interfaces.....	79
Management interface	80
VLAN interfaces.....	81
User-configured default VLAN.....	81
VLAN scale profile.....	82
Loopback interfaces.....	82
Port-channel interfaces.....	83
Create port-channel.....	83
Add port member.....	83
Minimum links.....	84
Assign Port Channel IP Address.....	84
Remove or disable port-channel.....	85

Load balance traffic.....	85
Change hash algorithm.....	85
Configure interface ranges.....	86
Switch-port profiles.....	87
S4148-ON series port profiles.....	87
S4148U-ON port profiles.....	88
Configure breakout mode.....	89
Breakout auto-configuration.....	90
Forward error correction.....	90
Energy-efficient Ethernet.....	91
Enable energy-efficient Ethernet.....	92
Clear interface counters.....	92
View EEE status/statistics.....	92
EEE commands.....	93
View interface configuration.....	96
Interface commands.....	98
channel-group.....	98
default vlan-id.....	98
description (Interface).....	99
duplex.....	99
feature auto-breakout.....	100
fec.....	100
interface breakout.....	100
interface ethernet.....	101
interface loopback.....	101
interface mgmt.....	101
interface null.....	102
interface port-channel.....	102
interface range.....	102
interface vlan.....	103
link-bundle-utilization.....	103
mode.....	104
mode l3.....	105
mtu.....	105
port-group.....	105
scale-profile vlan.....	106
show discovered-expanders.....	106
show interface.....	106
show inventory media.....	108
show link-bundle-utilization.....	108
show port-channel summary.....	109
show port-group.....	109
show switch-operating-mode.....	110
show switch-port-profile.....	110
show unit-provision.....	111
show vlan.....	111
shutdown.....	111
speed (Fibre Channel).....	112
speed (Management).....	112
switch-port-profile.....	113

switchport access vlan.....	114
switchport mode.....	115
switchport trunk allowed vlan.....	115
unit-provision.....	116
Chapter 3: Fibre Channel.....	117
Terminology.....	118
Virtual fabric.....	118
Fibre Channel zoning.....	121
F_Port on Ethernet.....	122
F_Port commands.....	122
fc alias.....	123
fc zone.....	123
fc zoneset.....	123
feature fc.....	124
member (alias).....	124
member (zone).....	124
member (zoneset).....	125
show fc alias.....	125
show fc interface-area-id mapping.....	125
show fc ns switch.....	126
show fc zone.....	127
show fc zoneset.....	127
zone default-zone permit.....	129
zoneset activate.....	129
NPG commands.....	129
fc port-mode F.....	129
feature fc npg.....	130
show npg devices.....	130
F_Port and NPG commands.....	131
clear fc statistics.....	131
fcoe	132
name.....	132
show fc statistics.....	133
show fc switch.....	133
show running-config vfabric.....	134
show vfabric.....	134
vfabric.....	135
vfabric (interface).....	135
vlan.....	136
FIP-snooping commands.....	136
feature fip-snooping.....	136
fip-snooping enable.....	136
fip-snooping fc-map.....	137
fip-snooping port-mode fcf	137
FCoE commands.....	137
clear fcoe database.....	138
clear fcoe statistics.....	138
fcoe max-sessions-per-enodemac.....	138
fcoe priority-bits.....	139

lldp tlv-select dcbxp-appln fcoe.....	139
show fcoe enode.....	139
show fcoe fcf.....	140
show fcoe sessions.....	140
show fcoe statistics.....	141
show fcoe system.....	141
show fcoe vlan.....	142
Chapter 4: Layer 2.....	143
802.1X.....	143
Port authentication.....	144
EAP over RADIUS.....	145
Configure 802.1X.....	145
Enable 802.1X.....	146
Identity retransmissions.....	147
Failure quiet period.....	147
Port control mode.....	148
Reauthenticate port.....	149
Configure timeouts.....	150
802.1X commands.....	151
Link Aggregation Control Protocol.....	155
Modes.....	156
Configuration.....	156
Interfaces.....	157
Rates.....	157
Sample configuration.....	158
LACP fallback.....	161
LACP commands.....	163
Link Layer Discovery Protocol.....	170
Optional TLVs.....	171
Organizationally-specific TLVs.....	171
Media endpoint discovery.....	172
Network connectivity device.....	172
LLDP-MED capabilities TLV.....	173
Network policies TLVs.....	173
Define network policies.....	174
Packet timer values.....	174
Disable and re-enable LLDP.....	175
Disable and re-enable LLDP on management ports.....	176
Advertise TLVs.....	176
Network policy advertisement.....	177
Fast start repeat count.....	177
View LLDP configuration.....	178
Adjacent agent advertisements.....	179
Time to live.....	180
LLDP commands.....	181
Media Access Control.....	192
Static MAC Address.....	192
MAC Address Table.....	192
Clear MAC Address Table.....	193

MAC Commands.....	193
Multiple Spanning-Tree Protocol.....	196
Configure MSTP.....	196
Create instances.....	197
Root selection.....	198
Non-Dell hardware.....	199
Region name or revision.....	199
Modify parameters.....	199
Interface parameters.....	200
Forward traffic.....	201
Spanning-tree extensions.....	201
MST commands.....	204
Rapid per-VLAN spanning-tree plus.....	212
Load balance and root selection.....	213
Enable RPVST+.....	213
Select root bridge.....	214
Root assignment.....	215
Loop guard.....	216
Global parameters.....	216
RPVST+ commands.....	217
Rapid Spanning-Tree Protocol.....	224
Enable globally.....	224
Global parameters.....	226
Interface parameters.....	227
Root bridge selection.....	227
EdgePort forward traffic.....	228
Spanning-tree extensions.....	228
RSTP commands.....	230
Virtual LANs.....	236
Default VLAN.....	236
Create or remove VLANs.....	237
Access mode.....	238
Trunk mode.....	239
Assign IP address.....	239
View VLAN configuration.....	240
VLAN commands.....	241
Port monitoring.....	243
Local port monitoring.....	243
Remote port monitoring.....	244
Encapsulated remote port monitoring.....	246
Flow-based monitoring.....	247
Remote port monitoring on VLT.....	247
Port monitoring commands.....	249
Chapter 5: Layer 3.....	254
Virtual routing and forwarding.....	254
Configure management VRF.....	254
Configure non-default VRF instances.....	256
Sample VRF configuration.....	258
View VRF instance information.....	262

VRF commands.....	263
Bidirectional Forwarding Detection.....	268
BFD session states.....	268
BFD three-way handshake.....	269
BFD configuration.....	270
Configure BFD globally.....	270
BFD for BGP.....	271
BFD commands.....	275
Border Gateway Protocol.....	278
Sessions and peers.....	279
Route reflectors.....	280
Multiprotocol BGP.....	280
Attributes.....	281
Selection criteria.....	281
Weight and local preference.....	282
Multiexit discriminators.....	282
Origin.....	283
AS path and next-hop.....	283
Best path selection.....	283
More path support.....	284
Advertise cost.....	284
4-Byte AS numbers.....	284
AS number migration.....	285
Configure Border Gateway Protocol.....	285
Enable BGP.....	286
Configure Dual Stack.....	288
Peer templates.....	289
Neighbor fall-over.....	291
Configure password.....	293
Fast external fallover.....	294
Passive peering.....	296
Local AS.....	296
AS number limit.....	297
Redistribute routes.....	298
Additional paths.....	299
MED attributes.....	299
Local preference attribute.....	299
Weight attribute.....	300
Enable multipath.....	301
Route-map filters.....	301
Route reflector clusters.....	302
Aggregate routes.....	302
Confederations.....	303
Route dampening.....	304
Timers.....	305
Neighbor soft-reconfiguration.....	305
BGP commands.....	306
Equal cost multi-path.....	336
Load balancing.....	336
ECMP commands.....	337

IPv4 routing.....	339
Assign interface IP address.....	339
Configure static routing.....	340
Address Resolution Protocol.....	341
IPv4 routing commands.....	341
IPv6 routing.....	345
Enable or disable IPv6.....	346
IPv6 addresses.....	346
Stateless autoconfiguration.....	348
Neighbor Discovery.....	348
Duplicate address discovery.....	350
Static IPv6 routing.....	350
IPv6 destination unreachable.....	351
IPv6 hop-by-hop options.....	351
View IPv6 information.....	351
IPv6 commands.....	352
Internet Group Management Protocol.....	363
IGMP snooping.....	363
IGMP snooping commands.....	364
Multicast Listener Discovery Protocol.....	372
MLD snooping.....	372
MLD snooping commands.....	374
Open shortest path first.....	380
Autonomous system areas.....	380
Areas, networks, and neighbors.....	381
Router types.....	381
Designated and backup designated routers.....	382
Link-state advertisements.....	383
Router priority.....	383
Shortest path first throttling.....	384
OSPFv2.....	385
OSPFv3.....	415
Object tracking manager.....	434
Interface tracking.....	435
Host tracking.....	436
Set tracking delays.....	437
Object tracking.....	437
View tracked objects.....	437
OTM commands.....	438
Policy-based routing.....	441
Access-list to match route-map.....	441
Set address to match route-map.....	441
Assign route-map to interface.....	442
View PBR information.....	442
PBR commands.....	443
Virtual Router Redundancy Protocol.....	445
Configuration.....	446
Create virtual router.....	446
Group version.....	447
Virtual IP addresses.....	447

Configure virtual IP address.....	448
Set group priority.....	449
Authentication.....	449
Disable preempt.....	450
Advertisement interval.....	451
Interface/object tracking.....	451
Configure tracking.....	452
VRRP commands.....	453
Chapter 6: UFT modes.....	458
Configure UFT modes.....	458
IPv6 extended prefix routes.....	459
UFT commands.....	460
hardware forwarding-table mode.....	460
hardware l3 ipv6-extended-prefix	460
show hardware forwarding-table mode.....	460
show hardware forwarding-table mode all.....	461
show hardware l3.....	461
Chapter 7: System management.....	462
Dynamic Host Configuration Protocol.....	462
Packet format and options.....	462
DHCP server.....	463
Automatic address allocation.....	464
Hostname resolution.....	465
Manual binding entries.....	466
DHCP relay agent.....	467
View DHCP Information.....	468
System domain name and list.....	468
DHCP commands.....	469
DNS commands.....	474
DHCP Limitations.....	476
Network Time Protocol.....	477
Enable NTP.....	478
Broadcasts.....	478
Source IP address.....	479
Authentication.....	479
NTP commands.....	480
System clock.....	485
System Clock commands.....	485
System banners.....	486
Login banner.....	486
MOTD banner.....	487
System banner commands.....	487
User session management.....	488
User session management commands.....	489
Telnet server.....	490
Telnet commands.....	490
Security.....	491

User re-authentication.....	492
Password strength.....	492
Role-based access control.....	493
Assign user role.....	493
RADIUS authentication.....	493
TACACS+ authentication.....	494
TACACS+ unknown or missing user role.....	495
SSH server.....	495
Virtual terminal line.....	496
Enable AAA accounting.....	497
Enable user lockout.....	497
Limit concurrent login sessions.....	498
Enable login statistics.....	498
Security commands.....	499
Simple Network Management Protocol.....	515
SNMP commands.....	515
Uplink Failure Detection.....	518
Configure uplink failure detection.....	519
UFD commands.....	521
OS10 image upgrade.....	525
Boot system partition.....	526
Upgrade commands.....	527
Chapter 8: OpenFlow.....	531
OpenFlow logical switch instance.....	532
OpenFlow controller.....	532
OpenFlow version 1.3.....	532
Ports.....	532
Flow table.....	532
Group table.....	533
Meter table.....	533
Instructions.....	533
Action set.....	533
Action types.....	534
Counters.....	534
OpenFlow protocol.....	536
OpenFlow use cases.....	548
Configure OpenFlow.....	548
Establish TLS connection.....	549
OpenFlow commands.....	550
controller.....	550
dpid-mac-address.....	551
in-band-mgmt.....	551
max-backoff.....	552
mode openflow-only.....	552
openflow.....	552
probe-interval.....	553
protocol-version.....	553
rate-limit packet_in.....	554
show openflow.....	555

show openflow flows.....	555
show openflow ports.....	556
show openflow switch.....	557
show openflow switch controllers.....	558
switch.....	559
OpenFlow-only mode commands.....	559

Chapter 9: Access Control Lists..... 562

IP ACLs.....	562
MAC ACLs.....	563
Control-plane ACLs.....	563
Control-plane ACL qualifiers.....	563
IP fragment handling.....	564
L3 ACL rules.....	565
Assign sequence number to filter.....	565
L2 and L3 ACLs.....	566
Assign and apply ACL filters.....	567
Ingress ACL filters.....	567
Egress ACL filters.....	568
Clear access-list counters.....	569
IP prefix-lists.....	569
Route-maps.....	569
Match routes.....	571
Set conditions.....	571
continue Clause.....	572
ACL flow-based monitoring.....	572
Enable flow-based monitoring.....	573
ACL commands.....	574
clear ip access-list counters.....	574
clear ipv6 access-list counters.....	574
clear mac access-list counters.....	574
deny.....	575
deny (IPv6).....	575
deny (MAC).....	576
deny icmp.....	577
deny icmp (IPv6).....	577
deny ip.....	578
deny ipv6.....	578
deny tcp.....	579
deny tcp (IPv6).....	579
deny udp.....	580
deny udp (IPv6).....	581
description.....	581
ip access-group.....	582
ip access-list.....	582
ip as-path access-list.....	582
ip community-list standard deny.....	583
ip community-list standard permit.....	583
ip extcommunity-list standard deny.....	584
ip extcommunity-list standard permit.....	584

ip prefix-list description.....	585
ip prefix-list deny.....	585
ip prefix-list permit.....	585
ip prefix-list seq deny.....	586
ip prefix-list seq permit.....	586
ipv6 access-group.....	587
ipv6 access-list.....	587
ipv6 prefix-list deny.....	587
ipv6 prefix-list description.....	588
ipv6 prefix-list permit.....	588
ipv6 prefix-list seq deny.....	589
ipv6 prefix-list seq permit.....	589
mac access-group.....	589
mac access-list.....	590
permit.....	590
permit (IPv6).....	591
permit (MAC).....	591
permit icmp.....	592
permit icmp (IPv6).....	592
permit ip.....	593
permit ipv6.....	593
permit tcp.....	594
permit tcp (IPv6).....	595
permit udp.....	595
permit udp (IPv6).....	596
remark.....	597
seq deny.....	597
seq deny (IPv6).....	598
seq deny (MAC).....	598
seq deny icmp.....	599
seq deny icmp (IPv6).....	599
seq deny ip.....	600
seq deny ipv6.....	600
seq deny tcp.....	601
seq deny tcp (IPv6).....	602
seq deny udp.....	602
seq deny udp (IPv6).....	603
seq permit.....	604
seq permit (IPv6).....	604
seq permit (MAC).....	605
seq permit icmp.....	606
seq permit icmp (IPv6).....	606
seq permit ip.....	607
seq permit ipv6.....	607
seq permit tcp.....	608
seq permit tcp (IPv6).....	608
seq permit udp.....	609
seq permit udp (IPv6).....	610
show access-group.....	611
show access-lists.....	611

show ip as-path-access-list	613
show ip community-list.....	613
show ip extcommunity-list.....	614
show ip prefix-list.....	614
Route-map commands.....	615
continue.....	615
match as-path.....	615
match community.....	615
match extcommunity.....	616
match interface.....	616
match ip address.....	616
match ip next-hop.....	617
match ipv6 address.....	617
match ipv6 next-hop.....	617
match metric.....	618
match origin.....	618
match route-type.....	618
match tag.....	619
route-map.....	619
set comm-list add.....	620
set comm-list delete.....	620
set community.....	620
set extcomm-list add.....	621
set extcomm-list delete.....	621
set extcommunity.....	621
set local-preference.....	622
set metric.....	622
set metric-type.....	623
set next-hop.....	623
set origin.....	624
set tag.....	624
set weight.....	624
show route-map.....	625
Chapter 10: Quality of service.....	626
Configure quality of service.....	626
Ingress traffic classification.....	628
Data traffic classification.....	628
Control-plane policing.....	633
Egress traffic classification.....	636
Policing traffic.....	637
Mark Traffic.....	637
Color traffic.....	638
Modify packet fields.....	638
Shaping traffic.....	638
Bandwidth allocation.....	639
Strict priority queuing.....	640
Buffer management.....	641
Configure ingress buffer.....	641
Configure egress buffer.....	642

Congestion avoidance.....	643
Storm control.....	645
RoCE for faster access and lossless connectivity.....	645
Configure RoCE on the switch.....	645
QoS commands.....	647
bandwidth.....	647
class.....	647
class-map.....	647
clear interface	648
clear qos statistics.....	648
clear qos statistics type.....	649
control-plane.....	649
flowcontrol.....	649
match.....	650
match cos.....	651
match dscp.....	651
match precedence.....	651
match queue.....	652
match vlan.....	652
mtu.....	652
pause.....	653
pfc-cos.....	654
pfc-max-buffer-size.....	654
pfc-shared-buffer-size.....	654
pfc-shared-headroom-buffer-size.....	655
police.....	655
policy-map.....	656
priority.....	656
priority-flow-control mode.....	656
qos-group dot1p.....	657
qos-group dscp.....	657
queue-limit.....	658
queue bandwidth.....	658
queue qos-group.....	659
random-detect (interface).....	659
random-detect (queue).....	659
random-detect color.....	660
random-detect ecn.....	660
random-detect ecn.....	661
random-detect pool.....	661
random-detect weight.....	661
service-policy.....	662
set cos.....	662
set dscp.....	662
set qos-group.....	663
shape.....	663
show class-map.....	664
show control-plane info.....	664
show control-plane statistics.....	665
show interface priority-flow-control.....	665

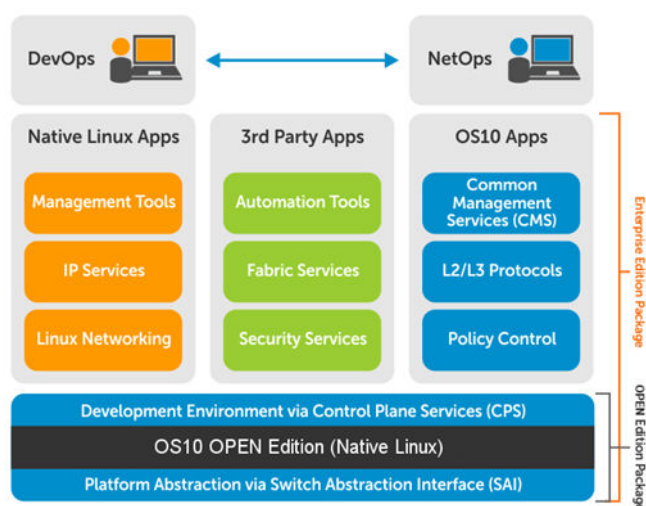
show qos interface.....	666
show policy-map.....	666
show qos control-plane.....	667
show qos egress buffers interface.....	667
show egress buffer-stats interface.....	667
show qos ingress buffers interface.....	668
show ingress buffer-stats interface.....	668
show queuing statistics.....	669
show qos system.....	670
show qos system buffers.....	670
show qos maps.....	671
show qos wred-profile.....	672
system qos.....	673
trust-map.....	674
trust dot1p-map.....	674
trust dscp-map.....	674
qos-map traffic-class.....	675
trust-map.....	675
wred.....	676
Chapter 11: Virtual Link Trunking.....	677
Terminology.....	678
VLT domain.....	678
VLT interconnect.....	679
Configure VLT.....	679
RSTP configuration.....	680
RPVST+ configuration.....	681
Create VLT domain.....	681
VLTi configuration.....	682
Configure the VLT MAC address.....	682
Configure the delay restore timer.....	683
Configure the VLT peer liveness check.....	683
Configure VLT port-channel.....	687
VLT unicast routing.....	688
VRRP Optimized Forwarding.....	688
Migrate VMs across data centers.....	689
View VLT information.....	693
VLT commands.....	695
backup destination.....	695
delay-restore.....	696
discovery-interface.....	696
peer-routing.....	697
peer-routing-timeout.....	697
primary-priority.....	697
show spanning-tree virtual-interface	698
show vlt.....	699
show vlt backup-link.....	700
show vlt mac-inconsistency.....	700
show vlt mismatch.....	701
show vlt role.....	702

show vlt vlt-port-detail.....	702
vlt-domain.....	703
vlt-port-channel.....	703
vlt-mac.....	703
vrrp mode active-active.....	704
Chapter 12: Converged data center services.....	705
Priority flow control.....	705
PFC configuration notes.....	706
Configure PFC.....	707
PFC commands.....	710
Enhanced transmission selection.....	713
ETS configuration notes.....	714
Configure ETS.....	714
ETS commands.....	717
Data center bridging eXchange	717
DCBX configuration notes.....	718
Configure DCBX	718
DCBX commands.....	721
Internet small computer system interface.....	724
iSCSI configuration notes.....	725
Configure iSCSI optimization.....	725
iSCSI synchronization on VLT.....	727
iSCSI commands.....	728
Converged network DCB example.....	732
Chapter 13: sFlow.....	739
Enable sFlow.....	739
Max-header size configuration.....	740
Collector configuration.....	741
Polling-interval configuration.....	741
Sample-rate configuration.....	742
Source interface configuration.....	742
View sFlow information.....	743
sFlow commands.....	744
sflow collector.....	744
sflow enable.....	745
sflow max-header-size.....	745
sflow polling-interval.....	745
sflow sample-rate.....	746
sflow source-interface.....	746
show sflow.....	747
Chapter 14: RESTCONF API.....	748
Configure RESTCONF API.....	748
CLI commands for RESTCONF API.....	749
rest api restconf.....	749
rest https cipher-suite.....	749
rest https server-certificate.....	750

rest https session timeout.....	750
RESTCONF API tasks.....	750
View XML structure of CLI commands.....	751
RESTCONF API layer 2 configuration.....	752
Chapter 15: Troubleshoot OS10.....	767
Diagnostic tools.....	767
Boot partition and image.....	768
Monitor processes.....	768
LED settings.....	769
Packet analysis.....	769
Port adapters and modules.....	770
Test network connectivity.....	770
View diagnostics.....	771
Diagnostic commands.....	773
Password recovery.....	784
Restore factory defaults.....	785
SupportAssist.....	785
Configure SupportAssist.....	786
Set company name.....	787
Set contact information.....	788
Schedule activity.....	788
View status.....	788
SupportAssist commands.....	790
Support bundle.....	796
Event notifications.....	797
generate support-bundle.....	797
System monitoring.....	797
System logging.....	798
View system logs.....	799
Environmental monitoring.....	800
Link-bundle monitoring.....	800
Alarm commands.....	801
Logging commands.....	804
Log into OS10 device.....	809
Frequently asked questions.....	810
Installation.....	810
Hardware.....	810
Configuration.....	811
Security.....	811
Layer 2.....	811
Layer 3.....	811
System management.....	812
Access control lists.....	812
Quality of service.....	812
Monitoring.....	812
Chapter 16: Support resources.....	814

Getting Started

Dell EMC Networking OS10 Enterprise Edition is a network operating system supporting multiple architectures and environments. The networking world is moving from a monolithic stack to a pick-your-own-world. The OS10 solution is designed to allow disaggregation of the network functionality.



Solutions

- Simplicity to integrate enabled devices into an existing infrastructure
- Provides the most up-to-date security fixes which supports a large community of engineers and security experts
- Utilizes an open distribution to simplify the addition of new customized applications or open source applications

Requirements

- Open network installation environment (ONIE)-enabled Dell EMC device
- OS10 software image stored on an HTTP server or universal serial bus (USB) media
- Familiarity with any Linux release

Supported Hardware

The Dell EMC switches supported are:

- S3048-ON
- S4048-ON, S4048T-ON
- S4112F-ON, S4112T-ON
- S4128F-ON, S4128T-ON
- S4148F-ON, S4148FE-ON, S4148T-ON, S4148U-ON
- S4248FB-ON, S4248FBL-ON
- S5148F-ON
- S6010-ON
- Z9100-ON
- Z9264F-ON

Download OS10 image and license

OS10 Enterprise Edition may come factory-loaded and is available for download from the Dell Digital Locker (DDL). A factory-loaded OS10 image has a perpetual license installed. An OS10 image that you download has a 120-day trial license and requires a

perpetual license to run beyond the trial period. See the [Quick Start Guide](#) shipped with your device and [My Account FAQs](#) for more information.

Download an OS10 image and license to:

- Re-install the license on a Dell EMC ONIE switch with factory-installed OS10 image and license.
- Install OS10 on a Dell EMC ONIE switch without an operating system (OS) or license installed:
 - Device converted from OS9 or a third-party OS after you uninstall (wipe clean) the original OS
 - Replacement device received from Dell EMC return material authorization (RMA)
- Upgrade the OS10 image (see [Upgrade OS10](#)).

Your OS10 purchase allows you to download software images posted within the first 90 days of ownership. To extend the software entitlement, you must have a Dell EMC ProSupport or ProSupport Plus contract on your hardware.

Re-install license on factory-loaded OS10

OS10 Enterprise Edition runs with a perpetual license on an ONIE-enabled device with OS10 factory-installed. The license file is installed on the switch. If the license becomes corrupted or is wiped out, you must download the license from DDL under the purchaser's account and reinstall it.

1. Sign in to [DDL](#) using your account credentials.
2. Locate the hardware product name with the entitlement ID and order number.
3. Check that the Service Tag of the purchased device displays in the `Assigned To:` field on the `Products` page.
4. Click `Key Available for Download`.
5. Select how you want to receive the license key — by email or downloaded to your local device.
6. Click `Submit`.
7. Save the `License.zip` file and follow the instructions in [Install license](#) to install the license.

Without operating system installed

You can purchase the OS10 Enterprise Edition image with an after point-of-sale (APOS) order for a Dell EMC ONIE-enabled device that does not have a default operating system or license installed. When the order is fulfilled, you receive an email notification with a software entitlement ID, order number, and link to the DDL.

Bind the software entitlement to the Service Tag of the switch to extend the entitled download period to be the same time as the support contract. OS10 software entitlement allows you to download OS10 software images posted before the purchase date and within 90 days of the date, by default.

1. Sign into [DDL](#) using your account credentials.
2. Locate the entry for your entitlement ID and order number sent by email, then select the product name.
3. On the **Product** page, the `Assigned To:` field on the `Product` tab is blank. Click `Key Available for Download`.
4. Enter the Service Tag of the device you purchased the OS10 Enterprise Edition for in the `Bind to:` and `Re-enter ID:` fields. This step binds the software entitlement to the service tag of the switch.
5. Select how you want to receive the license key — by email or downloaded to your local device.
6. Click `Submit` to download the `License.zip` file.
7. Select the `Available Downloads` tab.
8. Select the OS10 Enterprise Edition release to download, then click `Download`.
9. Read the Dell End User License Agreement. Scroll to the end of the agreement, then click `Yes, I agree`.
10. Select how you want to download the software files, then click `Download Now`.

After you download the OS10 Enterprise Edition image, unzip the `.tar` file by following these guidelines:

- Extract the OS10 binary file from the `.tar` file using any file archiver/compressor software. For example, to unzip a `.tar` file on a Linux server or from the ONIE prompt, enter:

```
tar -xf tar_filename
```

- On a Windows server, some Windows unzip applications insert extra carriage returns (CR) or line feeds (LF) when they extract the contents of a `.tar` file. The additional CRs or LFs may corrupt the downloaded OS10 binary image. Turn off this option if you use a Windows-based tool to untar an OS10 binary file.
- Generate a checksum for the downloaded OS10 binary image by running the `md5sum` command on the image file. Ensure that the generated checksum matches the checksum extracted from the `.tar` file.

```
md5sum image_filename
```

After you unzip the OS10 Enterprise Edition and download the license, see [Installation](#) and [Install license](#) for complete installation and license information.

RMA replacement

A replacement switch comes without an operation system or license installed. If you receive a replacement switch, you must assign the STAG of the replacement switch to the SW entitlement in DDL and install the OS10 software and license.

Follow the steps for an ONIE switch without an OS installed to download OS10 Enterprise Edition and the license. See [Installation](#) and [Install OS10 license](#) for complete installation and license information.

Installation using ONIE

If you purchase an open network install environment (ONIE)-only switch or if you want to replace an existing OS, you can install an OS10 software image using ONIE-based auto-discovery or a manual installation:

- **Automatic installation** — ONIE discovers network information including the DHCP server, connects to an image server, and downloads and installs an image automatically.
- **Manual installation** — Manually configure your network information if a DHCP server is not available, or if you install the OS10 software image using USB media.

If OS10 is pre-installed on a switch, zero-touch deployment (ZTD) is enabled by default. ZTD automatically downloads and installs an OS10 image in the standby partition. For more information, see [Zero-touch deployment](#).

System setup

Verify that the system is connected correctly before installation:

- Connect a serial cable and terminal emulator to the console serial port — required serial port settings are 115200, 8 data bits, and no parity.
- Connect the Management port to the network if you prefer downloading an image over a network. To locate the Console port and the Management port, see the *Getting Started Guide* shipped with your device or the platform-specific *Installation Guide* at www.dell.com/support.

Install OS10

If ONIE is installed on a device, navigate to the ONIE boot menu. An ONIE-enabled device boots up with pre-loaded diagnostics and ONIE software.

```
+-----+
|*ONIE: Install OS
| ONIE: Rescue
| ONIE: Uninstall OS
| ONIE: Update ONIE
| ONIE: Embed ONIE
| ONIE: Diag ONIE
+-----+
```

- **Install OS** — Boots to the ONIE prompt and installs an OS10 image using the automatic discovery process. When ONIE installs a new operating system (OS) image, the previously installed image and OS10 configuration are deleted.
- **Rescue** — Boots to the ONIE prompt and allows for manual installation of an OS10 image or updating ONIE.
- **Uninstall OS** — Deletes the contents of all disk partitions, including the OS10 configuration, except ONIE and diagnostics.
- **Update ONIE** — Installs a new ONIE version.
- **Embed ONIE** — Formats an empty disk and installs ONIE.
- **Diag ONIE** — Runs the system diagnostics.

After the ONIE process installs an OS10 image and you later reboot the switch in `ONIE: Install OS` mode (default), ONIE takes ownership of the system and remains in Install mode (ONIE Install mode is sticky) until an OS10 image successfully installs again. To boot the switch from ONIE for any reason other than installation, select the `ONIE: Rescue` or `ONIE: Update ONIE` option from the ONIE boot menu.

CAUTION: During an automatic or manual OS10 installation, if an error condition occurs that results in an unsuccessful installation, perform **Uninstall OS** first to clear the partitions if there is an existing OS on the device. If the problem persists, contact Dell EMC Technical Support.

Automatic installation

You can automatically install an OS10 image on a Dell ONIE-enabled device. Once the device successfully boots to `ONIE: Install OS`, auto-discovery obtains the hostname, domain name, Management interface IP address, as well as the IP address of the DNS name server(s) on your network from the DHCP server and DHCP options. The ONIE automatic-discovery process locates the stored software image, starts installation, then reboots the device with the new software image.

If a USB drive is inserted, auto-discovery searches the USB storage supporting FAT or EXT2 file systems. It also searches SCP, FTP, or TFTP servers with the default DNS name of the ONIE server. DHCP options are not used to provide the server IP, and the auto discovery method repeats until a successful software image installation occurs and reboots the switch.

Example for automatic installation

1. Use the `mv image_name onie-installer` command to rename the image as `onie-installer`.

```
mv PKGS_OS10-Base-10.3.1B.144-installer-x86_64.bin onie-installer
```

2. After renaming, the system enters the ONIE: Install mode. Enter the command `onie-discovery-start`, which automatically discovers the `onie-installer` image from the DHCP server.

```
ONIE:/ # onie-discovery-start
discover: installer mode detected.  Running installer.
Starting: discover... done.
ONIE:/ # Info: eth0:  Checking link... up.
Info: Trying DHCPv4 on interface: eth0
ONIE: Using DHCPv4 addr: eth0: 10.10.10.17 / 255.0.0.0
Info: eth1:  Checking link... down.
ONIE: eth1: link down.  Skipping configuration.
ONIE: Failed to configure eth1 interface
ONIE: Starting ONIE Service Discovery
Info: Fetching tftp://10.10.10.2/onie-installer-x86_64-dellemc_s4148fe_c2338 ...
Info: Fetching tftp://10.10.10.2/onie-installer-dellemc_s4148fe_c2338 ...
Info: Fetching tftp://10.10.10.2/onie-installer-x86_64-bcm ...
Info: Fetching tftp://10.10.10.2/onie-installer-x86_64 ...
Info: Fetching tftp://10.10.10.2/onie-installer ...
ONIE: Executing installer: tftp://10.10.10.2/onie-installer
...
...
...
Press <DEL> or <F2> to enter setup.
Welcome to GRUB!

GNU GRUB  version 2.02~beta2+e4a1fe391
  OS10-B
  EDA-DIAG
  ONIE      Booting `OS10-A'
Loading OS10 ...

[   3.883826] kvm: already loaded the other module
[   3.967628] dummy_irq: no IRQ given.  Use irq=N
[   3.973212] mic_init not running on X100 ret -19
[   3.980168] esas2r: driver will not be loaded because no ATTO esas2r devices were
found
[   4.021676] mtdoops: mtd device (mtddev=name/number) must be supplied
[   5.092316] i8042: No controller found
[   5.108356] fmc_write_eeprom fake-design-for-testing-f001: fmc_write_eeprom: no
busid passed, refusing all cards
[   5.120111] intel_rapl: driver does not support CPU family 6 model 77
[   4.226593] systemd-fsck[493]: OS10-SYSROOT1: clean, 23571/426544 files,
312838/1704960 blocks
Debian GNU/Linux 8 OS10 ttyS0
Dell EMC Networking Operating System (OS10)
OS10 login:
```

Manual installation

You can manually install an OS10 software image if a DHCP server is not available. If the IP address for the Management port (`eth0`) is not automatically discovered, ONIE sets the IP address to `192.168.3.10`. You must manually configure the Management port and configure the software image file to start installation.

1. Save the OS10 software image on an SCP/TFTP/FTP server.
2. Power up the device and select `ONIE Rescue` for manual installation.
3. (Optional) Stop the DHCP discovery if the device boots to ONIE Install.

```
$ onie-discovery-stop
```

4. Configure the IP addresses on the Management port, where *x.x.x.x* represents your internal IP address. After you configure the Management port, the response should be `up`.

```
$ ifconfig eth0 x.x.x.x netmask 255.255.0.0 up
```

5. Install the software on the device. The installation command accesses the OS10 software from the specified SCP, TFTP, or FTP URL, creates partitions, verifies installation, and reboots itself.

```
$ onie-nos-install image_filename location
```

For example, enter

```
ONIE:/ # onie-nos-install ftp://a.b.c.d/PKGS_OS10-Enterprise-x.x.xx.bin
```

Where *a.b.c.d* represents the location to download the image file from, and *x.x.xx* represents the version number of the software to install.

The OS10 installer image creates several partitions, including OS10-A (active and default) and OS10-B (standby). After installation completes, the system automatically reboots and loads OS10.

Install manually using USB drive

You can manually install the OS10 software image using USB media. Verify that the USB storage device supports a FAT or EXT2 file system. For instructions on how to format a USB device in FAT or EXT2 format, see the accompanying Windows documentation for FAT formatting or Linux documentation for FAT or EXT2 formatting.

1. Plug the USB storage device into the USB storage port on the device.
2. Power up the system to automatically boot with the `ONIE: Rescue` option.
3. (Optional) Stop the ONIE discovery process if the device boots to `ONIE: Install`.

```
$ onie-discovery-stop
```

4. Create a USB mount location on the system.

```
$ mkdir /mnt/media
```

5. Identify the path to the USB drive.

```
$ fdisk -l
```

6. Mount the USB media plugged in the USB port on the device.

```
$ mount -t vfat usb-drive-path /mnt/media
```

7. Install the software from the USB, where `/mnt/media` specifies the path where the USB partition is mounted.

```
$ onie-nos-install /mnt/media/image_file
```

The ONIE auto-discovery process discovers the image file at the specified USB path, loads the software image, and reboots. See the [ONIE User Guide](#) for more information.

Log into OS10

To log in to OS10 Enterprise Edition, power up the device and wait for the system to perform a power-on self test (POST). Enter `admin` for both the default user name and user password. For better security, change the default `admin` password during the first OS10 login. The system saves the new password for future logins. After you change the password through the CLI, enter the `write memory` command to save the configuration.

```
OS10 login: admin
Password: admin
Last login: Mon Mar 20 13:58:27 2017 on ttyS0
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
-----
-*          Dell EMC Network Operating System (OS10)          *-
-*                                                    *-
-* Copyright (c) 1999-2017 by Dell Inc. All Rights Reserved.  *-
-*                                                    *-
-----
```

This product is protected by U.S. and international copyright and intellectual property laws. Dell EMC and the Dell EMC logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

```
OS10# write memory
```

Install OS10 license

If OS10 is factory-loaded on your switch, you do not need to install an OS10 license. If you download OS10 on a trial basis, OS10 comes with a 120-day trial license. To continue with uninterrupted use, purchase and install a perpetual license to avoid the OS10 device rebooting every 72 hours.

After you install OS10 and log in, install the license to run the OS10 Enterprise Edition beyond the trial license period. See [Download OS10 image and license](#) for complete information. The OS10 license is installed in the `/mnt/license` directory.

1. Download the License.zip file from DDL as described in [Download OS10 image and license](#).
2. Open the zip file and locate the license file in the Dell folder. Copy the license file to a local or remote workstation.
3. Install the license file from the workstation in EXEC mode.

```
license install {ftp: | http: | localfs: | scp: | sftp: | tftp: | usb:} filepath/
filename
```

- `ftp://userid:passwd@hostip/filepath` — Copy from a remote FTP server
- `http://hostip/filepath` — Copy from a remote HTTP server
- `http://hostip` — Send request to a remote HTTP server.
- `localfs://filepath` — Install from a local file directory.
- `scp://userid:passwd@hostip/filepath` — Copy from a remote SCP server.
- `sftp://userid:passwd@hostip/filepath` — Copy from a remote SFTP server.
- `tftp://hostip/filepath` — Copy from a remote TFTP server.
- `usb://filepath` — Install from a file directory on a storage device connected to the USB storage port on the switch.
- `filepath/filename` — Enter the directory path where the license file is stored.

Install license

```
OS10# license install scp://user:userpwd@10.1.1.10/CFNNX42-NOSEEnterprise-License.xml
License installation success.
```

Verify license installation

```
OS10# show license status

System Information
-----
Vendor Name       :
Product Name     : S4000ON
Hardware Version  : X01
Platform Name    :
PPID             : TW0J09D32829849Q0164
Service Tag      : BJD7VS1
License Details
-----
Software         : OS10-Enterprise
Version          : 10.4.1.0X
```

```
License Type      : PERPETUAL
License Duration: Unlimited
License Status   : Active
License location: /mnt/license/BJD7VS1.lic
-----
```

Troubleshoot license installation failure

An error message displays if the installation fails.

```
License installation failed
```

1. Verify the installation path to the local or remote location you tried to download the license from.
2. Check the log on the remote server to see why the FTP or TFTP file transfer failed.
3. Ping the remote server from the switch — use the `ping` and `traceroute` commands to test network connectivity. Check the following if ping fails:
 - If the remote server is reachable through the management route, check if the management route is configured correctly.
 - If the remote server is reachable through a front-panel port, check if the static or dynamic route is present.
4. Install the server with the license file on the same subnet as the switch.
5. Check if the server is up and running.

Zero-touch deployment

Zero-touch deployment (ZTD) allows OS10 users to automate switch deployment:

- Upgrade an existing OS10 image.
- Execute a CLI batch file to configure the switch.
- Execute a post-ZTD script to perform additional functions.

ZTD is enabled by default when you boot up a switch with a factory-installed OS10 for the first time or when you perform an `ONIE: OS Install` from the ONIE boot menu. When a switch boots up in ZTD mode, it starts the DHCP client on all interfaces — management and front-panel ports. ZTD configures all interfaces for untagged VLAN traffic. The switch obtains an IP address and a ZTD provisioning script URL from a DHCP server running on the network, and downloads and executes the ZTD script.

- ZTD is supported only in an IPv4 network. ZTD is not supported by DHCPv6.
- At least one of the front-panel ports connected to the network on which the DHCP server is running must be in non-breakout mode.
- After booting up in ZTD mode, if a switch receives no DHCP server response with option 240 within five minutes, it automatically exits ZTD mode. During this time, you can abort ZTD by entering the `ztd cancel` command. The command unlocks the switch configuration so that you can enter OS10 CLI commands.
- When ZTD is enabled, the command-line interface is locked so that you cannot enter OS10 configuration commands. Only `show` commands are available.

According to the contents of the provisioning script, ZTD performs these tasks in this sequence. Although Steps 2, 3 and 4 are each optional, you must enter a valid URL path for at least one of the `IMG_FILE`, `CLI_CONFIG_FILE`, and `POST_SCRIPT_FILE` variables. For example, if you only want to configure the switch, enter only a `CLI_CONFIG_FILE` URL value. In this case, ZTD does not upgrade the OS10 image and does not execute a post-ZTD script.

1. Downloads the files specified in the ZTD provisioning script — OS10 image, CLI configuration batch file, and post-ZTD script.
 - In the provisioning script, enter the file names for the `IMG_FILE`, `CLI_CONFIG_FILE`, and `POST_SCRIPT_FILE` variables as shown in [ZTD provisioning script](#).
 - If no file names are specified, OS10 immediately exits ZTD and returns to CLI configuration mode.
 - If the download of any of the specified files fails, ZTD stops. OS10 exits ZTD and unlocks the CLI configuration mode.
2. If an OS10 image is specified for `IMG_FILE`, ZTD installs the software image in the standby partition. If no configuration file is specified for `CLI_CONFIG_FILE`, ZTD reloads the switch with the new OS10 image.
3. If an OS10 CLI batch file with configuration commands is specified for `CLI_CONFIG_FILE`, ZTD executes the commands in the `PRE-CONFIG` and `POST-CONFIG` sections. After executing the `PRE-CONFIG` commands, the switch reloads with the new OS10 image and then executes the `POST-CONFIG` commands. For more information, see [ZTD CLI batch file](#).
4. If a post-ZTD script file is specified for `POST_SCRIPT_FILE`, ZTD executes the script. For more information, see [Post-ZTD script](#).

NOTE: The ZTD process performs a single switch reboot. The switch reboot occurs only if either a new OS10 image is installed or if the `PRE-CONFIG` section of the CLI batch file has configuration commands that are executed.

ZTD prerequisites

- Store the ZTD provisioning script on a server that supports HTTP connections.
- Store the OS10 image, CLI batch file, and post-ZTD script on a file server that supports either HTTP, FTP, SFTP, or TFTP connections.
- Configure the DHCP server to provide option 240 that returns the URL of the ZTD provisioning script.
- In the ZTD provisioning script, enter the URL locations of an OS10 image, CLI batch file, and/or post-ZTD script. Enter at least one URL, otherwise the ZTD fails and exits to CLI configuration mode.

ZTD guidelines

- You can store the ZTD provisioning script, OS10 image, CLI batch file, and post-ZTD script on the same server, including the DHCP server.
- Write the ZTD provisioning script in bash.
- Write the post-ZTD script in bash or Python. Enter `#!/bin/bash` or `#!/usr/bin/python` as the first line in the script. The default python interpreter in OS10 is 2.7.

Use only common Linux commands, such as `curl`, and common Python language constructs. OS10 only provides a limited set of Linux packages and Python libraries.

- ZTD is disabled by default on automatically provisioned switch fabrics, such as Isilon backend, PowerEdge MX, and VxRail.

Cancel ZTD in progress

To exit ZTD mode and manually configure a switch by entering CLI commands, stop the ZTD process by entering the `ztd cancel` command. You can enter `ztd cancel` only when ZTD is in a waiting state; that is, before it receives an answer from the DHCP server. Otherwise, the command returns an error message; for example:

```
OS10# ztd cancel
% Error: ZTD cancel failed. ZTD process already started and cannot be cancelled at this stage.
```

Disable ZTD

To disable ZTD, enter the `reload` command. The switch reboots in ZTD disabled mode.

Re-enable ZTD

To automatically upgrade OS10 and/or activate new configuration settings, re-enable ZTD by rebooting the switch. Enter the `reload ztd` command. You are prompted to confirm the deletion of the startup configuration.

NOTE: To upgrade OS10 without losing the startup configuration, back up the startup configuration before ZTD runs the provisioning script. Then use the backup startup configuration to restore the previous system configuration.

```
OS10# reload ztd
This action will remove startup-config [confirm yes/no]:
```

View ZTD status

```
OS10# show ztd-status

-----
ZTD Status      : disabled
ZTD State       : completed
Protocol State  : idle
Reason          : ZTD process completed successfully at Mon Jul 16 19:31:57 2018
-----
```

ZTD logs

ZTD generates log messages about its current status.

```
[os10:notify], %Dell EMC (OS10) %ZTD-IN-PROGRESS: Zero Touch Deployment
applying post configurations.
```

ZTD also generates failure messages.

```
[os10:notify], %Dell EMC (OS10) %ZTD-FAILED: Zero Touch Deployment failed to
download the image.
```

Troubleshoot configuration locked

When ZTD is enabled, the CLI configuration is locked. If you enter a CLI command, the error message `configuration is locked` displays. To configure the switch, disable ZTD by entering the `ztd cancel` command.

```
OS10# configure terminal
% Error: ZTD is in progress(configuration is locked).
OS10# ztd cancel
```

ZTD DHCP server configuration

For ZTD operation, configure a DHCP server in the network by adding the required ZTD options; for example:

```
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;
option ztd-provision-url code 240 = text;


default-lease-time 600;
max-lease-time 7200;

subnet 50.0.0.0 netmask 255.255.0.0 {
range 50.0.0.10 50.0.0.254;
option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}

host ztd-leaf1 {
hardware ethernet 90:b1:1c:f4:a9:b1;
fixed-address 50.0.0.8;
option ztd-provision-url "http://50.0.0.1/ztd.sh";
}
```

ZTD provisioning script

Create a ZTD script file that you store on an HTTP server. Configure the URL of the script using DHCP option 240 (`ztd-provision-url`) on the DHCP server.

 **NOTE:** Downloading the ZTD provisioning script is supported only on HTTP connections.

ZTD downloads and executes the script to upgrade the OS10 image, configure the switch, and execute a post-ZTD script to perform additional functions.

- Write the ZTD provisioning script in bash. Enter `#!/bin/bash` as the first line in the script. You can use the sample script in this section as a basis.
- For `IMG_FILE`, enter the URL path of the OS10 image to download and upgrade the switch. The image is written to the standby partition.
- For `CLI_CONFIG_FILE`, enter the URL path of the CLI batch file to download and execute.
- For `POST_SCRIPT_FILE`, enter the URL path of the script to execute.
- ZTD fails and exits to CLI configuration mode if:
 - You do not specify at least one valid URL for the `IMG_FILE`, `CLI_CONFIG_FILE`, and `POST_SCRIPT_FILE` variables.
 - Any of the `IMG_FILE`, `CLI_CONFIG_FILE`, and `POST_SCRIPT_FILE` entries are invalid or if specified, the files cannot be downloaded.

For the `IMG_FILE`, `CLI_CONFIG_FILE`, and `POST_SCRIPT_FILE` files, you can specify HTTP, SCP, SFTP, or TFTP URLs. For example:

```
scp://userid:passwd@hostip/filepath
sftp://userid:passwd@hostip/filepath
```

Example

```
#!/bin/bash

#####
#
#           Example OS10 ZTD Provisioning Script
#
#####

##### UPDATE THE BELOW CONFIG VARIABLES ACCORDINGLY #####
##### ATLEAST ONE OF THEM SHOULD BE FILLED #####

IMG_FILE="http://50.0.0.1/OS10.bin"
CLI_CONFIG_FILE="http://50.0.0.1/cli_config"
POST_SCRIPT_FILE="http://50.0.0.1/no_post_script.py"

##### DO NOT MODIFY THE LINES BELOW #####

sudo os10_ztd_start.sh "$IMG_FILE" "$CLI_CONFIG_FILE" "$POST_SCRIPT_FILE"

#####          **END**          #####
```

ZTD CLI batch file

Create a CLI batch file that ZTD downloads and executes to configure a switch. The ZTD CLI batch file consists of two sections: PRE-CONFIG and POST-CONFIG.

ZTD executes the PRE-CONFIG commands first using the currently running OS10 image, not the OS10 image specified in the provisioning script. ZTD saves the PRE-CONFIG settings to the startup configuration.

If PRE-CONFIG commands are present, ZTD reloads the switch before executing the commands in the POST-CONFIG section. Enter OS10 configuration commands that require a switch reload, such as `switch-port-profile`, in the PRE-CONFIG section. If ZTD installs a new OS10 image (`IMG_FILE`), the new image is activated after the reload.

ZTD then executes the POST-CONFIG commands and saves the new settings in the startup configuration. No additional switch reload is performed.

Example

```
# PRE-CONFIG
configure terminal
hostname ZTD-3
exit
configure terminal
interface vlan 210
description ztd-jun29-210
no shutdown
exit

# POST-CONFIG
configure terminal
snmp-server contact DelleMC
exit
configure terminal
interface vlan 500
no shutdown
```

Post-ZTD script

As a general guideline, use a post-ZTD script to perform any additional functions required to configure and operate the switch. In the ZTD provisioning script, specify the post-ZTD script path for the `POST_SCRIPT_FILE` variable. You can use a script to notify an orchestration server that the ZTD configuration is complete. The server can then configure additional settings on the switch.

For example, during the ZTD phase, you can configure only a management VLAN and IP address, then allow an Ansible orchestration server to perform complete switch configuration. Here is a sample curl script that is included in the post-ZTD script to contact an Ansible server:

```
/usr/bin/curl -H "Content-Type:application/json" -k -X POST
--data '{"host_config_key":"'7d07e79ebdc8f7c292e495daac0fe16b'"}'
-u admin:admin https://10.16.134.116/api/v2/job_templates/9/callback/
```

ZTD commands

reload ztd

Reboots the switch and enables ZTD after the reload.

- Syntax** reload ztd
- Parameters** None
- Default** ZTD is enabled.
- Command Mode** EXEC
- Usage Information** Use the `reload ztd` command to automatically upgrade OS10 and/or activate new configuration settings. When you reload ZTD, you are prompted to confirm the deletion of the startup configuration.
- Example**

```
OS10# reload ztd
```
- Supported Releases** 10.4.1.0 or later

show ztd-status

Displays the current ZTD status: enabled, disabled, or canceled.

- Syntax** show ztd-status
- Parameters** None
- Default** None
- Command Mode** EXEC
- Usage Information** None
- Examples**

```
OS10# show ztd-status
-----
ZTD Status      : disabled
ZTD State       : completed
Protocol State  : idle
Reason          : ZTD process completed successfully at Mon Jul 16
                  19:31:57 2018
-----

OS10# show ztd-status
-----
ZTD Status      : disabled
ZTD State       : failed
Protocol State  : idle
Reason          : ZTD process failed to download post script file
-----
```

- **ZTD Status** — Current operational status: enabled or disabled.
- **ZTD State** — Current ZTD state: initialized, in-progress, successfully completed, failed, or canceled while in progress.
- **Protocol State** — Current state of ZTD protocol: initialized, idle while waiting to enable or complete ZTD process, waiting for DHCP post-hook callback, downloading files, installing image, executing pre-config or post-config CLI commands, or executing post-ZTD script file.
- **Reason** — Description of a successful or failed ZTD process.

Supported Releases 10.4.1.0 or later

ztd cancel

Stops ZTD while in progress. After you cancel ZTD, you can enter CLI commands to configure the switch.

Syntax `ztd cancel`

Parameters None

Default ZTD is enabled.

Command Mode EXEC

Usage Information When ZTD is enabled, the command-line interface is locked. You cannot enter OS10 configuration commands. Use the `ztd cancel` command to cancel the ZTD process and return to CLI configuration mode. You can enter `ztd cancel` only when ZTD is in a waiting state; that is, before it receives an answer from the DHCP server. Otherwise, the command returns an error message.

Example

```
OS10# ztd cancel
```

Supported Releases 10.4.1.0 or later

Remote access

You can remotely access the OS10 command-line interface (CLI) and the Linux shell. When you install OS10 the first time, connect to the switch using the serial port.

Configure remote access

- Configure the Management port IP address
- Configure a default route to the Management port
- Configure a user name and password

Remote access OS10 CLI

1. Open an SSH session using the IP address of the device. You can also use PuTTY or a similar tool to access the device remotely.

```
ssh admin@ip-address
password: admin
```

2. Enter `admin` for both the default user name and password to log into OS10. You are automatically placed in EXEC mode.

```
OS10#
```

Remote access Linux shell

```
ssh linuxadmin@ip-address
password: linuxadmin
```

Configure Management IP address

To remotely access OS10, assign an IP address to the management port. The management interface is used for OOB management purposes.

1. Configure the management interface from CONFIGURATION mode.

```
interface mgmt 1/1/1
```

2. By default, DHCP client is enabled on the Management interface. Disable the DHCP client operations in INTERFACE mode.

```
no ip address dhcp
```

3. Configure an IPv4 or IPv6 address on the Management interface in INTERFACE mode.

```
ip address A.B.C.D/mask
```

```
ipv6 address A:B/prefix-length
```

4. Enable the Management interface in INTERFACE mode.

```
no shutdown
```

Configure Management interface

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# no ip address dhcp
OS10(conf-if-ma-1/1/1)# ip address 10.1.1.10/24
OS10(conf-if-ma-1/1/1)# no shutdown
```

Management Route Configuration

To set up remote access to OS10, configure a management route after you assign an IPv4 or IPv6 address to the Management port. The default management route is the path used by a Management port to communicate with a different network. Management routes are separate from IPv4 and IPv6 routes and are only used to manage the system through the Management port.

```
management route 192.168.100.0/24 1.1.1.1
ip route 192.168.200.0/24 2.2.2.2

management route 192.168.300.0/24 managementethernet
ip route 192.168.400.0/24 interface ethernet 1/1/1
```

Before configuring the static IPv4 address for management interface port, remove the dynamic DHCP setting using the `no ip address dhcp` command.

Configure a management route to the network from which you access the system in CONFIGURATION mode. Repeat the command to configure multiple routes for the Management interface.

```
management route {ipv4-address/mask | ipv6-address/prefix-length}
{forwarding-router-address | managementethernet}
```

- `ipv4-address/mask` — Enter an IPv4 network address in dotted-decimal format (A.B.C.D), then a subnet mask in / prefix-length format (/x).
- `ipv6-address/prefix-length` — Enter an IPv6 address in x:x:x:x format with the prefix length in /x format (prefix range is /0 to /128).
- `forwarding-router-address` — Enter the next-hop IPv4/IPv6 address of a forwarding router for network traffic from the Management port.
- `managementethernet` — Configures the Management port as the interface for the route, and forces the route to be associated with the Management interface.

Configure management route

```
OS10(config)# management route 10.10.20.0/24 10.1.1.1
OS10(config)# management route 172.16.0.0/16 managementethernet
```

Configure user name and password

To set up remote access to OS10, create a new user name and password after you configure the management port and default route. The user role is a mandatory entry.

Enter the password in clear text. It is converted to SHA-512 format in the running configuration. A password must have at least nine alphanumeric and special characters, and at least five different characters from the password previously used for the same username.

For backward compatibility with OS10 releases 10.3.1E and earlier, passwords entered in MD-5, SHA-256, and SHA-512 format are supported.

To increase the required password strength, use the `password-attributes` command.

- Create a user name and password in CONFIGURATION mode.

```
username username password password role role
```

- `username username` — Enter a text string (up to 32 alphanumeric characters; 1 character minimum).
- `password password` — Enter a text string (up to 32 alphanumeric characters; 9 characters minimum).
- `role role` — Enter a user role:
 - `sysadmin` — Full access to all commands in the system, exclusive access to commands that manipulate the file system, and access to the system shell. A system administrator can create user IDs and user roles.
 - `secadmin` — Full access to configuration commands that set security policy and system access, such as password strength, AAA authorization, and cryptographic keys. A security administrator can display security information, such as cryptographic keys, login statistics, and log information.
 - `netadmin` — Full access to configuration commands that manage traffic flowing through the switch, such as routes, interfaces, and ACLs. A network administrator cannot access configuration commands for security features or view security information.
 - `netoperator` — Access to EXEC mode to view the current configuration. A network operator cannot modify any configuration setting on a switch.

Create user name and enter password in clear text

```
OS10(config)# username user05 password alpha404! role sysadmin
```

Upgrade OS10

To upgrade OS10, download a new OS10 Enterprise Edition image from the DDL.

1. Sign into [DDL](#) using your account credentials.
2. Locate the entry for your entitlement ID and order number, then select the product name.
3. Select the `Available Downloads` tab on the Product page.
4. Select the OS10 Enterprise Edition image to download, then click `Download`.
5. Read the Dell End User License Agreement, then scroll to the end of the agreement and click `Yes, I agree`.
6. Select how you want to download the software files, then click `Download Now`.

Install the OS10 image on an ONIE-enabled switch with an installed OS10 license. See [Install OS10 license](#) for complete instructions.

CLI Basics

The OS10 command-line interface (CLI) is the software interface you use to access a device running the software — from the console or through a network connection. The CLI is an OS10-specific command shell that runs on top of a Linux-based

operating system kernel. By leveraging industry-standard tools and utilities, the CLI provides a powerful set of commands that you can use to monitor and configure devices running OS10.

User accounts

OS10 defines two categories of user accounts — use `admin` for both the username and password to log into the CLI, or use `linuxadmin` to log into the Linux shell.

Key CLI features

Consistent command names	Commands that provide the same type of function have the same name, regardless of the portion of the system on which they are operating. For example, all <code>show</code> commands display software information and statistics, and all <code>clear</code> commands erase various types of system information.
Available commands	Information about available commands is provided at each level of the CLI command hierarchy. You can enter a question mark (?) at any level and view a list of the available commands, along with a short description of each command.
Command completion	Command completion for command names (keywords) and for command options is available at each level of the hierarchy. To complete a command or option that you have partially entered, press the Tab key or the Spacebar. If the partially entered letters being a string that uniquely identifies a command, the complete command name appears. A beep indicates that you have entered an ambiguous command, and the possible completions display. Completion also applies to other strings, such as interface names and configuration statements.

CLI command modes

The OS10 CLI has two top-level modes:

- **EXEC mode** — Used to monitor, troubleshoot, check status, and network connectivity.
- **CONFIGURATION mode** — Used to configure network devices.

When you enter CONFIGURATION mode, you are changing the current operating configuration, called the *running configuration*. By default, all configuration changes are automatically saved to the running configuration.

You can change this default behavior by switching to the transaction-based configuration mode. To switch to the transaction-based configuration mode, enter the `start transaction` command. When you switch to the transaction-based configuration mode, you are updating the candidate configuration. Changes to the candidate configuration are not added to the running configuration until you commit them, which activates the configuration. The `start transaction` command applies only to the current session. Changing the configuration mode of the current session to the transaction-based mode does not affect the configuration mode of other CLI sessions.

- After you explicitly enter the `commit` command to save changes to the candidate configuration, the session switches back to the default behavior of automatically saving the configuration changes to the running configuration.
- When a session terminates while in the transaction-based configuration mode, and you have not entered the `commit` command, the changes are maintained in the candidate configuration. You can start a new transaction-based configuration session and continue with the remaining configuration changes.
- All sessions in the transaction-based configuration mode update the same candidate configuration. When you enter the `commit` command on any session in the transaction-based configuration mode or you make configuration changes on any session in the non-transaction-based mode, you also commit the changes made to the candidate configuration in all other sessions running in the transaction-based configuration mode. This implies that inconsistent configuration changes may be applied to the running configuration. Dell EMC recommends that you only make configuration changes on a single CLI session at a time.
- When you enter the `lock` command in a CLI session, configuration changes are disabled on all other sessions, whether they are in the transaction-based configuration mode or the non-transaction-based configuration mode. For more information, see [Candidate configuration](#).

CLI command hierarchy

CLI commands are organized in a hierarchy. Commands that perform a similar function are grouped together under the same level of hierarchy. For example, all commands that display information about the system and the system software are grouped under the `show system` command, and all commands that display information about the routing table are grouped under the `show ip route` command.

CLI command categories

There are several broad groups of CLI commands available:

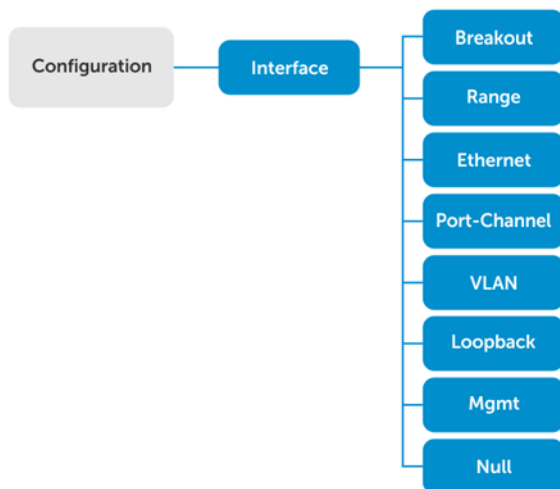
- copy** Copies files from one location on a device to another, from a device to a remote system, or from a remote system to a device.
- configure** Enters CONFIGURATION mode to configure routing protocols, interfaces, network management, and user access.
- exit** Moves up one command mode. Use the `end` command to go directly to EXEC mode.

CONFIGURATION Mode

When you initially log in to OS10, you are automatically placed in EXEC mode by default. To access CONFIGURATION mode, enter the `configure terminal` command. Use CONFIGURATION mode to manage interfaces, protocols, and features.

Interface mode is a sub-mode of CONFIGURATION mode. Interface mode is where you configure Layer 2 and Layer 3 protocols, and IPv4 and IPv6 services specific to an interface:

- Physical interfaces include the Management interface and Ethernet ports
- Logical interfaces include loopback, port-channel, and virtual local area networks (VLANs)



From CONFIGURATION mode, you can also configure L2 and L3 protocols with a specific protocol-configuration mode, such as Spanning-Tree Protocol (STP) or Border Gateway Protocol (BGP).

Command help

To view a list of valid commands for any CLI mode, enter `?`.

1. Enter `?` to view the commands available in EXEC mode.

```
OS10# ?
alarm          Alarm commands
alias          Set alias for a command
batch          Batch Mode
boot           Tell the system where to access the software image at
bootup
```

clear	Clear command
clock	Configure the system clock
commit	Commit candidate configuration
configure	Enter configuration mode
copy	Perform a file copy operation
debug	Debug command
delete	Perform a file delete operation on local file system
dir	Show the list of files for the specified system folder
discard	Discard candidate configuration
exit	Exit from the CLI
generate	Command to generate executed functionality
help	Display available commands
image	Image commands
kill-session	Kill a CLISH session
license	License and digital fulfillment commands
location-led	Set location LED
lock	Lock candidate configuration
move	Perform a file move/rename operation on local filesystem
no	No commands under exec mode
ping	ping -h shows help
ping6	ping6 -h shows help
reload	Reboot Dell EMC Networking Operating System
show	Show running system information
start	Activate transaction based configuration
support-assist-activity	Support Assist related activity
system	System command
terminal	Set terminal settings
traceroute	traceroute --help shows help
unlock	Unlock candidate configuration
validate	Validate candidate configuration
write	Copy from current system configuration

2. Enter CONFIGURATION mode.

```
OS10# configure terminal
OS10(config)#
```

3. Enter ? to show the commands available in CONFIGURATION mode.

```
OS10(config)# ?
aaa                Configure AAA
alias              Set alias for a command
class-map          Configure class map
clock              Configure clock parameters
control-plane      Control-plane configuration
crypto             Crypto commands
dcbx               DCBX commands
dot1x              Configure dot1x global information
end                Exit to the exec Mode
eula-consent       eula-consent configuration
exec-timeout       Set timeout (in seconds) for all CLI sessions
exit               Exit from current mode
feature            Enable feature
hash-algorithm     Hash algorithm configurations
help               Display available commands
host-description   Set the system host description
hostname           Set the system hostname
interface          Select an interface
ip                 Global IP configuration subcommands
ipv6               Configure ipv6
iscsi              enable iscsi globally
lACP               LACP commands
line               Configure a terminal line
link-bundle-utilization
Configure link bundle utilization trigger threshold
lldp               Configure LLDP parameters
load-balancing     Load balancing configurations
logging            Logging commands
login-statistics   Configure login statistics
mac                MAC Address Table Configuration Subcommands
management         management interface commands
monitor            Create a session for monitoring traffic
no                 To delete / disable commands in config mode
ntp                Configure NTP
```

policy-map	Configure policy map
qos-map	Configure QoS map
radius-server	Specify radius server host and configure communication
parameters	
route-map	Creates route-map
router	Enable a routing process
sflow	Configure sflow parameters
snmp-server	Configure SNMP server
spanning-tree	Spanning Tree Subsystem
support-assist	Support Assist feature configuration
system	System configuration
telnet	Configure telnet server settings
track	Configure object tracking
trust	Configure trust
unit-provision	Unit provision configuration
username	Create or modify users
vlt-domain	VLT domain configurations
vrrp	Configure VRRP global attributes
wred	Configure WRED profile

Check device status

Use show commands to check the status of a device and monitor activities.

- Enter show ? from EXEC mode to view a list of commands to monitor a device.

```
OS10# show ?
alarms          Display all current alarm situation in the system
alias          Show list of aliases
boot           Show boot information
candidate-configuration Current candidate configuration
class-map      Show QoS class-map configuration
cli-session    This command is deprecated please use 'show sessions'
instead
clock          Show the system date and time
command-history shows command history of the current user
control-plane  Display control-plane related informations
copy-file      Show file copy operation information
diag          Show diagnostic information for port adapters/modules
diff           Display differences between two configuration set
dot1x         Show dot1x information
environment    Show the environmental information of the system
eula-consent  Shows eula-consent for various modules
exec-timeout   Show the timeout value of CLI session (in seconds)
file          Display file content in specified location
hardware       Show hardware information
hash-algorithm Show hash algorithm information
hosts          show information about DNS
image         Show image information
interface     Interface status and configuration
inventory     Show the system inventory information
ip            show IP commands
ipv6          Display IPv6 neighbor information
iscsi         Show iscsi
lacp          Show LACP information
license       Show license and digital fulfillment related information
link-bundle-utilization Display the link-bundle utilization for the interfaces in
the bundle
lldp          Show lldp
load-balance  Show global traffic load-balance configuration
logging       Show logging messages
mac           MAC forwarding table
monitor       Show port monitoring sessions
network-policy Show network policy
ntp           NTP associations
parser-tree   Show parser tree
policy-map    Show policy-map information
port-channel  LAG status and configuration
processes     Show processes statistics
qos          Show ingress or egress QoS configuration
```

```

queuing          Show egress QoS counters
route-map        Show route map information
running-configuration Current operating configuration
sessions         Show active management sessions
sflow           Show sflow
spanning-tree    Show spanning tree information
startup-configuration Contents of startup configuration
storm-control     Show storm control configuration
support-assist   Shows information about the support assist module
system           Show system status information
tech-support     Collection of show commands
terminal         Show terminal configurations for this session
trace            Show trace messages
track            Show object tracking information
uptime           Show the system uptime
users            Show the current list of users logged into the system ,
and show the session id
version          Show the software version on the system
vlan             Vlan status and configuration
vlt              Show VLT domain info
vrrp             VRRP group status

```

- Enter `show command-history` from EXEC mode to view trace messages for each executed command.

```

OS10# show command-history
 1  Thu Apr 20 19:44:38 UTC 2017  show vlan
 2  Thu Apr 20 19:47:01 UTC 2017  admin
 3  Thu Apr 20 19:47:01 UTC 2017  monitor hardware-components controllers view 0
 4  Thu Apr 20 19:47:03 UTC 2017  system general info system-version view
 5  Thu Apr 20 19:47:16 UTC 2017  admin
 6  Thu Apr 20 19:47:16 UTC 2017  terminal length 0
 7  Thu Apr 20 19:47:18 UTC 2017  terminal datadump
 8  Thu Apr 20 19:47:20 UTC 2017  %abc
 9  Thu Apr 20 19:47:22 UTC 2017  switchshow
10  Thu Apr 20 19:47:24 UTC 2017  cmsh
11  Thu Apr 20 19:47:26 UTC 2017  show version
12  Thu Apr 20 19:47:28 UTC 2017  cmsh
13  Thu Apr 20 19:47:30 UTC 2017  show version
14  Thu Apr 20 19:47:32 UTC 2017  show system
15  Fri Apr 21 12:35:31 UTC 2017  BIOS 3.20.0.3

```

- Enter `clear command-history` to clear the trace messages displayed in `show command-history`.

```
OS10# clear command-history
```

- Check the `show command-history` to verify that the trace messages are cleared.
- Enter `show system` from EXEC mode to view the system status information.

```

OS10# show system

Node Id          : 1
MAC              : 34:17:eb:3a:bd:80
Number of MACs   : 256
Up Time         : 00:16:52

-- Unit 1 --
Status          : up
System Identifier : 1
Down Reason     : unknown
System Location LED : off
Required Type   : S5148F
Current Type    : S5148F
Hardware Revision : X01
Software Version : 10.4.1.0X
Physical Ports  : 48x25GbE, 6x100GbE
BIOS            : 3.36.0.1-2
SMF-FPGA        : 0.1
SMF-MSS         : 1.2.2
CPLD1           : 1.0
CPLD2           : 1.0
CPLD3           : 1.0
CPLD4           : 1.0

```

```

-- Power Supplies --
PSU-ID  Status      Type      AirFlow  Fan  Speed(rpm)  Status
-----
1       up          AC        NORMAL   1    11872       up
2       fail

-- Fan Status --
FanTray Status      AirFlow  Fan  Speed(rpm)  Status
-----
1       up          NORMAL   1    10570       up
                2    10598       up
2       up          NORMAL   1    10541       up
                2    10656       up
3       up          NORMAL   1    10598       up
                2    10802       up
4       up          NORMAL   1    10485       up
                2    10714       up

```

Candidate configuration

When you enter OS10 configuration commands in the transaction-based configuration mode, changes do not take effect immediately and are stored in the candidate configuration. The configuration changes become active on the network device only after you commit the changes with the `commit` command. Changes in the candidate configuration are validated and applied to the running configuration.

The candidate configuration allows you to avoid introducing errors during an OS10 configuration session. You can make changes and then check them before committing them to the active, running configuration on the network device.

Use the `show diff` command to check differences between the running configuration and the candidate configuration. After comparing the two, you can decide if you would like to commit the changes to the running configuration. Use the `discard` command to delete uncommitted changes.

- Enter `show ?` from EXEC mode to view a list of commands to monitor a device.

```

OS10# show ?
aaa                Current candidate aaa configuration
access-list        Current candidate access-list configuration
as-path            Current candidate as-path configuration
bgp                Current candidate bgp configuration
class-map          Current candidate class-map configuration
community-list     Current candidate community-list configuration
compressed         Current candidate configuration in compressed format
control-plane      Current candidate control-plane configuration
dot1x              Current candidate dot1x configuration
extcommunity-list  Current candidate extcommunity-list configuration
interface          Current candidate interface configuration
lACP               Current candidate lACP configuration
lldp               Current candidate lldp configuration
logging            Current candidate logging configuration
monitor            Current candidate monitor session configuration
ospf               Current candidate ospf configuration
ospfv3             Current candidate ospfv3 configuration
policy-map         Current candidate policy-map configuration
prefix-list        Current candidate prefix-list configuration
qos-map            Current candidate qos-map configuration
radius-server      Current candidate radius-server configuration
route-map          Current candidate route-map configuration
sflow              Current candidate sFlow configuration
snmp               Current candidate snmp configuration
spanning-tree      Current candidate spanning-tree configuration
support-assist     Current candidate support-assist configuration
system-qos         Current candidate system-qos configuration
trust-map          Current candidate trust-map configuration

```

users	Current candidate users configuration
vlt	Current candidate vlt domain configuration

Compressed configuration

OS10 offers the `show candidate-configuration compressed` and `show running-configuration compressed` commands that display interface-related configuration in a compressed manner. These commands group similar looking configuration. The compression is done only for interface-related configuration (VLAN and physical interfaces).

View compressed candidate configuration


```
OS10# show candidate-configuration compressed
interface breakout 1/1/1 map 40g-1x
interface breakout 1/1/2 map 40g-1x
interface breakout 1/1/3 map 40g-1x
interface breakout 1/1/4 map 40g-1x
interface breakout 1/1/5 map 40g-1x
interface breakout 1/1/6 map 40g-1x
interface breakout 1/1/7 map 40g-1x
interface breakout 1/1/8 map 40g-1x
interface breakout 1/1/9 map 40g-1x
interface breakout 1/1/10 map 40g-1x
interface breakout 1/1/11 map 40g-1x
interface breakout 1/1/12 map 40g-1x
interface breakout 1/1/13 map 40g-1x
interface breakout 1/1/14 map 40g-1x
interface breakout 1/1/15 map 40g-1x
interface breakout 1/1/16 map 40g-1x
interface breakout 1/1/17 map 40g-1x
interface breakout 1/1/18 map 40g-1x
interface breakout 1/1/19 map 40g-1x
interface breakout 1/1/20 map 40g-1x
interface breakout 1/1/21 map 40g-1x
interface breakout 1/1/22 map 40g-1x
interface breakout 1/1/23 map 40g-1x
interface breakout 1/1/24 map 40g-1x
interface breakout 1/1/25 map 40g-1x
interface breakout 1/1/26 map 40g-1x
interface breakout 1/1/27 map 40g-1x
interface breakout 1/1/28 map 40g-1x
interface breakout 1/1/29 map 40g-1x
interface breakout 1/1/30 map 40g-1x
interface breakout 1/1/31 map 40g-1x
interface breakout 1/1/32 map 40g-1x
ipv6 forwarding enable
username admin password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin
aaa authentication local
snmp-server contact http://www.dell.com/support
!
interface range ethernet 1/1/1-1/1/32
  switchport access vlan 1
  no shutdown
!
interface vlan 1
  no shutdown
!
interface mgmt1/1/1
  ip address dhcp
  no shutdown
  ipv6 enable
  ipv6 address autoconfig
!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi
```


View compressed running configuration

```
OS10# show running-configuration compressed
interface breakout 1/1/1 map 40g-1x
interface breakout 1/1/2 map 40g-1x
interface breakout 1/1/3 map 40g-1x
interface breakout 1/1/4 map 40g-1x
interface breakout 1/1/5 map 40g-1x
interface breakout 1/1/6 map 40g-1x
interface breakout 1/1/7 map 40g-1x
interface breakout 1/1/8 map 40g-1x
interface breakout 1/1/9 map 40g-1x
interface breakout 1/1/10 map 40g-1x
interface breakout 1/1/11 map 40g-1x
interface breakout 1/1/12 map 40g-1x
interface breakout 1/1/13 map 40g-1x
interface breakout 1/1/14 map 40g-1x
interface breakout 1/1/15 map 40g-1x
interface breakout 1/1/16 map 40g-1x
interface breakout 1/1/17 map 40g-1x
interface breakout 1/1/18 map 40g-1x
interface breakout 1/1/19 map 40g-1x
interface breakout 1/1/20 map 40g-1x
interface breakout 1/1/21 map 40g-1x
interface breakout 1/1/22 map 40g-1x
interface breakout 1/1/23 map 40g-1x
interface breakout 1/1/24 map 40g-1x
interface breakout 1/1/25 map 40g-1x
interface breakout 1/1/26 map 40g-1x
interface breakout 1/1/27 map 40g-1x
interface breakout 1/1/28 map 40g-1x
interface breakout 1/1/29 map 40g-1x
interface breakout 1/1/30 map 40g-1x
interface breakout 1/1/31 map 40g-1x
interface breakout 1/1/32 map 40g-1x
ipv6 forwarding enable
username admin password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin
aaa authentication local
snmp-server contact http://www.dell.com/support
!
interface range ethernet 1/1/1-1/1/32
  switchport access vlan 1
  no shutdown
!
interface vlan 1
  no shutdown
!
interface mgmt1/1/1
  ip address dhcp
  no shutdown
  ipv6 enable
  ipv6 address autoconfig
!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi
```

Show difference between candidate and running configurations

```
OS10# show diff candidate-configuration running-configuration
OS10#
```

 **NOTE:** If the show command does not return output, the candidate-configuration and running-configuration files match.

Prevent configuration changes

You can prevent configuration changes on sessions other than the current CLI session using the `lock` command. Use the `lock` and `unlock` commands in EXEC mode to respectively prevent and allow configuration changes on other sessions. When you enter the `lock` command on a CLI session, users cannot make configuration changes across any other active CLI sessions. When you close the CLI session on which you entered the `lock` command, configuration changes are automatically allowed on all other sessions.

Lock configuration changes

```
OS10# lock
```

Unlock configuration changes

```
OS10# unlock
```

Change to transaction-based configuration

To change to transaction-based configuration mode for a session, enter the `start transaction` command

1. Change to transaction-based configuration in EXEC mode.

```
start transaction
```

2. Enable, for example, an interface from INTERFACE mode.

```
interface ethernet 1/1/1  
no shutdown
```

3. Save the configuration.

```
do commit
```

NOTE: After you enter the `do commit` command, the current session switches back to the default behavior of committing all configuration changes automatically.

Save configuration changes manually

```
OS10# start transaction  
OS10# configure terminal  
OS10(config)#  
OS10(config)# interface ethernet 1/1/1  
OS10(config-if-eth1/1/1)# no shutdown  
OS10(config-if-eth1/1/1)# do commit
```

Copy running configuration

The running configuration contains the current OS10 system configuration and consists of a series of OS10 commands. Copy the running configuration to a remote server or local directory as a backup or for viewing and editing. The running configuration is copied as a text file, which you can view and edit with a text editor. To copy the running configuration to the startup configuration file, enter the `copy running-configuration startup-configuration` command.

Copy running configuration to local directory or remote server

```
OS10# copy running-configuration {config://filepath | home://filepath |  
ftp://userid:passwd@hostip/filepath | scp://userid:passwd@hostip/filepath |  
sftp://userid:passwd@hostip/filepath | tftp://hostip/filepath}
```

```
OS10# copy running-configuration scp://root:calvin@10.11.63.120/tmp/qaz.txt
```

Copy file to running configuration

To apply a set of commands to the current running configuration and execute them immediately, copy a text file from a remote server or local directory. The copied commands do not replace the existing commands. If the execution of a copied command fails, the successful execution of copied commands before the failure is maintained.

```
OS10# copy {config://filepath | home://filepath |
ftp://userid:passwd@hostip/filepath | scp://userid:passwd@hostip/filepath |
sftp://userid:passwd@hostip/filepath | tftp://hostip/filepath | http://userid@hostip/
filepath}
running-configuration
```

```
OS10# copy scp://root:calvin@10.11.63.120/tmp/qaz.txt running-configuration
```

Restore startup configuration

The startup configuration file is named `startup.xml` and is stored in the `config` system folder. To create a backup version, copy the startup configuration to a remote server or the local `config:` or `home:` directories.

To restore a backup configuration, copy a local or remote file to the startup configuration and reload the switch. After downloading a backup configuration, you must reload the system, otherwise the configuration does not take effect until you reboot.

Copy file to startup configuration

```
OS10# copy {config://filepath | home://filepath |
ftp://userid:passwd@hostip/filepath | scp://userid:passwd@hostip/filepath |
sftp://userid:passwd@hostip/filepath | tftp://hostip/filepath} config://startup.xml
```

Back up startup file

```
OS10# copy config://startup.xml config://backup-9-28.xml
```

Restore startup file from backup

```
OS10# copy config://backup-9-28.xml config://startup.xml
OS10# reload
```

Back up startup file to server

```
OS10# copy config://startup.xml scp://userid:password@hostip/backup-9-28.xml
```

Restore startup file from server

```
OS10# copy scp://admin:admin@hostip/backup-9-28.xml config://startup.xml
OS10# reload
```

Reload system image

Reboot the system manually using the `reload` command in EXEC mode. You are prompted to confirm the operation.

```
OS10# reload

System configuration has been modified. Save? [yes/no]:yes

Saving system configuration

Proceed to reboot the system? [confirm yes/no]:yes
```

To configure the OS10 image loaded at the next system boot, enter the `boot system` command in EXEC mode.

```
boot system {active | standby}
```

- Enter `active` to load the primary OS10 image stored in the A partition.

- Enter `standby` to load the secondary OS10 image stored in the B partition.

Set next boot image

```
OS10# boot system standby
OS10# show boot
Current system image information:
=====
Type           Boot Type  Active           Standby           Next-Boot
-----
Node-id 1     Flash Boot  [A] 10.2.9999E   [B] 10.2.9999E   [B] standby
```

Filter show commands

You can filter `show` command output to view specific information, or start the command output at the first instance of a regular expression or phrase.

- display-xml** Displays in XML format.
- except** Shows only text that does not match a pattern
- find** Searches for the first occurrence of a pattern and display all the subsequent configurations
- grep** Shows only text that matches a pattern
- no-more** Does not paginate output
- save** Saves the output to a file

Display all output

```
OS10# show running-configuration | no-more
```

Alias command

The `alias` command allows you to create shortcuts for commonly used or long commands, and execute long commands along with their parameters.

The alias supports the following modes:

- Persistent mode — The alias is persistent and can be used in other sessions as well. The aliases created in the Configuration mode are persistent.
- Non-persistent mode — The alias can be used only within the current session. Once the session is closed, the alias is removed from the system. The aliases created in Exec mode are non-persistent.

i **NOTE:** You cannot use existing keywords, parameters, and short form of keywords as alias names, nor can you create a shortcut for the `alias` command. The alias name is case-sensitive and can have a maximum of 20 characters.

- Create an alias in EXEC or CONFIGURATION mode — EXEC mode for non-persistent and CONFIGURATION mode for persistent aliases. The alias value is the actual command where you can use `$n` to enter the input parameters. You can substitute `$n` with either numbers ranging from 1 to 9 or with an asterisk (*) and enter the parameters while executing the commands using the alias. Use asterisk (*) to represent any number of parameters. The maximum number of input parameters is 9.

```
alias alias-name alias-value
```

- Execute the commands using the alias in the respective modes.
- View the current aliases.

```
show alias [brief | detail]
```

- Use the `no` form of the command to delete an alias.

```
no alias alias-name
```

Create alias

```
OS10# alias showint "show interface $*"
OS10(config)# alias goint "interface ethernet $1"
```

View alias output for showint

```
OS10# showint status
-----
Port          Description      Status   Speed   Duplex   Mode  Vlan  Tagged-Vlans
-----
Eth 1/1/1     up              40G     A       1       -
Eth 1/1/2     up              40G     A       1       -
Eth 1/1/3     up              40G     A       1       -
Eth 1/1/4     up              40G     A       1       -
Eth 1/1/5     up              40G     A       1       -
Eth 1/1/6     up              40G     A       1       -
Eth 1/1/7     up              40G     A       1       -
Eth 1/1/8     up              40G     A       1       -
Eth 1/1/9     up              40G     A       1       -
Eth 1/1/10    up              40G     A       1       -
Eth 1/1/11    up              40G     A       1       -
Eth 1/1/12    up              40G     A       1       -
Eth 1/1/13    up              40G     A       1       -
Eth 1/1/14    up              40G     A       1       -
Eth 1/1/15    up              40G     A       1       -
Eth 1/1/16    up              40G     A       1       -
Eth 1/1/17    up              40G     A       1       -
Eth 1/1/18    up              40G     A       1       -
Eth 1/1/19    up              40G     A       1       -
Eth 1/1/20    up              40G     A       1       -
Eth 1/1/21    up              40G     A       1       -
Eth 1/1/22    up              40G     A       1       -
Eth 1/1/23    up              40G     A       1       -
Eth 1/1/24    up              40G     A       1       -
Eth 1/1/25    up              40G     A       1       -
Eth 1/1/26    up              40G     A       1       -
Eth 1/1/27    up              40G     A       1       -
Eth 1/1/28    up              40G     A       1       -
Eth 1/1/29    up              40G     A       1       -
Eth 1/1/30    up              40G     A       1       -
Eth 1/1/31    up              40G     A       1       -
Eth 1/1/32    up              40G     A       1       -
-----
```

View alias output for goint

```
OS10(config)# goint 1/1/1
OS10(conf-if-eth1/1/1)#
```

View alias information

```
OS10# show alias
Name          Type
----          -
govlt         Config
goint         Config
shconfig      Local
showint       Local
shver         Local

Number of config aliases : 2
Number of local aliases  : 3
```

View alias information brief (displays the first 10 characters of the alias value)

```
OS10# show alias brief
Name          Type          Value
----          -
govlt         Config        "vlt-domain..."
goint         Config        "interface ..."
```

```
shconfig          Local      "show runni..."
showint           Local      "show inter..."
shver             Local      "show versi..."

Number of config aliases : 2
Number of local aliases : 3
```

View alias information in detail (displays the entire alias value)

```
OS10# show alias detail
Name                Type      Value
----                -
govlt               Config    "vlt-domain $1"
goint               Config    "interface ethernet $1"
shconfig            Local     "show running-configuration"
showint             Local     "show interface $*"
shver               Local     "show version"

Number of config aliases : 2
Number of local aliases : 3
```

Delete alias

```
OS10# no alias showint
OS10(config)# no alias goint
```

Multi-line alias

You can create multi-line alias where you can save a series of multiple commands in an alias. Multi-line alias is supported only in the Configuration mode.

You cannot use the exiting CLI keywords as alias names. The alias name is case-sensitive and can have a maximum of 20 characters.

- Create an alias in the CONFIGURATION mode. The switch enters the ALIAS mode.

```
alias alias-name
```

- Enter the commands to be executed prefixed by the `line n` command in the ALIAS mode. Enter the commands in double quotes and use `$n` to enter input parameters. You can substitute `$n` with either numbers ranging from 1 to 9 or with an asterisk (*) and enter the parameters while executing the commands using the alias. When you are using asterisk (*), you can use all the input parameters. The maximum number of input parameters is 9.

```
line nn command
```

- (Optional) You can enter the default values to be used for the parameters defined as `$n` in the ALIAS mode.

```
default n input-value
```

- (Optional) Enter a description for the multi-line alias the ALIAS mode.

```
description string
```

- Use the `no` form of the command to delete an alias in the CONFIGURATION mode.

```
no alias alias-name
```

You can modify the existing multi-line alias by entering the corresponding ALIAS mode.

Create multi-line alias

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# line 1 "interface $1 $2"
OS10(config-alias-mTest)# line 2 "no shutdown"
OS10(config-alias-mTest)# line 3 "show configuration"
OS10(config-alias-mTest)# default 1 "ethernet"
OS10(config-alias-mTest)# default 2 "1/1/1"
OS10(config-alias-mTest)# description InterfaceDetails
```

View alias output for mTest with default values

```
OS10(config)# mTest
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
  no shutdown
  switchport access vlan 1
```

View alias output for mTest with different values

```
OS10(config)# mTest ethernet 1/1/10
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# no shutdown
OS10(conf-if-eth1/1/10)# show configuration
!
interface ethernet1/1/10
  no shutdown
  switchport access vlan 1
```

Modify existing multi-line alias

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# line 4 "exit"
```

View the commands saved in the multi-line alias

```
OS10(config-alias-mTest)# show configuration
!
alias mTest
  description InterfaceDetails
  default 1 ethernet
  default 2 1/1/1
  line 1 "interface $1 $2"
  line 2 "no shutdown"
  line 3 "show configuration"
  line 4 exit
```

View alias information

```
OS10# show alias
Name                Type
----                -
mTest                Config

Number of config aliases : 1
Number of local aliases : 0
```

View alias information brief (displays the first 10 characters of each line of each alias)

```
OS10# show alias brief
Name                Type      Value
----                -
mTest                Config    line 1 "interface ..."
                    line 2 "no shutdow..."
                    line 3 "show confi..."
                    default 1 "ethernet"
                    default 2 "1/1/1"
```

```
Number of config aliases : 1
Number of local aliases : 0
```

View alias detail (displays the entire alias value)

```
OS10# show alias detail
Name                Type      Value
----                -
```

```
mTest          Config      line 1 "interface $1 $2"
                                line 2 "no shutdown"
                                line 3 "show configuration"
                                default 1 "ethernet"
                                default 2 "1/1/1"

Number of config aliases : 1
Number of local aliases : 0
```

Delete alias

```
OS10(config)# no alias mTest
```

Batch mode

Create and run a batch file to execute a sequence of multiple commands. A batch file is an unformatted text file that contains two or more commands. Store the batch file in the home directory.

Use vi or any other editor to create the batch file, then use the batch command to execute the file. To execute a series of commands in a file in batch mode (non-interactive processing), use the `batch` command. OS10 automatically commits all commands in a batch file — you do not have to enter the `commit` command.

If a command in the batch file fails, batch operation stops at that command. The remaining commands are not executed.

- Create a batch file (for example, `b.cmd`) on a remote device by entering a series of commands.

```
interface ethernet 1/1/1
no shutdown
no switchport
ip address 172.17.4.1/24
```

- Copy the command file to the home directory on the switch.

```
OS10# copy scp://os10user:os10passwd@10.11.222.1/home/os10/b.cmd home://b.cmd

OS10# dir home

Directory contents for folder: home
Date (modified)          Size (bytes)  Name
-----
2017-02-15T19:25:35Z    77           b.cmd
...
```

- Execute the batch file using the `batch /home/username/filename` command in EXEC mode.

```
OS10# batch /home/admin/b.cmd
Jun 26 18:29:12 OS10 dn_l3_core_services[723]: Node.1-Unit.1:PRI:notice [os10:trap],
%Dell EMC (OS10) %log-notice:IP_ADDRESS_ADD: IP Address add is successful.
IP 172.17.4.1/24 in VRF:default added successfully
```

- (Optional) Verify the new commands in the running configuration.

```
OS10# show running-configuration interface ethernet 1/1/1
!
interface ethernet1/1/1
no shutdown
no switchport
ip address 172.17.4.1/24
```

Linux shell commands

You can execute a single command, or a series of commands using a batch file from the Linux shell.

- Use the `-c` option to run a single command.

```
admin@OS10:/opt/dell/os10/bin$ clish -c "show version"

New user admin logged in at session 10
OS10# show version
Dell EMC Networking OS10-Enterprise
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
OS Version: 10.4.1.0X
Build Version: 10.4.1.0.X.9
Build Time: 2018-06-12T22:18:40-0700
System Type: S4148F-ON
Architecture: x86_64
Up Time: 2 days 03:37:25

User admin logged out at session 10
admin@OS10:/opt/dell/os10/bin$
```

- Use the `-B` option along with a batch file to execute a series of commands.

```
configure terminal
router bgp 100
neighbor 100.1.1.1
remote-as 104
no shutdown
```

Execute the batch file.

```
admin@OS10:/opt/dell/os10/bin$ clish -B ~/batch_cfg.txt

New user admin logged in at session 15
```

Verify the BGP configuration executed by the batch file.

```
admin@OS10:/opt/dell/os10/bin$ clish -c "show running-configuration bgp"

New user admin logged in at session 16
!
router bgp 100
!
 neighbor 100.1.1.1
  remote-as 104
  no shutdown
admin@OS10:/opt/dell/os10/bin$

User admin logged out at session 16
```

SSH commands

You can execute commands remotely using an SSH session. This is supported only for show commands.

- Enter the show command along with SSH.

```
$ ssh admin@ip-address show-command
```

```
$ ssh admin@10.11.98.39 "show version"
admin@10.11.98.39's password:
Dell EMC Networking OS10-Enterprise
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
OS Version: 10.4.1.0X
Build Version: 10.4.1.0.X.9
Build Time: 2018-06-12T22:18:40-0700
System Type: S4148F-ON
Architecture: x86_64
Up Time: 2 days 03:37:25
```

OS9 environment commands

You can configure commands in an OS9 environment by using the `feature config-os9-style` command. The current release supports VLAN tagging and port-channel grouping commands.

- VLAN Interface mode
 - tagged
 - no tagged
 - untagged
 - no untagged
- Port-channel Interface mode:
 - channel-member
 - no channel-member
- Enable the feature to configure commands in an OS9 environment in CONFIGURATION mode.

```
OS10(config)# feature config-os9-style
OS10(config)# exit
OS10# show running-configuration compressed
interface breakout 1/1/28 map 10g-4x
feature config-os9-style
```

- Once this feature is enabled, you can use the OS9 format of commands only in the new session. This configuration does not take effect in the current session.

```
OS10(config)# interface vlan 11
OS10(conf-if-vl-11)# tagged ethernet 1/1/15

OS10(conf-if-vl-11)# show configuration
!
interface vlan11
no shutdown
tagged ethernet 1/1/15
```

Common commands

alias

Creates a command alias.

Syntax	<code>alias <i>alias-name</i> <i>alias-value</i></code>
Parameters	<ul style="list-style-type: none">• <i>alias-name</i> — Enter the name of the alias (up to 20 characters).• <i>alias-value</i> — Enter the command to be executed within double quotes. Enter the \$ followed by either numbers ranging from 1 to 9 or with an asterisk (*) and enter the parameters while executing the commands using the alias. Use asterisk (*) to represent any number of parameters.
Default	Not configured
Command Mode	EXEC CONFIGURATION
Usage Information	Use this command to create a shortcut to long commands along with arguments. Use the numbers 1 to 9 along with the \$ to provide input parameters. The no version of this command deletes an alias.

Example

In the following example, when you enter `showint status`, note that the text on the CLI changes to show `interface status`. The alias changes to the actual command that you have specified in the alias definition.

```
OS10# alias showint "show interface $*"
OS10# showint status
```

Port	Description	Status	Speed	Duplex	Mode	Vlan	Tagged-Vlans
Eth 1/1/1		up	40G		A	1	-
Eth 1/1/2		up	40G		A	1	-
Eth 1/1/3		up	40G		A	1	-
Eth 1/1/4		up	40G		A	1	-
Eth 1/1/5		up	40G		A	1	-
Eth 1/1/6		up	40G		A	1	-
Eth 1/1/7		up	40G		A	1	-
Eth 1/1/8		up	40G		A	1	-
Eth 1/1/9		up	40G		A	1	-
Eth 1/1/10		up	40G		A	1	-
Eth 1/1/11		up	40G		A	1	-
Eth 1/1/12		up	40G		A	1	-
Eth 1/1/13		up	40G		A	1	-
Eth 1/1/14		up	40G		A	1	-
Eth 1/1/15		up	40G		A	1	-
Eth 1/1/16		up	40G		A	1	-
Eth 1/1/17		up	40G		A	1	-
Eth 1/1/18		up	40G		A	1	-
Eth 1/1/19		up	40G		A	1	-
Eth 1/1/20		up	40G		A	1	-
Eth 1/1/21		up	40G		A	1	-
Eth 1/1/22		up	40G		A	1	-
Eth 1/1/23		up	40G		A	1	-
Eth 1/1/24		up	40G		A	1	-
Eth 1/1/25		up	40G		A	1	-
Eth 1/1/26		up	40G		A	1	-
Eth 1/1/27		up	40G		A	1	-
Eth 1/1/28		up	40G		A	1	-
Eth 1/1/29		up	40G		A	1	-
Eth 1/1/30		up	40G		A	1	-
Eth 1/1/31		up	40G		A	1	-
Eth 1/1/32		up	40G		A	1	-

In the following example, when you enter `goint 1/1/1`, note that the text on the CLI changes to `interface ethernet 1/1/1`.

```
OS10# configure terminal
OS10(config)# alias goint "interface ethernet $1"
OS10(config)# goint 1/1/1
OS10(conf-if-eth1/1/1)#
```

Supported Releases 10.3.0E or later

alias (multi-line)

Creates a multi-line command alias.

Syntax `alias alias-name`

Parameters `alias-name` — Enter the name of the alias (up to 20 characters).

Default Not configured

Command Mode CONFIGURATION

Usage Information Use this command to save a series of multiple commands in an alias. The switch enters the ALIAS mode when you create an alias. You can enter the series of commands to be executed using the `line` command.

The no version of this command deletes an alias.

Example

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# line 1 "interface $1 $2"
OS10(config-alias-mTest)# line 2 "no shutdown"
OS10(config-alias-mTest)# line 3 "show configuration"
```

Supported Releases

10.4.0E(R1) or later

batch

Executes a series of commands in a file in batch (non-interactive) processing.

Syntax `batch /home/username/filename`

- Parameters**
- *username* — Enter the user name that was used to copy the command file.
 - *filename* — Enter the name of a batch command file.

Default Not configured

Command Mode EXEC

Usage Information Use this command to create a batch command file on a remote machine. Copy the command file to the home directory on your switch. Enter the `batch` command to execute commands in the file in batch mode. OS10 automatically commits all commands in a batch file; you do not have to enter the `commit` command. To display the files stored in the home directory, enter `dir home`. Use the `dir home` command to view the files stored in the home directory.

Example

```
batch /home/admin/b.cmd
Jun 26 18:29:12 OS10 dn_13_core_services[723]: Node.1-Unit.1:PRI:notice
[os10:trap],
%Dell EMC (OS10) %log-notice:IP_ADDRESS_ADD: IP Address add is
successful.
IP 172.17.4.1/24 in VRF:default added successfully
```

Supported Releases

10.2.0E or later

boot

Configures which OS10 image to use the next time the system boots up.

Syntax `boot system [active | standby]`

- Parameters**
- *active* — Reset the running partition as the next boot partition.
 - *standby* — Set the standby partition as the next boot partition.

Default Not configured

Command Mode EXEC

Usage Information Use this command to configure the location of the OS10 image used to reload the software at boot time. Use the `show boot` command to view the configured next boot image. This command is applied immediately.

Example

```
OS10# boot system standby
```

Supported Releases

10.2.0E or later

commit

Commits changes in the candidate configuration to the running configuration.

Syntax	<code>commit</code>
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to save changes to the running configuration. Use the <code>do commit</code> command to save changes in CONFIGURATION mode.
Example	<pre>OS10# commit</pre>
Example (configuration)	<pre>OS10(config)# do commit</pre>
Supported Releases	10.2.0E or later

configure

Enters CONFIGURATION mode from EXEC mode.

Syntax	<code>configure {terminal}</code>
Parameters	<code>terminal</code> — Enters CONFIGURATION mode from EXEC mode.
Default	Not configured
Command Mode	EXEC
Usage Information	Enter <code>conf t</code> for auto-completion.
Example	<pre>OS10# configure terminal OS10(config)#</pre>
Supported Releases	10.2.0E or later

copy

Copies the current running configuration to the startup configuration and transfers files between an OS10 switch and a remote device.

Syntax	<code>copy [running-configuration startup-configuration config://filepath coredump://filepath ftp://filepath home://filepath scp://filepath sftp://filepath supportbundle://filepath tftp://filepath usb://filepath]</code>
Parameters	<ul style="list-style-type: none">• <code>running-configuration startup-configuration</code> — (Optional) Copy the current running configuration file to the startup configuration file.• <code>config://filepath</code> — (Optional) Copy from configuration directory.• <code>coredump://filepath</code> — (Optional) Copy from the coredump directory.• <code>ftp://userid:passwd@hostip/filepath</code> — (Optional) Copy from a remote FTP server.• <code>home://username/filepath</code> — (Optional) Copy from the home directory.• <code>scp://userid:passwd@hostip/filepath</code> — (Optional) Copy from a remote SCP server.• <code>sftp://userid:passwd@hostip/filepath</code> — (Optional) Copy from a remote SFTP server.

- `supportbundle://filepath` — (Optional) Copy from the support-bundle directory.
- `tftp://hostip/filepath` — (Optional) Copy from a remote TFTP server.
- `usb:filepath` — (Optional) Copy from an USB file system.

Default Not configured

Command Mode EXEC

Usage Information Use this command to save running configuration to the startup configuration, transfer coredump files to a remote location, back up the startup configuration, retrieve a previously backed-up configuration, replace the startup configuration file, or transfer support bundles.

Example

```
OS10# dir coredump

Directory contents for folder: coredump
Date (modified)          Size (bytes)  Name
-----
-----
2017-02-15T19:05:41Z    12402278     core.netconfd-
pro.2017-02-15_19-05-09.gz

OS10# copy coredump://core.netconfd-pro.2017-02-15_19-05-09.gz scp://
os10user:os10passwd@10.11.222.1:/home/os10/core.netconfd-pro.2017-02-
-15_19-05-09.gz
```

Example (copy startup configuration)

```
OS10# dir config

Directory contents for folder: config
Date (modified)          Size (bytes)  Name
-----
-----
2017-02-15T20:38:12Z    54525        startup.xml

OS10# copy config://startup.xml scp://os10user:os10passwd@10.11.222.1:/
home/os10/backup.xml
```

Example (retrieve backed-up configuration)

```
OS10# copy scp://os10user:os10passwd@10.11.222.1:/home/os10/backup.xml
home://config.xml

OS10(conf-if-eth1/1/5)# dir home

Directory contents for folder: home
Date (modified)          Size (bytes)  Name
-----
-----
...
2017-02-15T21:19:54Z    54525        config.xml
...
```

Example (replace startup configuration)

```
OS10# home://config.xml config://startup.xml
```

Supported Releases 10.2.0E or later

default (alias)

Configures default values for input parameters in multi-line alias.

Syntax `default n value`

Parameters

- `n` — Enter the number of the argument (1 to 9).

- *value* — Enter the value for the input parameter.

Default Not configured

Command Mode ALIAS

Usage Information To use special characters in the input parameter value, enclose the string in double quotes. The `no` version of this command removes the default value.

Example

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# default 1 "ethernet 1/1/1"
```

Supported Releases 10.4.0E(R1) or later

delete

Removes or deletes the startup configuration file.

Syntax `delete [config://filepath | coredump://filepath | home://filepath | image://filepath | startup-configuration | supportbundle://filepath | usb://filepath]`

- Parameters**
- `config://filepath` — (Optional) Delete from configuration directory.
 - `coredump://filepath` — (Optional) Delete from coredump directory.
 - `home://filepath` — (Optional) Delete from home directory.
 - `image://filepath` — (Optional) Delete from image directory.
 - `startup-configuration` — (Optional) Delete startup configuration.
 - `supportbundle://filepath` — (Optional) Delete from support-bundle directory.
 - `usb://filepath` — (Optional) Delete from USB file system.

Default Not configured

Command Mode EXEC

Usage Information Use this command to remove a regular file, software image, or startup configuration. Removing the startup configuration restores the system to factory default. You need to reboot the switch — reload for the operation to take effect. Use caution when removing the startup configuration.

Example

```
OS10# delete startup-configuration
```

Supported Releases 10.2.0E or later

description (alias)

Configures a textual description for a multi-line alias.

Syntax `description string`

Parameters `string` — Enter a text string for the alias description.

Default Not configured

Command Mode ALIAS

- Usage Information**
- To use special characters as a part of the description string, enclose the string in double quotes.
 - Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks ("`text description`").
 - Enter a text string after the `description` command to overwrite any previous text string that you previously configured as the description.
 - The `no` version of this command removes the description.

Example

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# description "This alias configures interfaces"
```

Supported Releases

10.4.0E(R1) or later

dir

Displays files stored in available directories.

Syntax

```
dir {config | coredump | home | image | supportbundle | usb}
```

Parameters

- `config` — (Optional) Folder containing configuration files.
- `coredump` — (Optional) Folder containing coredump files.
- `home` — (Optional) Folder containing files in user's home directory.
- `image` — (Optional) Folder containing image files.
- `supportbundle` — (Optional) Folder containing support bundle files.
- `usb` — (Optional) Folder containing files on USB drive.

Default

Not configured

Command Mode

EXEC

Usage**Information**Use the `dir config` command to display configuration files. This command requires at least one parameter.**Example**

```
OS10# dir
config          Folder containing configuration files
coredump        Folder containing coredump files
home            Folder containing files in user's home directory
image           Folder containing image files
supportbundle   Folder containing support bundle files
```

Example (config)

```
OS10# dir config
Directory contents for folder: config
Date (modified)      Size (bytes)  Name
-----
2017-04-26T15:23:46Z  26704        startup.xml
```

Supported Releases

10.2.0E or later

discard

Discards any changes made to the candidate configuration file.

Syntax

```
discard
```

Parameters

None

Default

Not configured

Command Mode

EXEC

Usage**Information**

None

Example

```
OS10# discard
```

Supported Releases

10.2.0E or later

do

Executes most commands from all CONFIGURATION modes without returning to EXEC mode.

Syntax	<code>do command</code>
Parameters	<code>command</code> — Enter an EXEC-level command.
Default	Not configured
Command Mode	INTERFACE
Usage Information	None
Example	

```
OS10(config)# interface ethernet 1/1/7
OS10(conf-if-eth1/1/7)# no shutdown
OS10(conf-if-eth1/1/7)# do show running-configuration
...
!
interface ethernet1/1/7
  no shutdown
!
...
```

Supported Releases	10.2.0E or later
---------------------------	------------------

feature config-os9-style

Configure commands in OS9 environment.

Syntax	<code>feature config-os9-style</code>
Parameters	None
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	Once you enable the feature to configure the commands in OS9 format, log out of the session. In the next session, you can configure the commands in OS9 format. The current release supports VLAN tagging and Port channel grouping commands. This feature does not have any impact on the <code>show</code> commands. Use the <code>no</code> form of the command to disable the feature.
Example	

```
OS10(config)# feature config-os9-style
OS10# show running-configuration compressed
interface breakout 1/1/28 map 10g-4x
feature config-os9-style
```

Supported Releases	10.3.0E or later
---------------------------	------------------

exit

Returns to the next higher command mode.

Syntax	<code>exit</code>
Parameters	None
Default	Not configured

Command Mode	All
Usage Information	None
Example	<pre>OS10(conf-if-eth1/1/1)# exit OS10(config)#</pre>
Supported Releases	10.2.0E or later

license

Installs a license file from a local or remote location.

Syntax	<code>license install [ftp: http: localfs: scp: sftp: tftp: usb:] filepath</code>
Parameters	<ul style="list-style-type: none"> • <code>ftp:</code> — (Optional) Install from remote file system (<code>ftp://userid:passwd@hostip/filepath</code>). • <code>http[s]:</code> — (Optional) Install from remote file system (<code>http://hostip/filepath</code>). • <code>http[s]:</code> — (Optional) Request from remote server (<code>http://hostip</code>). • <code>localfs:</code> — (Optional) Install from local file system (<code>localfs://filepath</code>). • <code>scp:</code> — (Optional) Request from remote file system (<code>scp://userid:passwd@hostip/filepath</code>). • <code>sftp:</code> — (Optional) Request from remote file system (<code>sftp://userid:passwd@hostip/filepath</code>). • <code>tftp:</code> — (Optional) Request from remote file system (<code>tftp://hostip/filepath</code>). • <code>usb:</code> — (Optional) Request from USB file system (<code>usb://filepath</code>).
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to install the Enterprise Edition license file (see Download OS10 image and license for more information). OS10 requires a perpetual license to run beyond the 120-day trial license period. The license file is installed in the <code>/mnt/license</code> directory.
Example	<pre>OS10# license install scp://user:userpwd/10.1.1.10/CFNNX42-NOSEEnterprise-License.lic License installation success.</pre>
Supported Releases	10.3.0E or later

line (alias)

Configures the commands to be executed in a multi-line alias.

Syntax	<code>line nn command</code>
Parameters	<ul style="list-style-type: none"> • <code>nn</code> — Enter the line number (1 to 99). The commands are executed in the order of the line numbers. • <code>command</code> — Enter the command to be executed enclosed in double quotes.
Default	Not configured
Command Mode	ALIAS
Usage Information	The <code>no</code> version of this command removes the line number and the corresponding command from the multi-line alias.

Example

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# line 1 "interface $1 $2"
OS10(config-alias-mTest)# line 2 "no shutdown"
OS10(config-alias-mTest)# line 3 "show configuration"
```

Supported Releases 10.4.0E(R1) or later

lock

Locks the candidate configuration and prevents any configuration changes on any other CLI sessions, either in transaction or non-transaction-based configuration mode.

Syntax lock

Parameters None

Default Not configured

Command Mode EXEC

Usage Information The lock command fails if there are uncommitted changes in the candidate configuration.

Example

```
OS10# lock
```

Supported Releases 10.2.0E or later

management route

Configures an IPv4/IPv6 static route used by the Management port. Repeat the command to configure multiple management routes.

Syntax management route {*ipv4-address/mask* | *ipv6-address/prefix-length*}
{*forwarding-router-address* | managementethernet}

Parameters

- *ipv4-address/mask* — Enter an IPv4 network address in dotted-decimal format (A.B.C.D), then a subnet mask in prefix-length format (/xx).
- *ipv6-address/prefix-length* — Enter an IPv6 address in x:x:x:x:x format with the prefix length in /xxx format (prefix range is /0 to /128).
- *forwarding-router-address* — Enter the next-hop IPv4/IPv6 address of a forwarding router (gateway) for network traffic from the management port.
- *managementethernet* — Configure the Management port as the interface for the route; forces the route to be associated with the management interface.

Default Not configured

Command Mode CONFIGURATION

Usage Information Management routes are separate from IP routes and are only used to manage the system through the management port. To display the currently configured IPv4 and IPv6 management routes, enter the show ip management-route and show ipv6 management-route commands.

Example (IPv4)

```
OS10(config)# management route 10.10.20.0/24 10.1.1.1
OS10(config)# management route 172.16.0.0/16 managementethernet
```

Example (IPv6)

```
OS10(config)# management route 10::/64 10::1
```

Supported Releases 10.2.2E or later

move

Moves or renames a file on the config or home system directories.

- Syntax** `move [config: | home: | usb:]`
- Parameters**
- `config:` — Move from configuration directory (`config://filepath`).
 - `home:` — Move from home directory (`home://filepath`).
 - `usb:` — Move from USB file system (`usb://filepath`).

Default Not configured

Command Mode EXEC

Usage Information Use the `dir config` command to view the directory contents.

Example

```
OS10# move config://startup.xml config://startup-backup.xml
```

Example (dir)

```
OS10# dir config

Directory contents for folder: config
Date (modified)            Size (bytes)    Name
-----
2017-04-26T15:23:46Z      26704           startup.xml
```

Supported Releases 10.2.0E or later

no

Disables or deletes commands in EXEC mode.

Syntax `no [alias | debug | support-assist-activity | terminal]`

- Parameters**
- `alias` — Remove an alias definition.
 - `debug` — Disable debugging.
 - `support-assist-activity` — SupportAssist-related activity.
 - `terminal` — Reset terminal settings.

Default Not configured

Command Mode EXEC

Usage Information Use this command in EXEC mode to disable or remove configuration. Use the `no ?` in CONFIGURATION mode to view available commands.

Example

```
OS10# no alias goint
```

Supported Releases 10.2.0E or later

reload

Reloads the software and reboots the ONIE-enabled device.

Syntax `reload`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information

Use caution while using this command, as it reloads the OS10 image and reboots the device.

Example

```
OS10# reload
Proceed to reboot the system? [confirm yes/no]:y
```

Supported Releases

10.2.0E or later

show alias

Displays configured alias commands available in both persistent and non-persistent modes.

Syntax

```
show alias [brief | detail]
```

Parameters

- **brief** — Displays brief information of aliases.
- **detail** — Displays detailed information of aliases.

Default

None

Command Mode

EXEC

Usage Information

None

Example

```
OS10# show alias
Name                Type
----                -
govlt               Config
goint               Config
mTest               Config
shconfig            Local
showint             Local
shver               Local
Number of config aliases : 3
Number of local aliases : 3
```

Example (brief — displays the first 10 characters of the alias value))

```
OS10# show alias brief
Name                Type      Value
----                -
govlt               Config    "vlt-domain..."
goint               Config    "interface ..."
mTest               Config    line 1 "interface ..."
                   line 2 "no shutdow..."
                   line 3 "show confi..."
shconfig            Local     default 1 "ethernet"
                   default 2 "1/1/1"
showint             Local     "show runni..."
shver               Local     "show inter..."
                   "show versi..."
Number of config aliases : 3
Number of local aliases : 3
```

Example (detail — displays the entire alias value)

```
OS10# show alias detail
Name                Type      Value
----                -
govlt               Config    "vlt-domain $1"
goint               Config    "interface ethernet $1"
mTest               Config    line 1 "interface $1 $2"
                   line 2 "no shutdown"
                   line 3 "show configuration"
                   default 1 "ethernet"
                   default 2 "1/1/1"
```

```

shconfig          Local      "show running-configuration"
showint           Local      "show interface $*"
shver             Local      "show version"

Number of config aliases : 3
Number of local aliases : 3

```

Supported Releases 10.3.0E or later

show boot

Displays detailed information about the boot image.

Syntax show boot [detail]

Parameters None

Default Not configured

Command Mode EXEC

Usage Information The Next-Boot field displays the partition that the next reload uses.

Example

```

OS10# show boot
Current system image information:
=====
Type          Boot Type      Active           Standby          Next-Boot
-----
Node-id 1    Flash Boot    [A] 10.2.9999E    [B] 10.2.9999E    [A] active

```

```

OS10# show boot detail
Current system image information detail:
=====
Type:                Node-id 1
Boot Type:           Flash Boot
Active Partition:    A
Active SW Version:   10.2.9999E
Active SW Build Version: 10.2.9999E(3633)
Active Kernel Version: Linux 3.16.36
Active Build Date/Time: 2017-01-25T06:36:22Z
Standby Partition:   B
Standby SW Version:  10.2.9999E
Standby SW Build Version: 10.2.9999E(3633)
Standby Build Date/Time: 2017-01-25T06:36:22Z
Next-Boot:           active[A]

```

Supported Releases 10.2.0E or later

show candidate-configuration

Displays the current candidate configuration file.

Syntax show candidate-configuration [aaa | access-list | as-path | bgp | class-map | community-list | compressed | control-plane | dot1x | extcommunity-list | interface | lacp | line | lldp | logging | monitor | ospf | ospfv3 | policy-map | prefix-list | qos-map | radius-server | route-map | sflow | snmp | spanning-tree | support-assist | system-qos | trust-map | users | vlt]

Parameters

- aaa — (Optional) Current candidate AAA configuration.
- access-list — (Optional) Current candidate access-list configuration.

- `as-path` — (Optional) Current candidate as-path configuration.
- `bgp` — (Optional) Current candidate BGP configuration.
- `class-map` — (Optional) Current candidate class-map configuration.
- `community-list` — (Optional) Current candidate community-list configuration.
- `compressed` — (Optional) Current candidate configuration in compressed format.
- `control-plane` — (Optional) Current candidate control-plane configuration.
- `dot1x` — (Optional) Current candidate dot1x configuration.
- `extcommunity-list` — (Optional) Current candidate extcommunity-list configuration.
- `interface` — (Optional) Current candidate interface configuration.
- `lACP` — (Optional) Current candidate LACP configuration.
- `lldp` — (Optional) Current candidate LLDP configuration.
- `logging` — (Optional) Current candidate logging configuration.
- `monitor` — (Optional) Current candidate monitor session configuration.
- `ospf` — (Optional) Current candidate OSPF configuration.
- `ospfv3` — (Optional) Current candidate OSPFv3 configuration.
- `policy-map` — (Optional) Current candidate policy-map configuration.
- `prefix-list` — (Optional) Current candidate prefix-list configuration.
- `qos-map` — (Optional) Current candidate qos-map configuration.
- `radius-server` — (Optional) Current candidate RADIUS server configuration.
- `route-map` — (Optional) Current candidate route-map configuration.
- `sflow` — (Optional) Current candidate sFlow configuration.
- `snmp` — (Optional) Current candidate SNMP configuration.
- `spanning-tree` — (Optional) Current candidate spanning-tree configuration.
- `support-assist` — (Optional) Current candidate support-assist configuration.
- `system-qos` — (Optional) Current candidate system-qos configuration.
- `trust-map` — (Optional) Current candidate trust-map configuration.
- `users` — (Optional) Current candidate users configuration.
- `vlt` — (Optional) Current candidate VLT domain configuration.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show candidate-configuration
! Version 10.2.9999E
! Last configuration change at Apr 11 10:36:43 2017
!
username admin
password $6$q9QBeYjZ$jfxzVqGhkkX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface ethernet1/1/1
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/2
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/3
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/4
```

```

switchport access vlan 1
no shutdown
!
interface ethernet1/1/5
switchport access vlan 1
no shutdown
!
--more--

```

**Example
(compressed)**

```

OS10# show candidate-configuration compressed
username admin
password $6$q9QBeYjZ$jfxzVqGhkkX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface range ethernet 1/1/1-1/1/32
switchport access vlan 1
no shutdown
!
interface vlan 1
no shutdown
!
interface mgmt1/1/1
ip address 10.11.58.145/8
no shutdown
ipv6 enable
ipv6 address autoconfig

!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi

```

Supported Releases 10.2.0E or later

show environment

Displays information about environmental system components, such as temperature, fan, and voltage.

Syntax show environment

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```

OS10# show environment

Unit      State      Temperature
-----
1         up         43

Thermal sensors
Unit      Sensor-Id      Sensor-name      Temperature
-----
1         1              CPU On-Board temp sensor      32

```


1	2	Switch board temp sensor	28
1	3	System Inlet Ambient-1 temp sensor	27
1	4	System Inlet Ambient-2 temp sensor	25
1	5	System Inlet Ambient-3 temp sensor	26
1	6	Switch board 2 temp sensor	31
1	7	Switch board 3 temp sensor	41
1	8	NPU temp sensor	43

Supported Releases 10.2.0E or later

show inventory

Displays system inventory information.

Syntax show inventory

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show inventory
Product       : S4048ON
Description   : S4048-ON 48x10GbE, 6x40GbE QSFP+ Interface Module
Software version : 10.4.1.0.X.9
```

Unit	Type	Part Number	Rev	Piece	Part ID	Svc Tag	Exprs
* 1	S4048ON			----			
1	S4048ON-PWR-2-AC-R	0T9FNW	X01	TW-0T9FNW-28298-49Q-0034	AEIOU##	226	4
1	S4048ON-FANTRAY-1-R	0MGDH8	X01	TW-0MGDH8-28298-49Q-0451	AEIOU##	226	4
1	S4048ON-FANTRAY-2-R	0MGDH8	X01	TW-0MGDH8-28298-49Q-0450	AEIOU##	226	4
1	S4048ON-FANTRAY-3	P1FAN1	A01	CN-123456-FAN10-058-901			

Supported Releases 10.2.0E or later

show ip management-route

Displays the IPv4 routes used to access the management port.

Syntax show ip management-route [all | connected | summary]

- Parameters**
- all — (Optional) Display the IPv4 routes that the management interface uses.
 - connected — (Optional) Display only routes directly connected to a management interface.
 - summary — (Optional) Display the number of active and non-active management routes and their remote destinations.
 - static — (Optional) Display non-active management routes.

Default Not configured

Command Mode EXEC

Usage Information Use this command to view the IPv4 static and connected routes configured for the management port. Use the management route command to configure an IPv4 or IPv6 management route.

Example

```
OS10# show ip management-route
Destination      Gateway          State           Source
```

```
-----  
192.168.10.0/24      managementethernet    Connected    Connected
```

Supported Releases 10.2.2E or later

show ipv6 management-route

Displays the IPv6 routes used to access the management port.

Syntax `show ipv6 management-route [all | connected | summary]`

- Parameters**
- `all` — (Optional) Display the IPv6 routes that the management interface uses.
 - `connected` — (Optional) Display only routes directly connected to the management interface.
 - `summary` — (Optional) Display the number of active and non-active management routes and their remote destinations.
 - `static` — (Optional) Display non-active management routes.

Default Not configured

Command Mode EXEC

Usage Information Use this command to view the IPv6 static and connected routes configured for the management port. Use the `management route` command to configure an IPv4 or IPv6 management route.

Example

```
OS10# show ipv6 management-route  
  
Destination      Gateway          State  
-----  
2001:34::0/64    ManagementEthernet 1/1    Connected  
2001:68::0/64    2001:34::16      Active
```

Supported Releases 10.2.2E or later

show license status

Displays license status information.

Syntax `show license status`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information Use this command to view the `show license status` command to verify the current license for running OS10, its duration, and the service tag of the switch to which it is assigned.

Example

```
OS10# show license status  
  
System Information  
-----  
Vendor Name      :  
Product Name     :      S4000ON  
Hardware Version :      X01  
Platform Name    :  
PPID             :      TW0J09D32829849Q0164  
Service Tag      :      BJD7VS1  
License Details  
-----  
Software         :      OS10-Enterprise  
Version          :      10.4.1.0X  
License Type     :      PERPETUAL
```

```
License Duration:      Unlimited
License Status   :    Active
License location:    /mnt/license/BJD7VS1.lic
-----
```

Supported Releases 10.3.0E or later

show running-configuration

Displays the configuration currently running on the device.

Syntax `show running-configuration [aaa | access-list | as-path | bgp | class-map | community-list | compressed | control-plane | dot1x | extcommunity-list | interface | lacp | line | lldp | logging | monitor | ospf | ospfv3 | policy-map | prefix-list | qos-map | radius-server | route-map | sflow | snmp | spanning-tree | support-assist | system-qos | trust-map | users | vlt]`

- Parameters**
- `aaa` — (Optional) Current operating AAA configuration.
 - `access-list` — (Optional) Current operating access-list configuration.
 - `as-path` — (Optional) Current operating as-path configuration.
 - `bgp` — (Optional) Current operating BGP configuration.
 - `class-map` — (Optional) Current operating class-map configuration.
 - `community-list` — (Optional) Current operating community-list configuration.
 - `compressed` — (Optional) Current operating configuration in compressed format.
 - `control-plane` — (Optional) Current operating control-plane configuration.
 - `dot1x` — (Optional) Current operating dot1x configuration.
 - `extcommunity-list` — (Optional) Current operating extcommunity-list configuration.
 - `interface` — (Optional) Current operating interface configuration.
 - `lacp` — (Optional) Current operating LACP configuration.
 - `lldp` — (Optional) Current operating LLDP configuration.
 - `logging` — (Optional) Current operating logging configuration.
 - `monitor` — (Optional) Current operating monitor session configuration.
 - `ospf` — (Optional) Current operating OSPF configuration.
 - `ospfv3` — (Optional) Current operating OSPFv3 configuration.
 - `policy-map` — (Optional) Current operating policy-map configuration.
 - `prefix-list` — (Optional) Current operating prefix-list configuration.
 - `qos-map` — (Optional) Current operating qos-map configuration.
 - `radius-server` — (Optional) Current operating radius-server configuration.
 - `route-map` — (Optional) Current operating route-map configuration.
 - `sflow` — (Optional) Current operating sFlow configuration.
 - `snmp` — (Optional) Current operating SNMP configuration.
 - `spanning-tree` — (Optional) Current operating spanning-tree configuration.
 - `support-assist` — (Optional) Current operating support-assist configuration.
 - `system-qos` — (Optional) Current operating system-qos configuration.
 - `trust-map` — (Optional) Current operating trust-map configuration.
 - `users` — (Optional) Current operating users configuration.
 - `vlt` — (Optional) Current operating VLT domain configuration.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show running-configuration
! Version 10.2.9999E
! Last configuration change at Apr 11 01:25:02 2017
!
username admin
password $6$q9QBeYjZ$jfxzVqGhkkX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface ethernet1/1/1
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/3
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/4
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/5
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/6
 switchport access vlan 1
 no shutdown
--more--
```

Example (compressed)

```
OS10# show running-configuration compressed
username admin
password $6$q9QBeYjZ$jfxzVqGhkkX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface range ethernet 1/1/1-1/1/32
 switchport access vlan 1
 no shutdown
!
interface vlan 1
 no shutdown
!
interface mgmt1/1/1
 ip address 10.11.58.145/8
 no shutdown
 ipv6 enable
 ipv6 address autoconfig

!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi
```

Supported Releases

10.2.0E or later

show startup-configuration

Displays the contents of the startup configuration file.

Syntax	show startup-configuration [compressed]
Parameters	compressed — (Optional) View a compressed version of the startup configuration file.
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	

```
OS10# show startup-configuration
username admin
password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
ip route 0.0.0.0/0 10.11.58.1
!
interface ethernet1/1/1
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/2
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/3
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/4
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/5
  switchport access vlan 1
  no shutdown
!
--more--
```

Example (compressed)

```
OS10# show startup-configuration compressed
username admin
password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
ip route 0.0.0.0/0 10.11.58.1
!
interface range ethernet 1/1/1-1/1/32
  switchport access vlan 1
  no shutdown
!
interface vlan 1
  no shutdown
!
interface mgmt1/1/1
  ip address 10.11.58.145/8
  no shutdown
  ipv6 enable
  ipv6 address autoconfig
!
support-assist
```

```

!
policy-map type application policy-iscsi
!
class-map type application class-iscsi

```

Supported Releases 10.2.0E or later

show system

Displays system information.

Syntax show system [brief | node-id]

Parameters

- **brief** — View abbreviated list of system information.
- **node-id** — Node ID number.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```

OS10# show system

Node Id           : 1
MAC               : 00:0c:29:00:a5:d2
Number of MACs   : 256
Up Time          : 07:44:26

-- Unit 1 --
Status           : up
Down Reason      : unknown
System Location LED : off
Required Type    : S4048-ON
Current Type     : S4048-ON
Hardware Revision :
Software Version : 10.4.9999EX
Physical Ports   : 32x40GbE

-- Power Supplies --
PSU-ID  Status   Type    AirFlow  Fan  Speed(rpm)  Status
-----
1       up       DC      REVERSE  1    7200         up
2       up       DC      REVERSE  1    7200         up

-- Fan Status --
FanTray  Status   AirFlow  Fan  Speed(rpm)  Status
-----
1       up       REVERSE  1    7000         up
                2    7000         up
2       up       REVERSE  1    7000         up
                2    7000         up
3       up       REVERSE  1    7000         up
                2    7000         up

```

Example (node-id)

```

OS10# show system node-id 1 fanout-configured

Interface      Breakout capable      Breakout state
-----
Eth 1/1/1      Yes                   BREAKOUT_1x1

```

Eth 1/1/2	Yes	BREAKOUT_1x1
Eth 1/1/3	Yes	BREAKOUT_1x1
Eth 1/1/4	Yes	BREAKOUT_1x1
Eth 1/1/5	Yes	BREAKOUT_1x1
Eth 1/1/6	Yes	BREAKOUT_1x1
Eth 1/1/7	Yes	BREAKOUT_1x1
Eth 1/1/8	Yes	BREAKOUT_1x1
Eth 1/1/9	Yes	BREAKOUT_1x1
Eth 1/1/10	Yes	BREAKOUT_1x1
Eth 1/1/11	Yes	BREAKOUT_1x1
Eth 1/1/12	Yes	BREAKOUT_1x1
Eth 1/1/13	No	BREAKOUT_1x1
Eth 1/1/14	No	BREAKOUT_1x1
Eth 1/1/15	No	BREAKOUT_1x1
Eth 1/1/16	No	BREAKOUT_1x1
Eth 1/1/17	Yes	BREAKOUT_1x1
Eth 1/1/18	Yes	BREAKOUT_1x1
Eth 1/1/19	Yes	BREAKOUT_1x1
Eth 1/1/20	Yes	BREAKOUT_1x1
Eth 1/1/21	Yes	BREAKOUT_1x1
Eth 1/1/22	Yes	BREAKOUT_1x1
Eth 1/1/23	Yes	BREAKOUT_1x1
Eth 1/1/24	Yes	BREAKOUT_1x1
Eth 1/1/25	Yes	BREAKOUT_1x1
Eth 1/1/26	Yes	BREAKOUT_1x1
Eth 1/1/27	Yes	BREAKOUT_1x1
Eth 1/1/28	Yes	BREAKOUT_1x1
Eth 1/1/29	No	BREAKOUT_1x1
Eth 1/1/30	No	BREAKOUT_1x1
Eth 1/1/31	No	BREAKOUT_1x1
Eth 1/1/32	No	BREAKOUT_1x1

Example (brief)

```
OS10# show system brief

Node Id           : 1
MAC               : 34:17:18:19:20:21

-- Unit --
Unit  Status      ReqType      CurType      Version
-----
1     up           S4048        S4048        10.4.9999E(X)

-- Power Supplies --
PSU-ID  Status      Type      AirFlow      Fan  Speed(rpm)  Status
-----
1       fail
2       up           AC        REVERSE      1    14688       up

-- Fan Status --
FanTray  Status      AirFlow      Fan  Speed(rpm)  Status
-----
1       up           REVERSE      1    13063       up
                2    13020       up
2       up           REVERSE      1    12956       up
                2    12977       up
3       up           NORMAL       1    12956       up
                2    13063       up
```

Supported Releases

10.2.0E or later

show version

Displays software version information.


Syntax	<code>show version</code>
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	

```
OS10# show version
Dell EMC Networking OS10-Enterprise
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
OS Version: 10.4.1.0X
Build Version: 10.4.1.0.X.9
Build Time: 2018-06-12T22:18:40-0700
System Type: S4148F-ON
Architecture: x86_64
Up Time: 2 days 03:37:25
```

Supported Releases	10.2.0E or later
---------------------------	------------------

start

Activates the transaction-based configuration mode for the active session.

Syntax	<code>start transaction</code>
Parameters	<code>transaction</code> - Enables transaction-based configuration.
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to save changes to the candidate configuration before applying configuration changes to the running configuration.  NOTE: Before you start a transaction, you must lock the session using the <code>lock</code> command in EXEC mode. Otherwise, the configuration changes from other sessions get committed.

Example	<pre>OS10# start transaction</pre>
----------------	------------------------------------

Supported Releases	10.3.1E or later
---------------------------	------------------

system

Executes a Linux command from within OS10.

Syntax	<code>system command</code>
Parameters	<code>command</code> — Enter the Linux command to execute.
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# system bash
admin@OS10:~$ pwd
/config/home/admin
admin@OS10:~$ exit
OS10#
```

Supported Releases 10.2.0E or later

system identifier

Sets a non-default unit ID in a non-stacking configuration.

Syntax `system identifier system-identifier-ID`

Parameters `system-identifier-ID` — Enter the system identifier ID (1–9)

Default Not configured

Command Mode CONFIGURATION

Usage Information The system ID is displayed in the stack LED on the front panel.

Example

```
OS10(config)# system identifier 1
```

Supported Releases 10.3.0E or later

terminal

Sets the number of lines to display on the terminal and enables logging.

Syntax `terminal {length lines | monitor}`

Parameters

- `length lines` — Enter the number of lines to display on the terminal (0 to 512, default 24).
- `monitor` — Enables logging on the terminal.

Default 24 terminal lines

Command Mode EXEC

Usage Information Enter zero (0) for the terminal to display without pausing.

Example

```
OS10# terminal monitor
```

Supported Releases 10.2.0E or later

traceroute

Displays the routes that packets take to travel to an IP address.

Syntax `traceroute [vrf {management | vrf-name}] host [-46dFITnreAUDV] [-f first_ttl] [-g gate,...] [-i device] [-m max_ttl] [-N squeries] [-p port] [-t tos] [-l flow_label] [-w waittime] [-q nqueries] [-s src_addr] [-z sendwait] [--fwmark=num] host [packetlen]`

Parameters

- `vrf management` — (Optional) Traces the route to an IP address in the management VRF instance.
- `vrf vrf-name` — (Optional) Traces the route to an IP address in the specified VRF instance.

- *host* — Enter the host to trace packets from.
- *-i interface* — (Optional) Enter the IP address of the interface through which traceroute sends packets. By default, the interface is selected according to the routing table.
- *-m max_ttl* — (Optional) Enter the maximum number of hops (maximum time-to-live value) that traceroute probes (default 30).
- *-p port* — (Optional) Enter a destination port:
 - For UDP tracing, enter the destination port base that traceroute uses (the destination port number is incremented by each probe).
 - For ICMP tracing, enter the initial ICMP sequence value (incremented by each probe).
 - For TCP tracing, enter the (constant) destination port to connect.
 - *-P protocol* — (Optional) Use a raw packet of the specified protocol for traceroute. Default protocol is 253 (RFC 3692).
 - *-s source_address* — (Optional) Enter an alternative source address of one of the interfaces. By default, the address of the outgoing interface is used.
 - *-q nqueries* — (Optional) Enter the number of probe packets per hop (default 3).
 - *-N squeries* — (Optional) Enter the number of probe packets that are sent out simultaneously to accelerate traceroute (default 16).
 - *-t tos* — (Optional) For IPv4, enter the Type of Service (TOS) and Precedence values to use. 16 sets a low delay; 8 sets a high throughput.
 - *-UL* — (Optional) Use UDPLITE for tracerouting (default port is 53).
 - *-w waittime* — (Optional) Enter the time (in seconds) to wait for a response to a probe (default 5 seconds).
 - *-z sendwait* — (Optional) Enter the minimal time interval to wait between probes (default 0). A value greater than 10 specifies a number in milliseconds, otherwise it specifies a number of seconds. This option is useful when routers rate-limit ICMP messages.
 - *--mtu* — (Optional) Discovers the MTU from the path being traced.
 - *--back* — (Optional) Prints the number of backward hops when it seems different with the forward direction.
 - *host* — (Required) Enter the name or IP address of the destination device.
 - *packet_len* — (Optional) Enter the total size of the probing packet (default 60 bytes for IPv4 and 80 for IPv6).

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# traceroute www.dell.com
traceroute to www.dell.com (23.73.112.54), 30 hops max, 60 byte packets
 1 10.11.97.254 (10.11.97.254) 4.298 ms 4.417 ms 4.398 ms
 2 10.11.3.254 (10.11.3.254) 2.121 ms 2.326 ms 2.550 ms
 3 10.11.27.254 (10.11.27.254) 2.233 ms 2.207 ms 2.391 ms
 4 Host65.hbms.com (63.80.56.65) 3.583 ms 3.776 ms 3.757 ms
 5 host33.30.198.65 (65.198.30.33) 3.758 ms 4.286 ms 4.221 ms
 6 3.GigabitEthernet3-3.GW3.SCL2.ALTER.NET (152.179.99.173) 4.428 ms
 2.593 ms 3.243 ms
 7 0.xe-7-0-1.XL3.SJC7.ALTER.NET (152.63.48.254) 3.915 ms 3.603 ms
 3.790 ms
 8 TenGigE0-4-0-5.GW6.SJC7.ALTER.NET (152.63.49.254) 11.781 ms 10.600
 ms 9.402 ms
 9 23.73.112.54 (23.73.112.54) 3.606 ms 3.542 ms 3.773 ms
```

Example (IPv6)

```
OS10# traceroute 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
```

Supported Releases 10.2.0E or later

unlock

Unlocks a previously locked candidate configuration file.

Syntax	<code>unlock</code>
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	

```
OS10# unlock
```

Supported Releases	10.2.0E or later
---------------------------	------------------

write

Copies the current running configuration to the startup configuration file.

Syntax	<code>write {memory}</code>
Parameters	<code>memory</code> — Copy the current running configuration to the startup configuration.
Default	Not configured
Command Mode	EXEC
Usage Information	This command has the same effect as the <code>copy running-configuration startup-configuration</code> command. The running configuration is not saved to a local configuration file other than the startup configuration. Use the <code>copy</code> command to save running configuration changes to a local file.

Example	
----------------	--

```
OS10# write memory
```

Supported Releases	10.2.0E or later
---------------------------	------------------

Interfaces

You can configure and monitor physical interfaces (Ethernet), port-channels, and VLANs in L2 or L3 modes.

Table 1. Interface types

Interface type	Supported / default mode	Requires creation / default status
Ethernet (PHY)	L2, L3 / unset	No / no shutdown (enabled)
Management	N/A	No / no shutdown (enabled)
Loopback	L3 / L3	Yes / no shutdown (enabled)
Port-channel	L2, L3 / unset	Yes / no shutdown (enabled)
VLAN	L2, L3 / L3	Yes (except default) / no shutdown (enabled)

Ethernet interfaces

Ethernet port interfaces are enabled by default. To disable an Ethernet interface, enter the `shutdown` command.

To re-enable a disabled interface, enter the `no shutdown` command.

1. Configure an Ethernet port interface from global CONFIGURATION mode.

```
interface ethernet node/slot/port[:subport]
```

2. Disable and re-enable the Ethernet port interface in INTERFACE mode.

```
shutdown
```

```
no shutdown
```

Disable Ethernet port interface

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# shutdown
```

Enable Ethernet port interface

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
```

Unified port groups

In an OS10 unified port group, all ports operate in either Ethernet or Fibre Channel mode — you cannot mix modes for ports in the same unified port group. To activate Ethernet interfaces, configure a port group to operate in Ethernet mode and specify the port speed. To activate Fibre Channel interfaces, see [Fibre Channel interfaces](#).

On the S4148U-ON switch, the available Ethernet and Fibre Channel interfaces in a port group depend on the currently configured port profile. For more information, see [S4148U-ON port profiles](#).

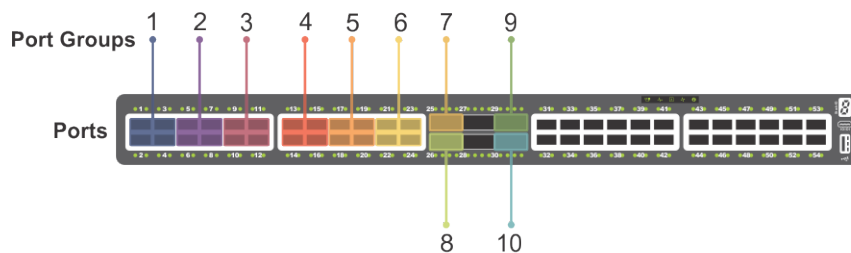


Figure 1. S4148U-ON unified port groups

To enable Ethernet interfaces in a unified port group:

1. Configure a unified port group in CONFIGURATION mode. Enter 1/1 for *node/slot*. The port-group range depends on the switch.

```
port-group node/slot/port-group
```

2. Activate the unified port group for Ethernet operation in PORT-GROUP mode. To activate a unified port group in Fibre Channel mode, see [Fibre Channel interfaces](#). The available options depend on the switch.

```
mode Eth {100g-1x | 50g-2x | 40g-1x | 25g-4x | 10g-4x}
```

- 100g-1x — Reset a port group to 100GE mode.
- 50g-2x — Split a port group into two 50GE interfaces.
- 40g-1x — Set a port group to 40GE mode for use with a QSFP+ 40GE transceiver.
- 25g-4x — Split a port group into four 25GE interfaces.
- 10g-4x — Split a port group into four 10GE interfaces.

3. Return to CONFIGURATION mode.

```
exit
```

4. Enter Ethernet Interface mode to configure other settings. Enter a single interface, a hyphen-separated range, or multiple interfaces separated by commas.

```
interface ethernet node/slot/port[:subport]
```

Configure Ethernet unified port interface

```
OS10(config)# port-group 1/1/13
OS10(conf-pg-1/1/13)# mode Eth 25g-4x
OS10(conf-pg-1/1/13)# exit
OS10(config)# interface ethernet 1/1/43:1
OS10(conf-if-eth1/1/43:1)#
```

View Ethernet unified port interface

```
OS10(config)# interface ethernet 1/1/43:1
OS10(conf-if-eth1/1/43:1)# show configuration
!
interface ethernet1/1/43:1
no shutdown
```

L2 mode configuration

Each physical Ethernet interface uses a unique MAC address. Port-channels and VLANs use a single MAC address. By default, all the interfaces operate in L2 mode. From L2 mode, you can configure switching and L2 protocols, such as VLANs and Spanning-Tree Protocol (STP) on an interface.

You can enable L2 switching on a port interface in access or trunk mode. By default, an interface is configured in access mode. Access mode allows L2 switching of untagged traffic on a single VLAN (VLAN 1 is the default). Trunk mode enables L2 switching of untagged traffic on the access VLAN, and tagged traffic on multiple (one or more) VLANs.

By default, native VLAN of a port is the default VLAN ID of the switch. You can change the native VLAN using the `switchport access vlan vlan-id` command.

A trunk interface carries VLAN traffic that is tagged using 802.1q encapsulation. If an access interface receives a packet with an 802.1q tag in the header that is different from the access VLAN ID, it drops the packet.

By default, a trunk interface carries only untagged traffic on the access VLAN — you must manually configure other VLANs for tagged traffic.

1. Select one of the two available options:

- Configure L2 trunking in INTERFACE mode and the tagged VLAN traffic that the port can transmit. By default, a trunk port is not added to any tagged VLAN. You must create a VLAN before you can assign the interface to it.

```
switchport mode trunk
switchport trunk allowed vlan vlan-id-list
```

- Reconfigure the access VLAN assigned to a L2 access or trunk port in INTERFACE mode.

```
switchport access vlan vlan-id
```

2. Enable the interface for L2 traffic transmission in INTERFACE mode.

```
no shutdown
```

L2 interface configuration

```
OS10(config)# interface ethernet 1/1/7
OS10(conf-if-eth1/1/7)# switchport mode trunk
OS10(conf-if-eth1/1/7)# switchport trunk allowed vlan 5,10
OS10(conf-if-eth1/1/7)# no shutdown
```

L3 mode configuration

Ethernet and port-channel interfaces are in L2 access mode by default. When you disable L2 mode and then assign an IP address to an Ethernet port interface, you place the port in L3 mode.

Configure one primary IP address in L3 mode. You can configure up to 255 secondary IP addresses on an interface. At least one interface in the system must be in L3 mode before you configure or enter a L3 protocol mode, such as OSPF.

1. Remove a port from L2 switching in INTERFACE mode.

```
no switchport
```

2. Configure L3 routing in INTERFACE mode. Add the keyword `secondary` to configure backup IP addresses.

```
ip address address [secondary]
```

3. Enable the interface for L3 traffic transmission in INTERFACE mode.

```
no shutdown
```

L3 interface configuration

```
OS10(config)# interface ethernet 1/1/9
OS10(conf-if-eth1/1/9)# no switchport
OS10(conf-if-eth1/1/9)# ip address 10.10.1.92/24
OS10(conf-if-eth1/1/9)# no shutdown
```

View L3 configuration error

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip address 1.1.1.1/24
% Error: remove Layer 2 configuration before assigning an IP
```

Fibre Channel interfaces

OS10 unified port groups support Fibre Channel (FC) interfaces. A unified port group operates in Fibre Channel or Ethernet mode. To activate FC interfaces, configure a port group to operate in Fibre Channel mode and specify the port speed. By default, FC interfaces are disabled. To enable an FC interface for data transmission, enter the `no shutdown` command.

On a S4148U-ON, FC interfaces are available in all port groups. The activated FC interfaces depend on the currently configured port profile. For more information, see [S4148U-ON port profiles](#).

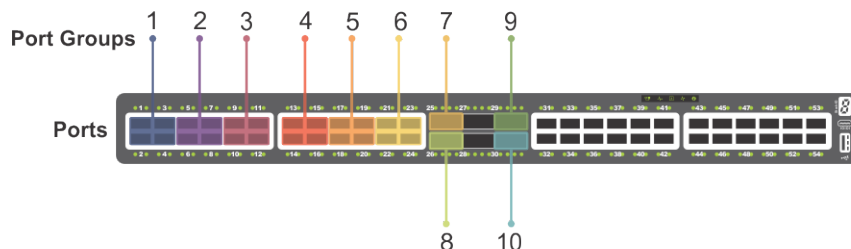


Figure 2. S4148U-ON unified port groups

To enable a Fibre Channel interface:

1. Configure a unified port group in CONFIGURATION mode. Enter 1/1 for *node/slot*. The port-group range depends on the switch.

```
port-group node/slot/port-group
```

2. Activate the unified port group for FC operation in PORT-GROUP mode. The available FC modes depend on the switch.

```
mode fc {32g-2x | 32g-1x | 16g-4x | 16g-2x | 8g-4x}
```

- 8g-4x — Split a unified port group into four 8 GFC interfaces.
- 16g-2x — Split a unified port group into two 16 GFC interfaces.
- 16g-4x — Split a unified port group into four 16 GFC interfaces; supports 4x32GFC oversubscription.
- 32g-1x — Split a unified port group into one 32 GFC interface.
- 32g-2x — Split a unified port group into two 32 GFC interfaces.

3. Return to CONFIGURATION mode.

```
exit
```

4. Enter FC Interface mode to enable data transmission. Enter a single interface, a hyphen-separated range, or multiple interfaces separated by commas.

```
interface fibrechannel node/slot/port[:subport]
```

5. (Optional) Reconfigure the interface speed for oversubscription in INTERFACE mode. Oversubscription allows a port to operate faster for bursty storage traffic.

```
speed {8 | 16 | 32 | auto}
```

6. Enable the FC interface in INTERFACE mode.

```
no shutdown
```

Configure FC interface

```
OS10(config)# port-group 1/1/13
OS10(conf-pg-1/1/13)# mode FC 16g-4x
OS10(conf-pg-1/1/13)# exit
OS10(config)# interface fibrechannel 1/1/43:1
OS10(conf-if-fc-1/1/43:1)# speed 32
OS10(conf-if-fc-1/1/43:1)# no shutdown
```

View FC interface

```
OS10(config)# interface fibrechannel 1/1/43:1
OS10(conf-if-fc-1/1/43:1)# show configuration
!
interface fibrechannel1/1/43:1
  no shutdown
  speed 32
  vfabric 100
```

```
OS10# show interface fibrechannel 1/1/43:1
Fibrechannel 1/1/43:1 is up, FC link is up
Address is 14:18:77:20:8d:fc, Current address is 14:18:77:20:8d:fc
Pluggable media present, QSFP-PLUS type is QSFPPLUS_4X16_16GBASE_FC_SW
  Wavelength is 850
  Receive power reading is 0.0
FC MTU 2188 bytes
LineSpeed 8G
Port type is F, Max BB credit is 1
WWN is 20:78:14:18:77:20:8d:cf
Last clearing of "show interface" counters: 00:02:32
Input statistics:
  33 frames, 3508 bytes
  0 class 2 good frames, 33 class 3 good frames
  0 frame too long, 0 frame truncated, 0 CRC
  1 link fail, 0 sync loss
  0 primitive seq err, 0 LIP count
  0 BB credit 0, 0 BB credit 0 packet drops
Output statistics:
  33 frames, 2344 bytes
  0 class 2 frames, 33 class 3 frames
  0 BB credit 0, 0 oversize frames
6356027325 total errors
Rate Info:
  Input 116 bytes/sec, 1 frames/sec, 0% of line rate
  Output 78 bytes/sec, 1 frames/sec, 0% of line rate
Time since last interface status change: 00:00:24
```

Management interface

The Management interface provides OOB management access to the network device. You can configure the Management interface, but the configuration options on this interface are limited. You cannot configure gateway addresses and IP addresses if it appears in the main routing table, and proxy ARP is not supported on this interface.

1. Configure the Management interface in CONFIGURATION mode.

```
interface mgmt 1/1/1
```

2. By default, DHCP client is enabled on the Management interface. Disable the DHCP client operations in INTERFACE mode.

```
no ip address dhcp
```

3. Configure an IP address and mask on the Management interface in INTERFACE mode.

```
ip address A.B.C.D/prefix-length
```

4. Enable the Management interface in INTERFACE mode.

```
no shutdown
```

Configure management interface

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# no ip address dhcp
OS10(conf-if-ma-1/1/1)# ip address 10.1.1.10/24
OS10(conf-if-ma-1/1/1)# no shutdown
```


VLAN interfaces

VLANs are logical interfaces and are, by default, in L2 mode. Physical interfaces and port-channels can be members of VLANs.

OS10 supports inter-VLAN routing. You can add IP addresses to VLANs and use them in routing protocols in the same manner that physical interfaces are used.

When using VLANs in a routing protocol, you must configure the `no shutdown` command to enable the VLAN for routing traffic. In VLANs, the `shutdown` command prevents L3 traffic from passing through the interface — L2 traffic is unaffected by this command.

- Configure an IP address in A.B.C.D/x format on the interface in INTERFACE mode. The secondary IP address is the interface's backup IP address.

```
ip address ip-address/mask [secondary]
```

Configure VLAN

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# ip address 1.1.1.2/24
```

You cannot simultaneously use egress rate shaping and ingress rate policing on the same VLAN.

User-configured default VLAN

By default, VLAN 1 serves as the default VLAN for switching untagged L2 traffic on OS10 ports in trunk or access mode. The default VLAN is used for untagged protocol traffic sent and received between switches, such as STPs. If VLAN 1 is used for data traffic for network-specific needs, reconfigure the VLAN ID of the default VLAN.

- Assign a new VLAN ID to the default VLAN in CONFIGURATION mode (1 to 4093).

```
default vlan-id vlan-id
```

In the `show vlan` output, an asterisk (*) indicates the default VLAN.

Reconfigure default VLAN

```
OS10# show vlan
Q: A - Access (Untagged), T - Tagged
  NUM      Status      Description                               Q Ports
*  1        up
Eth1/1/1-1/1/25,1/1/29,1/1/31-1/1/54

OS10(config)# interface vlan 10
Sep 19 17:28:10 OS10 dn_ifm[932]: Node.1-Unit.1:PRI:notice [os10:notify],
%Dell EMC (OS10) %IFM_ASTATE_UP: Interface admin state up :vlan10
OS10(conf-if-vl-10)# exit

OS10(config)# default vlan-id 10
Sep 19 17:28:15 OS10 dn_ifm[932]: Node.1-Unit.1:PRI:notice [os10:trap], %Dell EMC (OS10)
%IFM_OSTATE_DN: Interface operational state is down :vlan1
Sep 19 17:28:16 OS10 dn_ifm[932]: Node.1-Unit.1:PRI:notice [os10:trap], %Dell EMC (OS10)
%IFM_OSTATE_UP: Interface operational state is up :vlan10

OS10(config)# do show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs
Q: A - Access (Untagged), T - Tagged
  NUM      Status      Description                               Q Ports
  1        down
*  10       up
Eth1/1/1-1/1/25,1/1/29,1/1/31-1/1/54
```

VLAN scale profile

When you scale the number of VLANs on a switch, use the VLAN scale profile so that less memory is consumed. Enable the scale profile before you configure VLANs on the switch. The scale profile globally applies L2 mode on all VLANs you create and disables L3 transmission. To enable L3 routing traffic on a VLAN, use the `mode L3` command.

1. Configure the L2 VLAN scale profile in CONFIGURATION mode.

```
scale-profile vlan
```

2. (Optional) Enable L3 routing on a VLAN in INTERFACE VLAN mode.

```
mode L3
```

After you upgrade OS10 from an earlier version with configured VLANs, if you configure the VLAN scale profile and enable L3 routing on VLANs, save the configuration and reload the switch to apply the scale profile settings.

Apply VLAN scale profile

```
OS10(config)# scale-profile vlan
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# mode L3
```

Loopback interfaces

A loopback interface is a virtual interface in which the software emulates an interface. Because a loopback interface is not associated to physical hardware entities, the loopback interface status is not affected by hardware status changes.

Packets routed to a loopback interface are processed locally to the OS10 device. Because this interface is not a physical interface, you can configure routing protocols on this interface to provide protocol stability. You can place loopback interfaces in default L3 mode.

- Enter the loopback interface number in CONFIGURATION mode (0 to 16383).

```
interface loopback number
```

- Enter the loopback interface number to view the configuration in EXEC mode.

```
show interface loopback number
```

- Enter the loopback interface number to delete a loopback interface in CONFIGURATION mode.

```
no interface loopback number
```

View loopback interface

```
OS10# show interface loopback 4
Loopback 4 is up, line protocol is up
Hardware is unknown.
Interface index is 102863300
Internet address is 120.120.120.120/24
Mode of IPv4 Address Assignment : MANUAL
MTU 1532 bytes
Flowcontrol rx false tx false
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters : 00:00:11
Queuing strategy : fifo
  Input 0 packets, 0 bytes, 0 multicast
  Received 0 errors, 0 discarded
  Output 0 packets, 0 bytes, 0 multicast
  Output 0 errors, Output 0 invalid protocol
Time since last interface status change : 00:00:11
```

Port-channel interfaces

Port-channels are not configured by default. Link aggregation is a method of grouping multiple physical interfaces into a single logical interface — a link aggregation group (LAG) or port -channel. A port-channel aggregates the bandwidth of member links, provides redundancy, and load balances traffic. If a member port fails, the OS10 device redirects traffic to the remaining ports.

A physical interface can belong to only one port-channel at a time, and a port-channel must contain interfaces of the same interface type and speed. OS10 supports up to 128 port-channels, with up to 32 ports per channel.

To configure a port-channel, use the same configuration commands as for Ethernet port interfaces. Port-channels are transparent to network configurations and managed as a single interface. For example, configure one IP address for the group, and use the IP address for all routed traffic on the port-channel.

By configuring port channels, you can create larger capacity interfaces by aggregating a group of lower speed links. For example, you can build a 40G interface by aggregating four 10G Ethernet interfaces together — if one of the four interfaces fails, traffic is redistributed across the three remaining interfaces.

Static Port-channels are statically configured.

Dynamic Port-channels are dynamically configured using Link Aggregation Control Protocol (LACP).

Member ports of a LAG are added and programmed into the hardware in a predictable order based on the port ID, instead of in the order in which the ports come up. Load balancing yields predictable results across resets and reloads.

Create port-channel

You can create up to 128 port-channels, with up to 32 port members per group. Configure a port-channel similarly to a physical interface — you can enable or configure protocols, or assign access control lists (ACLs) to a port channel. After you enable the port-channel, you can place it in L2 or L3 mode.

To place the port-channel in L2 mode or configure an IP address to place the port-channel in L3 mode, use the `switchport` command.

1. Create a port-channel in CONFIGURATION mode.

```
interface port-channel id-number
```

2. Ensure that the port-channel is active in PORT-CHANNEL mode.

```
no shutdown
```

Create port-channel

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# no shutdown
```

Add port member

When you add an interface to a port-channel:

- The administrative status is applied to the port-channel.
- The port-channel configuration is applied to the member interfaces.
- A port-channel operates in either L2 (default) or L3 mode. To place a port-channel in L2 mode, use the `switchport mode` command. To place a port-channel in L3 mode and remove L2 configuration before you configure an IP address, use the `no switchport` command.
- All interfaces should have the same speed.
- An interface should not contain any non-default L2/L3 configuration settings — only the `description` and `shutdown` or `no shutdown` commands are supported. You cannot add an IP address or a static MAC address to a member interface.
- You cannot enable flow control on a port-channel interface — flow control is supported on physical interfaces that are port-channel members.
- Port-channels support LACP (802.3ad). LACP identifies similarly configured links and dynamically groups ports into a logical channel. LACP activates the maximum number of compatible ports that the switch supports in a port-channel.

If you globally disable spanning-tree operation, L2 interfaces that are LACP-enabled port-channel members may flap due to packet loops.

Add port member — static LAG

A static port-channel (LAG) contains member interfaces that you manually assign using the `channel-group mode on` command.

```
OS10(config)# interface port-channel 10
Aug 24 4:5:38: %Node.1-Unit.1:PRI:OS10 %dn_ifm
%log-notice:IFM_ASTATE_UP: Interface admin_state up.:port-channel10
Aug 24 4:5:38: %Node.1-Unit.1:PRI:OS10 %dn_ifm
%log-notice:IFM_OSTATE_DN: Interface operational state is down.:port-channel10
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# channel-group 10 mode on
Aug 24 4:5:56: %Node.1-Unit.1:PRI:OS10 %dn_ifm
%log-notice:IFM_OSTATE_UP: Interface operational state is up.:port-channel10
```

Add port member — dynamic LACP

LACP enables ports to be dynamically bundled as members of a port-channel. To configure a port for LACP operation, use the `channel-group mode {active|passive}` command. Active and passive modes allow LACP to negotiate between ports to determine if they can form a port-channel based on their configuration settings.

```
OS10(config)# interface port-channel 100
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# channel-group 100 mode active
```

Minimum links

Configure minimum links in a port-channel (LAG) that must be in *oper up* status to consider the port-channel to be in *oper up* status.

- Enter the number of links in a LAG that must be in *oper up* status in PORT-CHANNEL mode (1 to 32, default 1).

```
minimum-links number
```

Configure minimum operationally up links

```
OS10(config)# interface po 1
OS10(conf-if-po-1)# minimum-links 5
```

Assign Port Channel IP Address

You can assign an IP address to a port channel and use port channels in L3 routing protocols.

- Configure an IP address and mask on the interface in INTERFACE PORT-CHANNEL mode.
 - `ip address ip-address mask [secondary-ip-address]`
 - `ip-address mask` — Specify an IP address in dotted-decimal format (A.B.C.D) and the mask in slash format.
 - `secondary-ip-address` — Specify a secondary IP address in dotted-decimal format (A.B.C.D), which will act as the interface's backup IP address.

Assign Port Channel IP Address

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# ip address 1.1.1.1/24
OS10(conf-if-po-1)#
```

Remove or disable port-channel

You can delete or disable a port-channel.

1. Delete a port-channel in CONFIGURATION mode.

```
no interface port-channel channel-number
```

2. Disable a port-channel to place all interfaces within the port-channel operationally down in CONFIGURATION mode.

```
shutdown
```

Delete port-channel

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# no interface port-channel 10
```

Load balance traffic

You can use hashing to load balance traffic across the member interfaces of a port-channel. Load balancing uses source and destination packet information to distribute traffic over multiple interfaces when transferring data to a destination.

For packets without an L3 header, OS10 automatically uses the `load-balancing mac-selection destination-mac` command for hash algorithms by default.

When you configure an IP and MAC hashing scheme at the same time, the MAC hashing scheme takes precedence over the IP hashing scheme.

- Select one or more methods of load balancing and replace the default IP 4-tuple method of balancing traffic over a port-channel in CONFIGURATION mode.

```
OS10(config)# load-balancing
  ingress-port      Ingress port configurations
  tcp-udp-selection TCP-UDP port for load-balancing configurations
  ip-selection      IPV4 load-balancing configurations
  ipv6-selection    IPV6 load-balancing configurations
  mac-selection     MAC load-balancing configurations
```

- `ingress-port [enable]` — Enables the ingress port configuration. This option is not supported on S5148F-ON.
- `tcp-udp-selection [l4-destination-port | l4-source-port]` — Uses the Layer 4 destination IP address, or Layer 4 source IP address in the hash calculation. This option is not supported on S5148F-ON.
- `ip-selection [destination-ip | source-ip | protocol | vlan-id | l4-destination-port | l4-source-port]` — Uses the destination IP address, source IP address, protocol, VLAN ID, Layer 4 destination IP address, or Layer 4 source IP address in the hash calculation.
- `ipv6-selection [destination-ip | source-ip | protocol | vlan-id | l4-destination-port | l4-source-port]` — Uses the destination IPv6 address, source IPv6 address, protocol, VLAN ID, Layer 4 destination IPv6 address, or Layer 4 source IPv6 address in the hash calculation.
- `mac-selection [destination-mac | source-mac] [ethertype | vlan-id]` — Uses the destination MAC address or source MAC address, and ethertype, or VLAN ID in the hash calculation.

Configure load balancing

```
OS10(config)# load-balancing ip-selection destination-ip source-ip
```

Change hash algorithm

The `load-balancing` command selects the hash criteria applied to load balancing of traffic on port-channels. If you do not obtain even traffic distribution, use the `hash-algorithm` command to select the hash scheme for LAG. Rotate or shift the L2-bit LAG hash until the desired traffic distribution is achieved.

- Change the default (0) to another algorithm and apply it to LAG hashing in CONFIGURATION mode.

```
hash-algorithm lag crc
```

Change hash algorithm

```
OS10(config)# hash-algorithm lag crc
```

Configure interface ranges

Bulk interface configuration allows you apply the same configuration to multiple interfaces - either physical or logical, or to display their current configuration. You can also create multiple logical interfaces in bulk. An interface range is a set of interfaces to which you can apply the same command.

You can use interface ranges for:

- Ethernet physical interfaces
- Port channels
- VLAN interfaces

Bulk configuration excludes any non-existing interfaces in an interface range from the configuration. You can configure a default VLAN only if the interface range being configured consists of only VLAN ports.

The `interface range` command allows you to create an interface range allowing other commands to be applied to that range of interfaces.

Configure range of Ethernet addresses and enable them

```
OS10(config)# interface range ethernet 1/1/1-1/1/5
OS10(conf-range-eth1/1/1-1/1/5)# no shutdown
```

View the configuration

```
OS10(conf-range-eth1/1/1-1/1/5)# show configuration
!
interface ethernet1/1/1
  no shutdown
  switchport access vlan 1
!
interface ethernet1/1/2
  no shutdown
  switchport access vlan 1
!
interface ethernet1/1/3
  no shutdown
  switchport access vlan 1
!
interface ethernet1/1/4
  no shutdown
  switchport access vlan 1
!
interface ethernet1/1/5
  no shutdown
  switchport access vlan 1
```

Configure range of VLANs

```
OS10(config)# interface range vlan 1-100
OS10(conf-range-vl-1-100)#
```

Configure range of port channels

```
OS10(config)# interface range port-channel 1-25
OS10(conf-range-po-1-25)#
```

Switch-port profiles

A port profile determines the enabled front-panel ports and supported breakout modes on Ethernet and unified ports. Change the port profile on a switch to customize uplink and unified port operation, and the availability of front-panel data ports.

To change the port profile at the next reboot, enter the `switch-port-profile` command with the desired profile, save it to the startup configuration, and reload the switch.

1. Configure a platform-specific port profile in CONFIGURATION mode. For a standalone switch, enter 1/1 for node/unit.

```
switch-port-profile node/unit profile
```

2. Save the port profile change to the startup configuration in EXEC mode.

```
write memory
```

3. Reload the switch in EXEC mode.

```
reload
```

The switch reboots with the new port configuration and resets the system defaults, except for the switch-port profile and these configured settings:

- Management interface 1/1/1 configuration
- Management IPv4/IPv6 static routes
- System hostname
- Unified Forwarding Table (UFT) mode
- ECMP maximum paths

You must manually reconfigure other settings on a switch after you apply a new port profile and reload the switch.

NOTE: After you change the switch-port profile, do not immediately back up and restore the startup file without entering `write memory` and reloading the switch. Otherwise, the new profile does not take effect.

Configure port profile

```
OS10(config)# switch-port-profile 1/1 profile-6
OS10(config)# exit
OS10# write memory
OS10# reload
```

Verify port profile

```
OS10(config)# show switch-port-profile 1/1

| Node/Unit | Current      | Next-boot   | Default     |
|-----+-----+-----+-----+
| 1/1      | profile-2   | profile-2   | profile-1   |

Supported Profiles:
profile-1
profile-2
profile-3
profile-4
profile-5
profile-6
```

S4148-ON series port profiles

On the S4148-ON series, port profiles determine the available front-panel Ethernet ports and supported breakout interfaces on uplink ports. In the port profile illustration, blue boxes indicate the supported ports and breakout interfaces. Blank spaces indicate ports and speeds that are not available.

- 10GE mode is an SFP+ 10GE port or a 4x10G breakout of a QSFP+ or QSFP28 port.
- 25GE is a 4x25G breakout of a QSFP28 port.
- 40GE mode is a QSFP+ port or a QSFP28 port that supports QSFP+ 40GE transceivers.
- 50GE is a 2x50G breakout of a QSFP28 port.

- 100GE mode is a QSFP28 port.

NOTE: For S4148U-ON port profiles with both unified and Ethernet ports, see [S4148U-ON port profiles](#). An S4148U-ON unified port supports Fibre Channel and Ethernet modes.

For example, `profile-1` enables 10G speed on forty-eight ports (1-24 and 31-54), and 4x10G breakouts on QSFP28 ports 25-26 and 29-30; QSFP+ ports 27 and 28 are deactivated. `profile-3` enables 10G speed on forty ports, and 4x10G breakouts on all QSFP28 and QSFP+ ports. Similarly, `profile-1` disables 40G speed on ports 25-30; `profile-3` enables 40G on these ports. See [switch-port-profile](#) for a detailed description.

Profile	Port Modes	SFP+				SFP+				SFP+				SFP+				SFP+				QSFP28				QSFP28				QSFP+				QSFP+				QSFP28				QSFP28				SFP+				SFP+				SFP+				SFP+			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54						
Profile-1 (default)	1GE/10GE	[Blue]																																																											
	25GE	[Blue]																																																											
	40GE	[Blue]																																																											
	100GE	[Blue]																																																											
Profile-2	1GE/10GE	[Blue]																																																											
	25GE	[Blue]																																																											
	40GE	[Blue]																																																											
	100GE	[Blue]																																																											
Profile-3	1GE/10GE	[Blue]																																																											
	25GE	[Blue]																																																											
	40GE	[Blue]																																																											
	100GE	[Blue]																																																											
Profile-4	1GE/10GE	[Blue]																																																											
	25GE	[Blue]																																																											
	40GE	[Blue]																																																											
	100GE	[Blue]																																																											
Profile-5	1GE/10GE	[Blue]																																																											
	25GE	[Blue]																																																											
	40GE	[Blue]																																																											
	100GE	[Blue]																																																											
Profile-6	1GE/10GE	[Blue]																																																											
	25GE	[Blue]																																																											
	40GE	[Blue]																																																											
	100GE	[Blue]																																																											

1GE mode: 1GE is supported only on SFP+ ports; 1GE is not supported on QSFP+ and QSFP28 ports 25-26.

Breakout interfaces: Use the `interface breakout` command in Configuration mode to configure 4x10G, 4x25G, and 2x50G breakout interfaces.

S4148U-ON port profiles

S4148U-ON port profiles determine the available front-panel unified and Ethernet ports and supported breakout interfaces. In the port profile illustration, blue boxes indicate the supported Ethernet port modes and breakout interfaces. Brown boxes indicate the supported Fibre Channel port modes and breakout interfaces. Blank spaces indicate ports and speeds that are not available. Unified port groups are numbered 1–10.

S4148U-ON unified port modes—SFP+ ports 1-24 and QSFP28 ports 25-26 and 29-30:

- 10GE is an SFP+ port in Ethernet mode or a 4x10G breakout of a QSFP+ or QSFP28 port in Ethernet mode.
- 25GE is a 4x25G breakout of a QSFP28 Ethernet port.
- 40GE is a QSFP+ or QSFP28 Ethernet port that uses QSFP+ 40GE transceivers.
- 50GE is a 2x50G breakout of a QSFP28 Ethernet port.
- 100GE is a QSFP28 Ethernet port.
- 4x8GFC are breakout interfaces in an SFP+ or QSFP28 FC port group.
- 2x16GFC are breakout interfaces (subports 1 and 3) in an SFP+ or QSFP28 FC port group.
- 4x16GFC are breakout interfaces in a QSFP28 FC port group.
- 1x32GFC (subport 1) are breakout interfaces in a QSFP28 FC port group.

S4148U-ON Ethernet modes—QSFP+ ports 27-28 and SFP+ ports 31-54:

- 10GE mode is an SFP+ 10GE port or a 4x10G breakout of a QSFP+ port.
- 40GE mode is a QSFP+ port.

For example, all S4148U-ON activate support 10G speed on unified ports 1-24 and Ethernet ports 31-54, but only `profile-1` and `profile-2` activate QSFP+ ports 27-28 in 40GE mode with 4x10G breakouts. Similarly, all S4148U-ON profiles activate 8GFC speed on unified ports 1-24, but only `profile-1`, `profile-2`, and `profile-3` activate 2x16GFC in port groups 1-6. In QSFP28 port groups, `profile-1` and `profile-2` support 1x32GFC; `profile-3` and `profile-4` support 4x16GFC.

Unified Port Group	SFP+	SFP+	SFP+	SFP+	SFP+	SFP+	QSFP28	QSFP28	QSFP+	QSFP+	QSFP28	QSFP28	SFP+	SFP+	SFP+	SFP+	SFP+	SFP+																																							
Port Number	1	2	3	4	5	6	7	8			9	10																																													
Uplink Port Breakouts	1 2 3 4				5 6 7 8				9 10 11 12				13 14 15 16				17 18 19 20				21 22 23 24				25 26 27 28				29 30 31 32				33 34 35 36				37 38 39 40				41 42 43 44				45 46 47 48				49 50 51 52				53 54 55 56				
Profile	Port Modes																																																								
Profile-1 (default)	1GE/10GE	[Active]																																																							
	25GE	[Active]																																																							
	40GE	[Active]																																																							
	50GE	[Active]																																																							
	100GE	[Active]																																																							
Profile-2*	4x8GFC**	[Active]																																																							
	2x16GFC**	[Active]																																																							
	4x16GFC**	[Active]																																																							
	1x32GFC	[Active]																																																							
	2x32GFC	[Active]																																																							
Profile-3	1GE/10GE	[Active]																																																							
	25GE	[Active]																																																							
	40GE	[Active]																																																							
	50GE	[Active]																																																							
	100GE	[Active]																																																							
Profile-4	4x8GFC**	[Active]																																																							
	2x16GFC**	[Active]																																																							
	4x16GFC**	[Active]																																																							
	1x32GFC	[Active]																																																							
	2x32GFC	[Active]																																																							

*profile-1 and profile-2 activate the same port mode capability on unified and Ethernet ports. The difference is that in profile-1, by default SFP+ unified ports 1-24 come up in Fibre Channel mode with 2x16GFC breakouts per port group. In profile-2, by default SFP+ unified ports 1-24 come up in Ethernet 10GE mode. profile-1 allows you to connect FC devices for plug-and-play; profile-2 is designed for a standard Ethernet-based data network.

****Oversubscription:** Configure oversubscription to support bursty storage traffic on a Fibre Channel interface. Oversubscription allows a port to operate faster, but may result in traffic loss. To support oversubscription, use the `speed` command in Interface configuration mode. This command is not supported on an Ethernet interface. In S4148U-ON port profiles:

- SFP+ and QSFP28 port groups in 4x8GFC mode support 16GFC oversubscription on member interfaces.
- QSFP28 ports in 2x16GFC mode support 32GFC oversubscription. SFP+ port groups in 2x16GFC mode do not support 32GFC oversubscription. 2x16GFC mode activates subports 1 and 3.
- QSFP28 ports in 4x16GFC mode support 32GFC oversubscription.

Breakout interfaces:

- To configure breakout interfaces on a unified port, use the `mode {FC | Eth}` command in Port-Group configuration mode. The `mode {FC | Eth}` command configures a unified port to operate at line rate and guarantees no traffic loss.
- To configure breakout interfaces on a QSFP+ Ethernet port, use the `interface breakout` command in global Configuration mode.

1GE mode: Only SFP+ ports support 1GE; QSFP+ and QSFP28 ports 25-30 do not support 1GE.

Configure breakout mode

Using a supported breakout cable, you can split a 40GE QSFP+ or 100GE QSFP28 Ethernet port into separate breakout interfaces. All breakout interfaces have the same speed. You can set a QSFP28 port to operate in 40GE mode with a QSFP+ transceiver.

```
interface breakout node/slot/port map {10g-4x | 25g-4x | 40g-1x | 50g-2x | 100g-1x}
```

- `node/slot/port` — Enter the physical port information.
- `10g-4x` — Split a QSFP28 or QSFP+ port into four 10G interfaces
- `25g-4x` — Split a QSFP28 port into four 25G interfaces.
- `40g-1x` — Set a QSFP28 port for use with a QSFP+ 40G transceiver.
- `50g-2x` — Split a QSFP28 port into two 50G interfaces.
- `100g-1x` — Reset a QSFP28 port to 100G speed.

To configure an Ethernet breakout interface, enter the `interface ethernet node/slot/port:subport` command in CONFIGURATION mode.

Each breakout interface operates at the configured speed. Enter the `no` version of the `interface breakout` command to reset a port to its default speed — 40G or 100G.

To configure breakout interfaces on a unified port, enter the `mode {Eth | FC}` command in Port-Group Configuration mode.

Configure interface breakout

```
OS10(config)# interface breakout 1/1/7 map 10g-4x
```

Display interface breakout

```
OS10# show interface status
```

Port	Description	Status	Speed	Duplex	Mode	Vlan	Tagged-Vlans
Eth 1/1/1		down	0	auto	-		
Eth 1/1/2		down	0	auto	A	1	-
Eth 1/1/7:1		down	0	auto	A	1	-
Eth 1/1/7:2		down	0	auto	A	1	-
Eth 1/1/7:3		down	0	auto	A	1	-
Eth 1/1/7:4		down	0	auto	A	1	-
Eth 1/1/25		down	0	auto	A	1	-

Breakout auto-configuration

You can globally enable front-panel Ethernet ports to automatically detect SFP pluggable media in a QSFP+ or QSFP28 port. The port autoconfigures breakout interfaces for media type and speed. For example, if you plug a 40G DAC cable with 4x10G far-side transceivers into a QSFP28 port, the port autoconfigures in 10g-4x Interface-breakout mode.

RJ-45 ports and ports that are members of a port group do not support breakout auto-configuration. The breakout auto-configuration feature is disabled by default.

Enable breakout auto-configuration

```
OS10(config)# feature auto-breakout
```

Display breakout auto-configuration

Before you plug a cable in Ethernet port 1/1/25:

```
OS10# show interface status
```

Port	Description	Status	Speed	Duplex	Mode	Vlan	Tagged-Vlans
Eth 1/1/1		down	0	auto	-		
Eth 1/1/2		down	0	auto	A	1	-
Eth 1/1/25		down	0	auto	A	1	-
Eth 1/1/29		down	0	auto	A	1	-

After you enter `feature auto-breakout` and plug a breakout cable in Ethernet port 1/1/25:

```
OS10# show interface status
```


Port	Description	Status	Speed	Duplex	Mode	Vlan	Tagged-Vlans
Eth 1/1/1		down	0	auto	-		
Eth 1/1/2		down	0	auto	A	1	-
Eth 1/1/25:1		down	0	auto	A	1	-
Eth 1/1/25:2		down	0	auto	A	1	-
Eth 1/1/25:3		down	0	auto	A	1	-
Eth 1/1/25:4		down	0	auto	A	1	-
Eth 1/1/29		down	0	auto	A	1	-

Forward error correction

Forward error correction (FEC) is used to enhance data reliability.

FEC modes supported in OS10:

- CL74-FC — Supports 25G
- CL91-RS — Supports 100G
- CL108-RS — Supports 25G
- off — Disables FEC

 **NOTE:** OS10 does not support FEC on 10G and 40G.

Configure FEC

```
OS10(config)# interface ethernet 1/1/41
OS10(conf-if-eth1/1/41)# fec CL91-RS
```

View FEC configuration

```
OS10# show interface ethernet 1/1/41
Ethernet 1/1/41 is up, line protocol is up
Hardware is Dell EMC Eth, address is e4:f0:04:3e:1a:06
  Current address is e4:f0:04:3e:1a:06
Pluggable media present, QSFP28 type is QSFP28_100GBASE_CR4_2M
  Wavelength is 64
  Receive power reading is
Interface index is 17306108
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Disabled
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 100G, Auto-Negotiation on
FEC is cl91-rs, Current FEC is cl91-rs
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 00:00:17
Queuing strategy: fifo
Input statistics:
  7 packets, 818 octets
  2 64-byte pkts, 0 over 64-byte pkts, 5 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  7 Multicasts, 0 Broadcasts, 0 Unicasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output statistics:
  15 packets, 1330 octets
  10 64-byte pkts, 0 over 64-byte pkts, 5 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  15 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 Collisions, 0 wred drops
Rate Info(interval 30 seconds):
  Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
  Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 00:00:13
--more--
```

Energy-efficient Ethernet

Energy-efficient Ethernet (EEE) reduces power the consumption of physical layer devices (PHYs) during idle periods. EEE allows Dell Networking devices to conform to green computing standards.

An Ethernet link consumes power when a link is idle. EEE allows for Ethernet links to use the regular power mode only during data transmission. EEE is enabled on devices that support LOW POWER IDLE (LPI) mode. Such devices can save power by entering LPI mode during periods when no data is transmitted.

In LPI mode, systems on both ends of the link saves power by shutting down certain services. EEE transitions into and out of LPI mode transparently to upper-layer protocols and applications.

EEE advertises during the auto-negotiation stage. Auto-negotiation detects abilities supported by the device at the other end of the link, determines common abilities, and configures joint operation.

Auto-negotiation performs at power-up, on command from the LAN controller, on detection of a PHY error, or following Ethernet cable re-connection. During the link establishment process, both link partners indicate their EEE capabilities. If EEE is supported by both link partners for the negotiated PHY type, the EEE function is used independently in either direction.

Changing the EEE configuration resets the interface because the device restarts Layer 1 auto-negotiation. You may want to enable Link Layer Discovery Protocol (LLDP) for devices that require longer wake-up times before they are able to accept data on their receive paths. Doing so enables the device to negotiate for extended system wake-up times from the transmitting link partner.

Enable energy-efficient Ethernet

To reduce power consumption, enable EEE. EEE is disabled by default.

1. Enter the physical Ethernet interface information in CONFIGURATION mode.

```
interface ethernet node/slot/port[:subport]
```

2. Enable EEE in INTERFACE mode.

```
eee
```

Enable EEE

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# eee
```

Disable EEE

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no eee
```

Clear interface counters

You can clear EEE counters for physical Ethernet interfaces globally or per interface.

Clear all EEE counters

```
OS10# clear counters interface eee
Clear all eee counters [confirm yes/no]:yes
```

Clear counters for specific interface

```
OS10# clear counters interface 1/1/48 eee
Clear eee counters on ethernet1/1/48 [confirm yes/no]:yes
```

View EEE status/statistics

You can view the EEE status or statistics for a specified interface, or all interfaces, using show commands.

View EEE status for a specified interface

```
OS10# show interface ethernet 1/1/48 eee
```

Port	EEE	Status	Speed	Duplex
Eth 1/1/48	on	up	1000M	

View EEE status on all interfaces

```
OS10# show interface eee
```

Port	EEE	Status	Speed	Duplex
------	-----	--------	-------	--------

```

Eth 1/1/1      off up      1000M
...
Eth 1/1/47    on  up      1000M
Eth 1/1/48    on  up      1000M
Eth 1/1/49    n/a
Eth 1/1/50    n/a
Eth 1/1/51    n/a
Eth 1/1/52    n/a

```

View EEE statistics for a specified interface

```

OS10# show interface ethernet 1/1/48 eee statistics
Eth 1/1/48
  EEE           : on
  TxIdleTime(us) : 2560
  TxWakeTime(us) : 5
  Last Clearing  : 18:45:53
  TxEventCount   : 0
  TxDuration(us) : 0
  RxEventCount   : 0
  RxDuration(us) : 0

```

View EEE statistics on all interfaces

```

OS10# show interface eee statistics

```

Port	EEE	TxEventCount	TxDuration(us)	RxEventCount	RxDuration(us)
Eth 1/1/1	off	0	0	0	0
...					
Eth 1/1/47	on	0	0	0	0
Eth 1/1/48	on	0	0	0	0
Eth 1/1/49	n/a				
...					
Eth 1/1/52	n/a				

EEE commands

clear counters interface eee

Clears all EEE counters.

Syntax `clear counters interface eee`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information Use this command to clear all EEE counters.

Example

```

OS10# clear counters interface eee
Clear all eee counters [confirm yes/no]:yes

```

Supported Releases 10.3.0E or later

clear counters interface ethernet eee

Clears EEE counters on a specified interface.

Syntax `clear counters interface ethernet node/slot/port[:subport] eee`

Parameters node/slot/port[:subport]—Enter the interface information.

Default Not configured

Command Mode EXEC

Usage Information Use this command to clear EEE counters on a specified Ethernet interface.

Example

```
OS10# clear counters interface 1/1/48 eee
Clear eee counters on ethernet1/1/48 [confirm yes/no]:yes
```

Supported Releases 10.3.0E or later

eee

Enables or disables energy-efficient Ethernet (EEE) on physical ports.

Syntax eee

Parameters None

Default Enabled on Base-T devices and disabled on S3048-ON and S4048T-ON.

Command Mode Interface

Usage Information To disable EEE, use the no version of this command.

Example (Enable EEE)

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# eee
```

Example (Disable EEE)

```
OS10(config)# interface ethernet 1/1/2
OS10(config-if-eth1/1/2)# no eee
```

Supported Releases 10.3.0E or later

show interface eee

Displays the EEE status for all interfaces.

Syntax show interface eee

Parameters None

Default Not configured

Command Mode EXEC

Example

```
OS10# show interface eee

Port          EEE  Status  Speed  Duplex
-----
Eth 1/1/1     off  up      1000M
...
Eth 1/1/47    on   up      1000M
Eth 1/1/48    on   up      1000M
Eth 1/1/49    n/a
Eth 1/1/50    n/a
Eth 1/1/51    n/a
Eth 1/1/52    n/a
```

Supported Releases 10.3.0E or later

show interface eee statistics

Displays EEE statistics for all interfaces.

Syntax `show interface eee statistics`

Parameters None

Default Not configured

Command Mode EXEC

Example

```
OS10# show interface eee statistics
Port          EEE  TxEventCount  TxDuration(us)  RxEventCount  RxDuration(us)
-----
Eth 1/1/1     off  0             0                0              0
...
Eth 1/1/47    on   0             0                0              0
Eth 1/1/48    on   0             0                0              0
Eth 1/1/49    n/a  0             0                0              0
...
Eth 1/1/52    n/a  0             0                0              0
```

Supported Releases 10.3.0E or later

show interface ethernet eee

Displays the EEE status for a specified interface.

Syntax `show interface ethernet node/slot/port[:subport] eee`

Parameters `node/slot/port[:subport]`—Enter the interface information.

Default Not configured

Command Mode EXEC

Example

```
OS10# show interface ethernet 1/1/48 eee
Port          EEE  Status  Speed  Duplex
-----
Eth 1/1/48    on   up      1000M
```

Supported Releases 10.3.0E or later

show interface ethernet eee statistics

Displays EEE statistics for a specified interface.

Syntax `show interface ethernet node/slot/port[:subport] eee statistics`

Parameters `node/slot/port[:subport]`—Enter the interface information.

Default Not configured

Command Mode EXEC

Example

```
OS10# show interface ethernet 1/1/48 eee statistics
Eth 1/1/48
  EEE                : on
  TxIdleTime(us)    : 2560
  TxWakeTime(us)    : 5
  Last Clearing     : 18:45:53
  TxEventCount      : 0
  TxDuration(us)    : 0
  RxEventCount      : 0
  RxDuration(us)    : 0
```

Supported Releases 10.3.0E or later

View interface configuration

To view basic interface information, use the `show interface`, `show running-configuration`, and `show interface status` commands. You can stop scrolling output from a `show` command by entering CTRL+C. Display information about a physical or virtual interface in EXEC mode (including up/down status, MAC and IP addresses, and input/output traffic counters).

```
show interface [type]
```

- `phy-eth node/slot/port[:subport]` — Display information about physical media connected to the interface.
- `status` — Display interface status.
- `ethernet node/slot/port[:subport]` — Display Ethernet interface information.
- `loopback id` — Display loopback interface information (0 to 16383).
- `mgmt node/slot/port` — Display Management interface information.
- `port-channel id-number` — Display port-channel interface information (1 to 128).
- `vlan vlan-id` — Display the VLAN interface information (1 to 4093).

View interface information

```
OS10# show interface
Ethernet 1/1/1 is up, line protocol is up
Hardware is Dell EMC Eth, address is 00:0c:29:98:1b:79
  Current address is 00:0c:29:98:1b:79
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
  Wavelength is 64
  SFP receive power reading is 0.0
Interface index is 16866084
Internet address is not set
Mode of IPv4 Address Assignment: not set
MTU 1532 bytes
LineSpeed 40G, Auto-Negotiation on
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 3 weeks 1 day 22:48:51
Queuing strategy: fifo
Input statistics:
  0 packets, 0 octets
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output statistics:
  0 packets, 0 octets
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
  Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
  Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
```



```
Time since last interface status change: 3 weeks 1 day 20:30:38
--more--
```

View specific interface information

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 ip address 1.1.1.1/24
 no switchport
 no shutdown
```

View candidate configuration

```
OS10(conf-if-eth1/1/1)# show configuration candidate
!
interface ethernet1/1/1
 ip address 1.1.1.1/24
 no switchport
 no shutdown
```

View running configuration

```
OS10# show running-configuration
Current Configuration ...
!
interface Ethernet 2/6
 no ip address
 shutdown
!
interface Ethernet 2/7
 no ip address
 shutdown
!
interface Ethernet 2/8
 no ip address
 shutdown
!
interface Ethernet 2/9
 no ip address
 shutdown
...
```

View L3 interfaces

```
OS10# show ip interface brief
Interface Name          IP-Address      OK      Method      Status      Protocol
=====
Ethernet 1/1/1          unassigned     YES     unset       up          up
Ethernet 1/1/2          unassigned     YES     unset       up          up
Ethernet 1/1/3          unassigned     YES     unset       up          up
Ethernet 1/1/4          unassigned     YES     unset       up          up
Ethernet 1/1/5          unassigned     YES     unset       up          up
Ethernet 1/1/6          unassigned     YES     unset       up          up
Ethernet 1/1/50:1       101.1.1.2/30   YES     manual      up          up
```

View VLAN configuration

```
OS10(config)# do show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs
Q: A - Access (Untagged), T - Tagged
  NUM      Status      Description          Q Ports
*    1      up          Eth1/1/5-1/1/8,1/1/27-1/1/28,1/1/31-1/1/54
1002      down
```

Interface commands

channel-group

Assigns an interface to a port-channel group.

Syntax `channel-group channel-number mode {active | on | passive}`

- Parameters**
- *channel-number* — Enter a port-channel number (1 to 128).
 - *mode* — Sets the LACP actor mode.
 - *active* — Sets channeling mode to active.
 - *on* — Sets channeling mode to static.
 - *passive* — Sets channeling mode to passive.

Default Not configured

Command Mode INTERFACE

Usage Information The `no` version of this command resets the value to the default, and unassigns the interface from the port-channel group.

Example

```
OS10(config)# interface ethernet 1/1/2:1
OS10(conf-if-eth1/1/2:1)# channel-group 20 mode active
```

Supported Releases 10.3.0E or later

default vlan-id

Reconfigures the VLAN ID of the default VLAN.

Syntax `default vlan-id vlan-id`

Parameters *vlan-id* — Enter the default VLAN ID number (1 to 4093).

Default VLAN 1

Command Mode CONFIGURATION

Usage Information By default, VLAN 1 serves as the default VLAN for switching untagged L2 traffic on OS10 ports in trunk or access mode. If VLAN 1 is used for data traffic for network-specific needs, reconfigure the VLAN ID of the default VLAN. The command reconfigures the access VLAN ID (default VLAN) of all ports in switchport access mode. Ensure that the VLAN ID exists before configuring it as default VLAN.

Example

```
OS10(config)# default vlan-id 10

OS10(config)# do show running-configuration
...
!
interface vlan1
no shutdown
!
interface vlan10
no shutdown
!
interface ethernet1/1/1
no shutdown
switchport access vlan 10
!
interface ethernet1/1/2
no shutdown
switchport access vlan 10
!
interface ethernet1/1/3
```

```
no shutdown
switchport access vlan 10
!
interface ethernet1/1/4
no shutdown
switchport access vlan 10
```

Supported Releases 10.4.0E(R1) or later

description (Interface)

Configures a textual description of an interface.

Syntax `description string`

Parameters `string` — Enter a text string for the interface description (up to 240 characters).

Default Not configured

Command Mode INTERFACE

Usage Information

- To use special characters as a part of the description string, enclose the string in double quotes.
- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks ("`text description`").
- Enter a text string after the `description` command to overwrite any previous text string that you previously configured as the description.
- Use the `show running-configuration interface` command to view descriptions configured for each interface.
- The `no` version of this command deletes the description.

Example

```
OS10(conf-if-eth1/1/7)# description eth1/1/7
```

Supported Releases 10.2.0E or later

duplex

Configures duplex mode on the Management port.

Syntax `duplex {full | half | auto}`

Parameters

- `full` — Specify to set the physical interface to transmit in both directions.
- `half` — Specify to set the physical interface to transmit in only one direction.
- `auto` — Specify to set the physical interface to transmit automatically.

Defaults Not configured

Command Mode CONFIGURATION

Usage Information This command can only be used on the Management port. The `no` version of this command resets the value to the default.

Example

```
OS10(conf-if-ma-1/1/1)# duplex auto
```

Supported Releases 10.3.0E or later

feature auto-breakout

Enables front-panel Ethernet ports to automatically detect SFP pluggable media and autoconfigure breakout interfaces.

Syntax	<code>feature auto-breakout</code>
Parameters	None
Default	Not configured
Command mode	CONFIGURATION
Usage information	<p>After you enter the <code>feature auto-breakout</code> command and plug a supported breakout cable in a QSFP+ or QSFP28 port, the port autoconfigures breakout interfaces for media type and speed.</p> <p>The <code>no</code> version of this command disables the auto-breakout feature. The media type plugged into a port is no longer automatically learned. Use the <code>interface breakout</code> command to manually configure breakout interfaces.</p>
Example	<pre>OS10(config)# feature auto-breakout</pre>
Supported releases	10.4.0E(R1) or later

fec

Configures Forward Error Correction on 25G and 100G interfaces.

Syntax	<code>fec {CL74-FC CL91-RS CL108-RS off}</code>
Parameters	<ul style="list-style-type: none">• <code>CL74-FC</code> — Supports 25G• <code>CL91-RS</code> — Supports 100G• <code>CL108-RS</code> — Supports 25G• <code>off</code> — Disables FEC
Defaults	<ul style="list-style-type: none">• For 25G interfaces: off• For 100G interfaces: CL91-RS
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# interface ethernet 1/1/41 OS10(conf-if-eth1/1/41)# fec CL91-RS</pre>
Supported Releases	10.3.0E or later

interface breakout

Splits a front-panel Ethernet port into multiple breakout interfaces.

Syntax	<code>interface breakout <i>node/slot/port</i> map {100g-1x 40g-1x 25g-4x 10g-4x 10g-4x 25g-4x}</code>
Parameters	<ul style="list-style-type: none">• <code>node/slot/port</code> — Enter the physical port information.• <code>100g-1x</code> — Reset a QSFP28 port to 100G speed.• <code>40g-1x</code> — Set a QSFP28 port for use with a QSFP+ 40GE transceiver.• <code>25g-4x</code> — Split a QSFP28 port into four 25GE interfaces.• <code>10g-4x</code> — Split a QSFP28 or QSFP+ port into four 10GE interfaces
Default	Not configured

Command Mode	CONFIGURATION
Usage Information	<ul style="list-style-type: none"> • Each breakout interface operates at the configured speed; for example, 10G or 25G. • The <code>no interface breakout node/slot/port</code> command resets a port to its default speed — 40G or 100G. • To configure breakout interfaces on a unified port, use the <code>mode {Eth FC}</code> command in the Port-Group configuration mode.
Example	<pre>OS10(config)# interface breakout 1/1/41 map 10g-4x</pre>
Supported Releases	10.2.2E or later

interface ethernet

Configures a physical Ethernet interface.

Syntax	<code>interface ethernet node/slot/port:subport</code>
Parameters	<code>node/slot/port:subport</code> — Enter the Ethernet interface information.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes the interface.
Example	<pre>OS10(config)# interface ethernet 1/1/10:1 OS10(conf-if-eth1/1/10:1)#</pre>
Supported Releases	10.2.0E or later

interface loopback

Configures a loopback interface.

Syntax	<code>interface loopback id</code>
Parameters	<code>id</code> — Enter the loopback interface ID number (0 to 16383).
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes the loopback interface.
Example	<pre>OS10(config)# interface loopback 100 OS10(conf-if-lo-100)#</pre>
Supported Releases	10.2.0E or later

interface mgmt

Configures the Management port.

Syntax	<code>interface mgmt node/slot/port</code>
Parameters	<code>node/slot/port</code> — Enter the physical port interface information for the Management interface.

Default	Enabled
Command Mode	CONFIGURATION
Usage Information	You cannot delete a Management port. To assign an IP address to the Management port, use the <code>ip address</code> command.
Example	<pre>OS10(config)# interface mgmt 1/1/1 OS10(conf-if-ma-1/1/1)#</pre>
Supported Releases	10.2.0E or later

interface null

Configures a null interface on the switch.

Syntax	<code>interface null <i>number</i></code>
Parameters	<i>number</i> — Enter the interface number to set as null (0).
Default	0
Command Mode	CONFIGURATION
Usage Information	You cannot delete the Null interface. The only configuration command possible in a Null interface is <code>ip unreachable</code> .
Example	<pre>OS10(config)# interface null 0 OS10(conf-if-nu-0)#</pre>
Supported Releases	10.3.0E or later

interface port-channel

Creates a port-channel interface.

Syntax	<code>interface port-channel <i>channel-id</i></code>
Parameters	<i>channel-id</i> — Enter the port-channel ID number (1 to 128).
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes the interface.
Example	<pre>OS10(config)# interface port-channel 10 OS10(conf-if-po-10)#</pre>
Supported Releases	10.2.0E or later

interface range

Configures a range of Ethernet, port-channel, or VLAN interfaces for bulk configuration.

Syntax	<code>interface range {ethernet <i>node/slot/port[:subport]-node/slot/port[:subport], [...]</i> {port-channel <i>IDnumber-IDnumber, [...]</i> vlan <i>vlanID-vlanID, [...]</i>}</code>
---------------	---

Parameters	<ul style="list-style-type: none"> • <code>node/slot/port[:subport]-node/slot/port[:subport]</code> — Enter a range of Ethernet interfaces. • <code>IDnumber-IDnumber</code> — Enter a range of port-channel numbers (1 to 128). • <code>vlanID-vlanID</code> — Enter a range VLAN ID numbers (1 to 4093).
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	<p>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.</p> <ul style="list-style-type: none"> • Bulk configuration is created if at least one interface is valid. • Non-existing interfaces are excluded from the bulk configuration with a warning message. • This command has multiple port ranges, the smaller port range is excluded from the prompt. • If you enter overlapping port ranges, the port range is extended to the smallest port and the largest end port. • You can only use VLAN and port-channel interfaces created using the <code>interface vlan</code> and <code>interface port-channel</code> commands. • You cannot create virtual interfaces (VLAN, port-channel) using the <code>interface range</code> command. • The <code>no</code> version of this command deletes the interface range.
Example	<pre>OS10(config)# interface range ethernet 1/1/7-1/1/24 OS10(conf-range-eth1/1/7-1/1/24)#</pre>
Supported Releases	10.2.0E or later

interface vlan

Creates a VLAN interface.

Syntax	<code>interface vlan <i>vlan-id</i></code>
Parameters	<code>vlan-id</code> — Enter the VLAN ID number (1 to 4093).
Default	VLAN 1
Command Mode	CONFIGURATION
Usage Information	FTP, TFTP, MAC ACLs, and SNMP operations are not supported — IP ACLs are supported on VLANs only. The <code>no</code> version of this command deletes the interface.
Example	<pre>OS10(config)# interface vlan 10 OS10(conf-if-vl-10)#</pre>
Supported Releases	10.2.0E or later

link-bundle-utilization

Configures link-bundle utilization.

Syntax	<code>link-bundle-utilization trigger-threshold <i>value</i></code>
Parameters	<code>value</code> — Enter the percentage of port-channel bandwidth that triggers traffic monitoring on port-channel members (0 to 100).
Default	Disabled
Command Mode	CONFIGURATION

Usage Information None

Example

```
OS10(config)# link-bundle-utilization trigger-threshold 10
```

Supported Releases 10.2.0E or later

mode

Configures a front-panel unified port group to operate in Fibre Channel or Ethernet mode, or a QSFP28-DD port to operate in Ethernet mode, with the specified speed on activated interfaces.

Syntax `mode {Eth {100g-2x | 100g-1x | 40g-2x | 40g-1x | 25g-8x [fabric-expander-mode] | 25g-4x | 10g-8x | 10g-4x} | FC {32g-2x | 32g-1x | 16g-4x | 16g-2x | 8g-4x}}`

- Parameters**
- `mode Eth` — Configure a port group in Ethernet mode and set the speed to:
 - `100g-2x` — Split a QSFP28-DD port into two 100GE interfaces.
 - `100g-1x` — Reset a QSFP28 port group to 100GE mode.
 - `40g-2x` — Split a port group into two 40GE interfaces.
 - `40g-1x` — Set a port group to 40G mode for use with a QSFP+ 40GE transceiver.
 - `25g-8x fabric-expander-mode` — Split a QSFP28-DD port into eight 25GE interfaces for connection to a Fabric Expander.
 - `25g-8x` — Split a port group into eight 25GE interfaces.
 - `25g-4x` — Split a port group into four 25GE interfaces.
 - `10g-8x` — Split a port group into eight 10GE interfaces.
 - `10g-4x` — Split a port group into four 10GE interfaces.
 - `mode FC` — Configure a port group in Fibre Channel mode and set the speed to:
 - `32g-2x` — Split a port group into two 32GFC interfaces, subports 1 and 3.
 - `32g-1x` — Split a port group into one 32GFC interface, subport 1.
 - `16g-4x` — Split a port group into four 16GFC interfaces; supports 4x32GFC oversubscription.
 - `16g-2x` — Split a port group into two 16GFC interfaces using ports 1 and 3.
 - `8g-4x` — Split a port group into four 8GFC interfaces.

Default S4148U-ON: Depends on the port profile activated.

Command Mode PORT-GROUP

- Usage Information**
- The `mode {FC | Eth}` command configures a port group to operate at line rate and guarantees no traffic loss.
 - The `no` version of the command resets port-group interfaces to the default Ethernet port mode/speed. Use the `no mode` command before you reset the mode on an interface.
 - To configure oversubscription on a FC interface, use the `speed` command.
 - To configure breakout interfaces on an Ethernet port, use the `interface breakout` command.
 - To view the currently active ports and subports, use the `show interfaces status` command.

Example

```
OS10(conf-pg-1/1/2)# mode FC 16g-2x
OS10(conf-pg-1/1/8)# mode Eth 10g-4x
```

Example: Reset mode

```
OS10(conf-pg-1/1/2)# mode FC 16g-2x
OS10(conf-pg-1/1/2)# no mode
OS10(conf-pg-1/1/2)# mode Eth 10g-4x
```

Supported Releases 10.3.1E or later

mode l3

After you configure the VLAN scale profile, enables L3 routing on a VLAN.

Syntax	<code>mode l3</code>
Parameters	None
Defaults	Not configured
Command Mode	INTERFACE VLAN
Usage Information	To configure the VLAN scale profile, use the <code>scale-profile vlan</code> command. The scale profile globally applies L2 mode on all VLANs you create and disables L3 transmission. To enable L3 routing traffic on a VLAN, use the <code>mode l3</code> command.
Example	<pre>OS10(config)# interface vlan 10 OS10(conf-if-vl-10)# mode l3</pre>
Supported Releases	10.4.0E(X2) or later

mtu

Sets the link maximum transmission unit (MTU) frame size for an Ethernet L2 or L3 interface.

Syntax	<code>mtu value</code>
Parameters	<i>value</i> — Enter the maximum frame size in bytes (1280 to 65535).
Default	1532 bytes
Command Mode	INTERFACE
Usage Information	<p>To return to the default MTU value, use the <code>no mtu</code> command. If an IP packet includes a Layer 2 header, the IP MTU must be at least 32 bytes smaller than the L2 MTU.</p> <ul style="list-style-type: none">• Port-channels<ul style="list-style-type: none">○ All members must have the same link MTU value and the same IP MTU value.○ The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the port channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.• VLANs<ul style="list-style-type: none">○ All members of a VLAN must have same IP MTU value.○ Members can have different link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.○ The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN contains tagged members with a link MTU of 1522 and IP MTU of 1500 and untagged members with link MTU of 1518 and IP MTU of 1500. The VLAN's link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.
Example	<pre>OS10(conf-if-eth1/1/7)# mtu 3000</pre>
Supported Releases	10.2.0E or later

port-group

Configures a group of front-panel unified ports or a double-density QSFP28 (QSFP28-DD) port.

Syntax	<code>port-group node/slot/port-group</code>
---------------	--


Parameters	<ul style="list-style-type: none"> • <i>node/slot</i> — Enter 1/1 for <i>node/slot</i> when you configure a port group. • <i>port-group</i> — Enter the port-group number (1–14). The available port-group range depends on the switch.
Default	Not configured
Command mode	CONFIGURATION
Usage information	<p>Enter PORT-GROUP mode to:</p> <ul style="list-style-type: none"> • Configure unified ports in Fibre Channel or Ethernet mode and break out interfaces with a specified speed. • Break out a QSFP28-DD port into multiple interfaces with a specified speed. <p>To view the ports that belong to a port group, enter the <code>show port-group</code> command.</p>
Example	<pre>OS10(config)# port-group 1/1/8 OS10(conf-pg-1/1/8)#</pre>
Supported releases	10.3.1E or later

scale-profile vlan

Configures the L2 VLAN scale profile on a switch.

Syntax	<code>scale-profile vlan</code>
Parameters	None
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	<p>Use the VLAN scale profile when you scale the number of VLANs so that less memory is consumed. Enable the scale profile before you configure VLANs on the switch. The scale profile globally applies L2 mode on all VLANs you create and disables L3 transmission. The <code>no</code> version of the command disables L2 VLAN scaling. To enable L3 routing traffic on a VLAN, use the <code>mode L3</code> command.</p>
Example	<pre>OS10(config)# scale-profile vlan</pre>
Supported Releases	10.4.0E(X2) or later

show discovered-expanders

 **NOTE:** This command will be supported in future releases.

Syntax	<code>show discovered-expanders</code>
---------------	--

show interface

Displays interface information.

Syntax	<code>show interface [type]</code>
Parameters	<p><code>interface type</code> — Enter the interface type:</p> <ul style="list-style-type: none"> • <code>phy-eth node/slot/port[:subport]</code> — Display information about physical ports connected to the interface. • <code>status</code> — Display interface status. • <code>ethernet node/slot/port[:subport]</code> — Display Ethernet interface information. • <code>loopback id</code> — Display loopback IDs (0 to 16383).

- `mgmt node/slot/port` — Display Management interface information.
- `null` — Display null interface information.
- `port-channel id-number` — Display port channel interface IDs (1 to 128).
- `vlan vlan-id` — Display the VLAN interface number (1 to 4093).

Default Not configured

Command Mode EXEC

Usage Information Use the `do show interface` command to view interface information from other command modes.

Example

```
OS10# show interface
Ethernet 1/1/2 is up, line protocol is up
Hardware is Dell EMC Eth, address is 00:0c:29:54:c8:57
Current address is 00:0c:29:54:c8:57
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
Wavelength is 64
Receive power reading is 0.0
Interface index is 17305094
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Enabled
Link local IPv6 address: fe80::20c:29ff:fe54:c857/64
Global IPv6 address: 2::1/64
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 40G, Auto-Negotiation on
FEC is auto, Current FEC is off
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 00:40:14
Queuing strategy: fifo
Input statistics:
  0 packets, 0 octets
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output statistics:
  0 packets, 0 octets
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
  Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
  Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 3 weeks 1 day 20:30:38

--more--
```

Example (port channel)

```
OS10# show interface port-channel 1
Port-channel 1 is up, line protocol is down
Address is 90:b1:1c:f4:a5:8c, Current address is 90:b1:1c:f4:a5:8c
Interface index is 85886081
Internet address is not set
Mode of IPv4 Address Assignment: not set
MTU 1532 bytes
LineSpeed 0
Minimum number of links to bring Port-channel up is 1
Maximum active members that are allowed in the portchannel is 5
Members in this channel:
ARP type: ARPA, ARP Timeout: 60
```

```
OS10# show interface port-channel summary
LAG Mode Status Uptime Ports
22 L2 up 20:38:08 Eth 1/1/10 (Up)
Eth 1/1/11 (Down)
```

```

23 L2 up 20:34:32 Eth 1/1/12 (Inact)
Eth 1/1/20 (Up)
Eth 1/1/21 (Up)
Eth 1/1/22 (Up)

```

Supported Releases 10.2.0E or later

show inventory media

Displays installed media in switch ports.

Syntax `show inventory media`

Parameters None

Command Mode EXEC

Usage Information Use the `show inventory media` command to verify the media type inserted in a port.

Example

```

OS10# show inventory media
-----
                        System Inventory Media
-----
Node/Slot/Port  Category      Media                               Serial      Dell EMC
Number          Qualified
-----
1/1/1           Not Present
1/1/2           SFP-PLUS      SFPPLUS 10GBASE SR  AM70843    true
1/1/3           Not Present
1/1/4           SFP-PLUS      SFPPLUS 10GBASE SR  AKN0LC7    false
1/1/5           SFP-PLUS      SFPPLUS 10GBASE SR  AM718GQ    true
1/1/6           SFP-PLUS      SFPPLUS 10GBASE SR  AM708XM    true
1/1/7           SFP-PLUS      SFPPLUS 10GBASE SR  AQ2237K    true
1/1/8           SFP-PLUS      SFPPLUS 10GBASE SR  AGT047N    true
1/1/9           Not Present
1/1/10          Not Present
1/1/11          Not Present
1/1/12          Not Present
1/1/13          Not Present
1/1/14          Not Present
1/1/15          SFP-PLUS      SFPPLUS 10GBASE SR  AK60QJN    false
1/1/16          SFP-PLUS      SFPPLUS 10GBASE SR  AL30KWM    true
1/1/17          SFP-PLUS      SFPPLUS 10GBASE SR  AQ22DMB    true
1/1/18          SFP-PLUS      SFPPLUS 10GBASE SR  AQM146U    true
...

```

Supported Releases 10.2.0E or later

show link-bundle-utilization

Displays information about the link-bundle utilization.

Syntax `show link-bundle-utilization`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show link-bundle-utilization

Link-bundle trigger threshold - 60
```

Supported Releases

10.2.0E or later

show port-channel summary

Displays port-channel summary information.

Syntax show port-channel summary**Parameters** None**Default** Not configured**Command Mode** EXEC**Usage Information** None**Example**

```
OS10(conf-if-eth1/1/4)# do show port-channel summary
Flags: D - Down I - member up but inactive P - member up and active
U - Up (port-channel)

Group Port-Channel Type Protocol Member Ports

22 port-channel22 (U) Eth STATIC 1/1/2(D) 1/1/3(P)
23 port-channel23 (D) Eth DYNAMIC 1/1/4(I)
```

Example (Interface)

```
OS10(conf-range-eth1/1/10-1/1/11,1/1/13,1/1/14)# do show port-channel
summary
Flags: D - Down U - member up but inactive P - member up and active
U - Up (port-channel)

Group Port-Channel Type Protocol Member Ports

22 port-channel22 (U) Eth STATIC 1/1/10(P) 1/1/11(P) 1/1/12(P) 1/1/13(P)
1/1/14(P) 1/1/15(P) 1/1/16(P) 1/1/17(P) 1/1/18(P) 1/1/19(P)
23 port-channel23 (D) Eth STATIC
OS10(config)# interface range e1/1/12-1/1/13,1/1/15,1/1/17-1/1/18
OS10(conf-range-eth1/1/12-1/1/13,1/1/15,1/1/17-1/1/18)# no channel-group
OS10(conf-range-eth1/1/12-1/1/13,1/1/15,1/1/17-1/1/18)# do show port-
channel summary
Flags: D - Down U - member up but inactive P - member up and active
U - Up (port-channel)

Group Port-Channel Type Protocol Member Ports

22 port-channel22 (U) Eth STATIC 1/1/10(P) 1/1/11(P) 1/1/14(P) 1/1/16(P)
1/1/19(P)
23 port-channel23 (D) Eth STATIC
```

Supported Releases

10.2.0E or later

show port-group

Displays the current port-group configuration on a switch.

Syntax show port-group**Parameters** None

Default None

Command Mode EXEC

Usage Information To view the ports that belong to each port group, use the `show port-group` command. To configure a port group, enter the `port-group` command.

Example:
S4148U-ON

```
OS10(config)# show port-group
port-group mode ports
1/1/1 Eth 10g-4x 1 2 3 4
1/1/2 FC 16g-2x 5 6 7 8
1/1/3 FC 16g-2x 9 10 11 12
1/1/4 FC 16g-2x 13 14 15 16
1/1/5 FC 16g-2x 17 18 19 20
1/1/6 FC 16g-2x 21 22 23 24
1/1/7 Eth 100g-1x 25
1/1/8 Eth 40g-1x 26
1/1/9 Eth 100g-1x 29
1/1/10 Eth 40g-1x 30
```

Supported Releases 10.3.1E or later

show switch-operating-mode

Displays the current operating mode of a supported switch.

Syntax `show switch-operating-mode`

Parameters None

Command Mode EXEC

Usage Information Some OS10 switches operate in Full Switch and SmartFabric modes. The default is Full Switch mode.

Example

```
OS10# show switch-operating-mode
Switch-Operating-Mode : Smart Fabric Mode
```

Supported Releases 10.4.0E(R3) or later

show switch-port-profile

Displays the current and default port profile on a switch.

Syntax `show switch-port-profile node/slot`

Parameters • `node/slot` — Enter the switch information. For a standalone switch, enter 1/1.

Default `profile-1`

Command Mode EXEC

Usage Information A switch-port profile determines the available front-panel ports and breakout modes on Ethernet and unified ports. To display the current port profile, enter the `show switch-port-profile` command. To reset the switch to the default port profile, enter the `no switch-port-profile node/slot` command.

Example

```
OS10(config)# show switch-port-profile 1/1

| Node/Unit | Current      | Next-boot    | Default      |
|-----|-----|-----|-----|
| 1/1      | profile-2   | profile-2    | profile-1   |
```

```
Supported Profiles:
profile-1
profile-2
profile-3
profile-4
profile-5
profile-6
```

Supported Releases 10.3.1E or later

show unit-provision

i **NOTE:** This command will be supported in future releases.

Syntax `show unit-provision`

show vlan

Displays the current VLAN configuration.

Syntax `show vlan [vlan-id]`

Parameters `vlan-id` — (Optional) Enter a VLAN ID (1 to 4093).

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring
VLANs
Q: A - Access (Untagged), T - Tagged
NUM Status Description Q Ports
1 down
```

Supported Releases 10.2.0E or later

shutdown

Disables an interface.

Syntax `shutdown`

Parameters None

Default Disabled

Command Mode INTERFACE

Usage Information

This command marks a physical interface as unavailable for traffic. Disabling a VLAN or a port-channel causes different behavior. When you disable a VLAN, the L3 functions within that VLAN are disabled, and L2 traffic continues to flow. Use the `shutdown` command on a port-channel to disable all traffic on the port-channel, and the individual interfaces. Use the `no shutdown` command to enable a port-channel on the interface. The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port-channel.

Example

```
OS10(config)# interface ethernet 1/1/7
OS10(conf-if-eth1/1/7)# no shutdown
```

Supported Releases 10.2.0E or later

speed (Fibre Channel)

Configures the transmission speed of a Fibre Channel interface.

Syntax `speed {8 | 16 | 32 | auto}`

Parameters Set the speed of a Fibre Channel interface to:

- 8 — 8GFC
- 16 — 16GFC
- 32 — 32GFC
- auto — Set the port speed to the speed of the installed media.

Defaults Auto

Command Mode INTERFACE

Usage Information The `speed` command is supported only on the Management and Fibre Channel interfaces. This command is not supported on Ethernet interfaces.

- To configure oversubscription for bursty storage traffic on a FC interface, use the `speed` command. Oversubscription allows a port to operate faster, but may result in traffic loss. For example, QSFP28 port groups in 4x8GFC mode support 16GFC oversubscription on member interfaces. QSFP28 breakout interfaces in 4x16GFC mode support 32GFC oversubscription.
- The `no` version of this command resets the port speed to the default value `auto`.

Example

```
OS10(conf-if-fc-1/1/2)# speed 16
```

Supported Releases 10.3.1E or later

speed (Management)

Configures the transmission speed of the Management interface.

Syntax `speed {10 | 100 | 1000 | auto}`

Parameters Set the management port speed to:

- 10 — 10M
- 100 — 100M
- 1000 — 1000M
- auto — Set the port to auto-negotiate speed with a connected device.

Defaults Auto

Command Mode INTERFACE

Usage Information The `speed` command is supported only on the Management and Fibre Channel interfaces. This command is not supported on Ethernet interfaces.

- When you manually configure the management port speed, match the speed of the remote device. Dell EMC highly recommends using auto-negotiation for the management port.
- The `no` version of this command resets the port speed to the default value `auto`.

Example

```
OS10(conf-if-ma-1/1/1)# speed auto
```


Supported Releases 10.3.0E or later

switch-port-profile

Configures a port profile on the switch. The port profile determines the available front-panel ports and breakout modes.

Syntax	<code>switch-port-profile node/unit profile</code>
Parameters	<ul style="list-style-type: none">• <code>node/unit</code> — Enter switch information. For a standalone switch, enter 1/1.• <code>profile</code> — Enter the name of a platform-specific profile.
Default	<code>profile-1</code>
Command Mode	CONFIGURATION
Usage Information	<ul style="list-style-type: none">• S4148-ON series port profiles:<ul style="list-style-type: none">○ <code>profile-1</code> — SFP+ 10G ports (1-24 and 31-54) and QSFP28 100G ports (25-26 and 29-30) are enabled. QSFP28 ports support 100GE and 4x10G, 4x25G, and 2x50G breakouts.○ <code>profile-2</code> — SFP+ 10G ports (1-24 and 31-50), QSFP+ 40G ports (27-28), and QSFP28 ports in 40G mode (25-26 and 29-30) are enabled. QSFP+ and QSFP28 ports support 40GE and 4x10G breakouts.○ <code>profile-3</code> — SFP+ 10G ports (5-24 and 31-50), QSFP+ 40G ports (27-28), and QSFP28 ports with 40G and 100G capability (25-26 and 29-30) are enabled. QSFP+ ports support 40GE and 4x10G breakouts. QSFP28 ports support 100GE and 4x25G breakouts with QSFP28 transceivers, and 40GE and 4x10G breakouts with QSFP+ transceivers.○ <code>profile-4</code> — SFP+ 10G ports (5-24 and 31-50), QSFP+ 40G ports (27-28), and QSFP28 ports with 40G and 100G capability (25-26 and 29-30) are enabled. QSFP+ ports support 40GE and 4x10G breakouts. QSFP28 ports support 100GE and 2x50G breakouts with QSFP28 transceivers, and 40GE and 4x10G breakouts with QSFP+ transceivers.○ <code>profile-5</code> — SFP+ 10G ports (1-24 and 31-54), QSFP+ 40G ports (27-28), QSFP28 ports with 40G capability (26 and 30), and QSFP28 ports with 40G and 100G capability (25 and 29) are enabled. QSFP+ ports support 40GE and 4x10G breakouts. QSFP28 ports 26 and 30 support 40GE and 4x10G breakouts with QSFP+ transceivers. QSFP28 ports 25 and 29 support 100GE and 4x25G breakouts with QSFP28 transceivers, and 40GE and 4x10G breakouts with QSFP+ transceivers.○ <code>profile-6</code> — SFP+ 10G ports (1-24 and 31-54), QSFP+ 40G ports (27-28), QSFP28 ports with 40G capability (26 and 30), and QSFP28 ports with 40G and 100G capability (25 and 29) are enabled. QSFP+ ports support 40GE and 4x10G breakouts. QSFP28 ports 26 and 30 support 40GE and 4x10G breakouts with QSFP+ transceivers. QSFP28 ports 25 and 29 support 100GE and 2x50G breakouts with QSFP28 transceivers, and 40GE and 4x10G breakouts with QSFP+ transceivers.• S4148U-ON port profiles:<ul style="list-style-type: none">○ <code>profile-1</code> — SFP+ unified ports (1-24), QSFP28 unified ports (25-26 and 29-30), QSFP+ Ethernet ports (27-28), and SFP+ Ethernet ports (31-54) are enabled.<ul style="list-style-type: none">▪ SFP+ unified port groups operate in FC mode with 2x16GFC breakouts (ports 1 and 3) by default and support 4x8GFC. SFP+ unified ports support Ethernet 10GE mode.▪ QSFP28 unified ports 25 and 29 operate in Ethernet 100GE mode by default, and support 40GE with QSFP+ transceivers and 4x10G breakouts. QSFP28 ports 25 and 29 support 1x32GFC, 2x16GFC, and 4x8GFC in FC mode.▪ QSFP28 unified ports 26 and 30 operate in Ethernet 40GE mode by default and support 4x10G breakouts. QSFP28 ports 26 and 30 support 1x32GFC, 2x16GFC, and 4x8GFC in FC mode.▪ QSFP+ Ethernet ports operate at 40GE by default and support 4x10G breakouts.▪ SFP+ Ethernet ports operate at 10GE.

- `profile-2` — SFP+ unified ports (1-24), QSFP28 unified ports (25-26 and 29-30), QSFP+ Ethernet ports (27-28), and SFP+ Ethernet ports (31-54) are enabled.
 - SFP+ unified ports operate in Ethernet 10GE mode by default. SFP+ unified port groups support 4x8GFC and 2x16GFC breakouts (ports 1 and 3) in FC mode.
 - QSFP28 unified ports 25 and 29 operate in Ethernet 100GE mode by default, and support 40GE with QSFP+ transceivers and 4x10G breakouts. QSFP28 ports 25 and 29 support 1x32GFC, 2x16GFC, and 4x8GFC in FC mode.
 - QSFP28 unified ports 26 and 30 operate in Ethernet 40GE mode by default and support 4x10G breakouts. QSFP28 ports 26 and 30 support 1x32GFC, 2x16GFC, and 4x8GFC in FC mode.
 - QSFP+ Ethernet ports operate at 40GE by default and support 4x10G breakouts.
 - SFP+ Ethernet ports operate at 10GE.
- `profile-3` — SFP+ unified ports (1-24), QSFP28 unified ports (25-26 and 29-30), and SFP+ Ethernet ports (31-54) are enabled. QSFP+ Ethernet ports (27-28) are not available.
 - SFP+ unified ports operate in Ethernet 10GE mode by default. SFP+ unified port groups support 4x8GFC and 2x16GFC breakouts (ports 1 and 3) in FC mode.
 - QSFP28 unified ports operate in Ethernet 100GE mode by default and support 4x25G and 4x10G breakouts. QSFP28 ports support 2x16GFC and 4x16GFC breakouts in FC mode.
 - SFP+ Ethernet ports operate at 10GE.
- `profile-4` — SFP+ unified ports (1-24), QSFP28 unified ports (25-26 and 29-30), and SFP+ Ethernet ports (31-54) are enabled. QSFP+ Ethernet ports (27-28) are not available.
 - SFP+ unified ports operate in Ethernet 10GE mode by default. SFP+ unified ports support 4x8FC in FC mode.
 - QSFP28 unified ports operate in Ethernet 100GE mode by default, and support 2x50G, 4x25G, and 4x10G breakouts. QSFP28 ports support 4x16GFC breakouts in FC mode.
 - SFP+ Ethernet ports operate at 10GE.

Usage Information

- Setting a port group in 2x16GFC mode activates odd-numbered interfaces 1 and 3. A port group in 1x32GFC mode activates only interface 1.
- To display the current port profile on a switch, enter the `show switch-port-profile` command.
- To change the port profile on a switch, enter the `switch-port-profile` command with the desired profile, save it to the startup configuration, and reload the switch. The switch reboots with new port configuration. The `no` version of the command resets to the default profile. When a switch reloads with a new port profile, the startup configuration resets to system defaults, except for the switch-port profile and these configured settings:
 - Management interface 1/1/1 configuration
 - Management IPv4/IPv6 static routes
 - System hostname
 - Unified Forwarding Table (UFT) mode
 - ECMP maximum paths

You must manually reconfigure other settings on a switch after you apply a new port profile and reload the switch.

Example

```
OS10(config)# switch-port-profile 1/1 profile-1
Warning: Switch port profile will be applied only after a save and
reload. All management port
configurations will be retained but all other configurations will be
wiped out after the reload.
OS10(config)# do write memory
OS10(config)# do reload
```

Supported Releases

10.3.0E or later

switchport access vlan

Assigns access VLAN membership to a port in L2 access or trunk mode.

Syntax

```
switchport access vlan vlan-id
```

Parameters

`vlan vlan-id` — Enter the VLAN ID number (1 to 4093).

Default	VLAN 1
Command Mode	INTERFACE
Usage Information	This command enables L2 switching for untagged traffic and assigns a port interface to default VLAN 1. Use this command to change the assignment of the access VLAN that carries untagged traffic. You must create the VLAN before you can assign an access interface to it. The <code>no</code> version of this command resets access VLAN membership on a L2 access or trunk port to VLAN 1.
Example	<pre>OS10(conf-if-eth1/1/3)# switchport mode access OS10(conf-if-eth1/1/3)# switchport access vlan 100</pre>
Supported Releases	10.2.0E or later

switchport mode

Places an interface in L2 access or trunk mode.

Syntax	<code>switchport mode {access trunk}</code>
Parameters	<ul style="list-style-type: none"> • <code>access</code> — Enables L2 switching of untagged frames on a single VLAN. • <code>trunk</code> — Enables L2 switching of untagged frames on the access VLAN, and of tagged frames on the VLANs specified with the <code>switchport trunk allowed vlan</code> command.
Default	<code>access</code>
Command Mode	INTERFACE
Usage Information	<ul style="list-style-type: none"> • If an IP address is assigned to an interface, you cannot use this command to enable L2 switching — you must first remove the IP address. • The <code>access</code> parameter automatically adds an interface to default VLAN 1 to transmit untagged traffic. Use the <code>switchport access vlan</code> command to change the access VLAN assignment. • The <code>trunk</code> parameter configures an interface to transmit tagged VLAN traffic. You must manually configure VLAN membership for a trunk port with the <code>switchport trunk allowed vlan</code> command. • Use the <code>no switchport</code> command to remove all L2 configuration when you configure an interface in L3 mode. • Use the <code>no switchport mode</code> command to restore a trunk port on an interface to L2 access mode on VLAN 1.
Example	<pre>OS10(conf-if-eth1/1/7)# switchport mode access</pre>
Supported Releases	10.2.0E or later

switchport trunk allowed vlan

Configures the tagged VLAN traffic that a L2 trunk interface can carry. An L2 trunk port has no tagged VLAN membership and does not transmit tagged traffic.

Syntax	<code>switchport trunk allowed vlan <i>vlan-id-list</i></code>
Parameters	<i>vlan-id-list</i> — Enter the VLAN numbers of the tagged traffic that the L2 trunk port can carry. Comma-separated and hyphenated VLAN number ranges are supported.
Default	None
Command Mode	INTERFACE
Usage Information	Use the <code>no</code> version of this command to remove the configuration.

Example

```
OS10(conf-if-eth1/1/2)# switchport trunk allowed vlan 1000
```

```
OS10(conf-if-eth1/1/2)# no switchport trunk allowed vlan 1000
```

**Supported
Releases**

10.2.0E or later

unit-provision

This command will be supported in future releases.

Syntax

```
unit-provision node/unit-id provision_name
```

Fibre Channel

OS10 switches with Fibre Channel (FC) ports operate in one of the following modes: Direct attach (F_Port), NPIV Proxy Gateway (NPG), or FIP Snooping Bridge (FSB). In the FSB mode, you cannot use the FC ports.

OS10 switches with Ethernet ports operate in FIP Snooping Bridge (FSB).

F_Port

Fibre Channel fabric port (F_Port) is the switch port that connects the FC fabric to a node. S4148U-ON switches support F_Port.

Enable Fibre Channel F_Port mode globally using the `feature fc domain-ID domain-ID` command in CONFIGURATION mode.

Enable Fibre Channel F_Port mode

```
OS10(config)# feature fc domain-id 100
```

NPIV Proxy Gateway

A node port (N_Port) is a port on a network node that acts as a host or storage device, and is used in FC point-to-point or FC switched fabric topologies.

N_Port ID Virtualization (NPIV) allows multiple N_Port IDs to share a single physical N_Port.

The NPIV Proxy Gateway (NPG) provides Fibre Channel over Ethernet (FCoE) to Fibre Channel (FC) bridging and vice versa. Starting from OS 10.4.1, NPG supports FC to FC switching as well.

Enable NPG mode globally using the `feature fc npg` command in CONFIGURATION mode.

You can use the `fc port-mode F` command on FC interfaces to change the port mode from default N_Port.

Enable NPG mode

```
OS10(config)# feature fc npg
```

NOTE: In a switch configured to operate in NPG or F-Port mode, OS10 does not support scale profile VLAN configuration. If you want to use scale profile configuration in NPG or F-Port mode, enable CPU based VLAN flooding on vfabric VLAN using the `mode L3` command.

FIP snooping bridge

Fibre Channel over Ethernet (FCoE) encapsulates FC frames over Ethernet networks.

FCoE Initialization protocol (FIP) establishes FC connectivity with Ethernet ports.

FIP snooping bridge (FSB) implements security characteristics to admit valid FCoE traffic in the Ethernet networks.

FIP and FCoE provide FC emulation over Ethernet links.

NOTE: OS10 switches do not support multi-hop FIP snooping bridge (multi-hop FSB) capability; links to other FIP snooping bridges on a FIP snooping-enabled device (bridge-to-bridge links) are not supported.

Enable FIP snooping mode

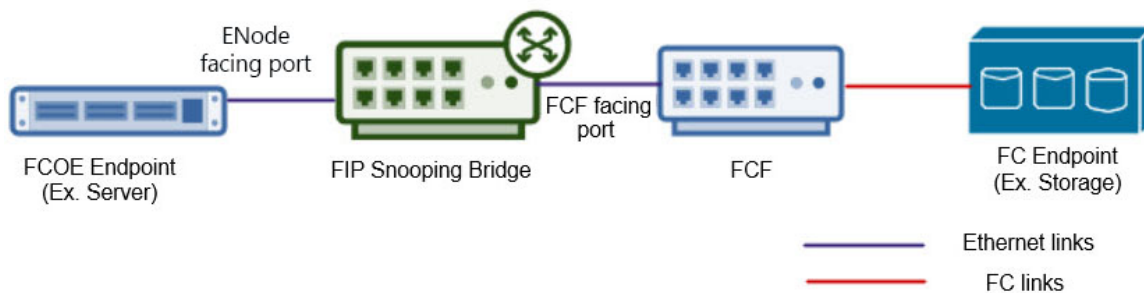
```
OS10(config)# feature fip-snooping
```

An Ethernet switch configured to operate in FSB mode snoops FIP packets on FCoE enabled VLANs and discovers the following information:

- End nodes (ENodes)
- Fibre Channel Forwarder (FCF)
- Connections between ENodes and FCFs
- Sessions between ENodes and FCFs

NOTE: OS10 supports multiple ENodes in F_Port mode.

Using the discovered information, the switch installs ACL entries that provide security and point-to-point link emulation.



Terminology

ENode	End Node or FCoE node
FC	Fibre Channel
FC ID	A 3-byte address used by FC to identify the end points
FC Map	A 3-byte prefix configured per VLAN, used to frame FCoE MAC address
FCF	Fibre Channel Forwarder
FCoE	Fibre Channel over Ethernet
FCoE MAC	Unique MAC address used to identify an FCoE session. This is a combination of FC ID and FC Map.
FIP	FCoE Initialization Protocol
NPG	NPIV Proxy Gateway
NPIV	N_Port ID Virtualization

Virtual fabric

Virtual fabrics (vfabric) divide a physical fabric into logical fabrics.

Manage each vfabric independently. The fabric ID identifies each vfabric.

You can configure only one vfabric in the F_Port mode and multiple vfabric in the NPG mode.

The F_Port and NPG modes are mutually exclusive.

If you have already configured a vfabric in F_Port mode, while configuring vfabric in NPG mode, disable the F_Port mode. The existing vfabric is removed when you disable F_Port mode and you need to configure new vfabric in NPG mode. If you are moving from NPG mode to F_Port mode, then disable the NPG mode and create new vfabric in F_Port mode.

Zoning allows you to increase network security by partitioning the devices connected to the vfabric into subsets. Partitioning restricts unnecessary interactions between the members of vfabric. See also [Fibre Channel zoning](#) on page 121.

After configuring a vfabric ID, you can create a name, associate a VLAN to carry traffic to the vfabric, configure FCoE parameters, configure the default zone, and activate the zoneset.

NOTE: Do not associate a VLAN that is already in use, as a vfabric VLAN.

Configure vfabric in F_Port mode

1. Configure a vfabric using the `vfabric fabric-ID` command in CONFIGURATION mode. The switch enters vfabric CONFIGURATION mode. Enter the following commands.
2. Associate a VLAN ID to the vfabric with the `vlan vlan-ID` command.
3. Add an FC map with the `fcoe fcmap fc-map` command.
4. Activate a zoneset using the `zoneset activate zoneset-name` command.

5. Allow access to all logged-in members in the absence of active zoneset configuration using the `zone default-zone permit` command. The logged-in members are the FC nodes that are successfully logged into the FC fabric, identified by the `vfabric`.
6. (Optional) Add a name to the `vfabric` using the `name vfabric-name` command.
7. Apply the `vfabric` to FC interfaces using the `vfabric fabric-ID` command in FC INTERFACE mode.

Example configuration of `vfabric` in F_Port mode

```
OS10(config)# vfabric 100
OS10(conf-vfabric-100)# name 100
OS10(conf-vfabric-100)# vlan 1023
OS10(conf-vfabric-100)# fcoe fcmap 0xEFC64
OS10(conf-vfabric-100)# zoneset activate set
OS10(conf-vfabric-100)# zone default-zone permit
OS10(conf-vfabric-100)# exit
OS10(config)# interface fibrechannel 1/1/1
OS10(conf-if-fcl/1/1)# vfabric 100
```

View `vfabric` configuration

```
OS10(conf-vfabric-100)# show configuration
!
vfabric 100
 name 100
 vlan 1023
 fcoe fcmap 0xEFC64
 zoneset activate set
 zone default-zone permit
```

```
OS10# show vfabric
Fabric Name          100
Fabric Type          FPORT
Fabric Id            100
Vlan Id              1023
FC-MAP               0xEFC64
Config-State         ACTIVE
Oper-State           UP
=====
Switch Config Parameters
=====
Domain ID            100
=====
Switch Zoning Parameters
=====
Default Zone Mode:   Allow
Active ZoneSet:      set
=====
Members
fibrechannel1/1/1
fibrechannel1/1/2
fibrechannel1/1/3
fibrechannel1/1/4
fibrechannel1/1/5
fibrechannel1/1/6
fibrechannel1/1/7
fibrechannel1/1/8
fibrechannel1/1/9
fibrechannel1/1/10
fibrechannel1/1/11
fibrechannel1/1/12
fibrechannel1/1/15
fibrechannel1/1/17
fibrechannel1/1/18
fibrechannel1/1/19
fibrechannel1/1/20
fibrechannel1/1/21
fibrechannel1/1/22
fibrechannel1/1/23
fibrechannel1/1/24
fibrechannel1/1/25:1
fibrechannel1/1/29:1
```

```
fibrechannell1/1/30:1
fibrechannell1/1/30:3
=====
```

Configure vfabric in NPG mode

1. Configure a vfabric using the `vfabric fabric-ID` command in CONFIGURATION mode. The switch enters vfabric CONFIGURATION mode. Enter the following commands.
2. Associate a VLAN ID to the vfabric with the `vlan vlan-ID` command.
3. Add FCoE parameters with the `fcoe {fcmmap fc-map | fcf-priority fcf-priority-value | fka-adv-period adv-period | vlan-priority vlan-priority-value | keep-alive}` command.
4. (Optional) Add a name to the vfabric using the `name vfabric-name` command.
5. Apply the vfabric to interfaces using the `vfabric fabric-ID` command in INTERFACE mode.

Example configuration of vfabric in NPG mode

```
OS10(config)# vfabric 10
OS10(conf-vfabric-10)# name 10
OS10(conf-vfabric-10)# vlan 100
OS10(conf-vfabric-10)# fcoe fcmmap 0x0efc01
OS10(conf-vfabric-10)# fcoe fcf-priority 128
OS10(conf-vfabric-10)# fcoe fka-adv-period 8
OS10(conf-vfabric-10)# fcoe vlan-priority 3
OS10(conf-vfabric-10)# exit
OS10(config)# interface ethernet 1/1/31
OS10(conf-if-eth1/1/31)# vfabric 10
```

View vfabric configuration

```
OS10(conf-vfabric-10)# show configuration
!
vfabric 10
name 10
vlan 100
fcoe fcmmap 0xEFC01
fcoe fcf-priority 128
fcoe fka-adv-period 8
fcoe vlan-priority 3
```

```
OS10# show vfabric
Fabric Name 10
Fabric Type NPG
Fabric Id 10
Vlan Id 100
FC-MAP 0xEFC01
Vlan priority 3
FCF Priority 128
FKA-Adv-Period Enabled,8
Config-State ACTIVE
Oper-State DOWN
=====
Members
=====
```

```
OS10# show running-configuration vfabric
!
vfabric 10
name 10
vlan 100
fcoe fcmmap 0xEFC01
fcoe fcf-priority 128
fcoe fka-adv-period 8
fcoe vlan-priority 3
```


Fibre Channel zoning

Fibre Channel (FC) zoning partitions a FC fabric into subsets to restrict unnecessary interactions, improve security, and manage the fabric more effectively. Create zones and add members to the zone. Identify a member by an FC alias, World Wide Name (WWN), or FC ID. A zone can have a maximum of 255 unique members. Create zonesets and add the zones to a zoneset. A switch can have multiple zonesets, but you can activate only one zoneset at a time in a fabric.

1. (Optional) Create an FC alias using the `fc alias alias-name` command in CONFIGURATION mode. The switch enters Alias CONFIGURATION mode.
2. Add members to the alias using the `member {wwn wwn-ID | fc-id fc-id}` command in Alias CONFIGURATION mode. You can add a maximum of 255 unique members.
3. Create a zone using the `fc zone zone-name` command in the CONFIGURATION mode. The switch enters Zone CONFIGURATION mode.
4. Add members to the zone with the `member {alias-name alias-name | wwn wwn-ID | fc-id fc-id}` command in Zone CONFIGURATION mode.
5. Create a zoneset using the `fc zoneset zoneset-name` command in CONFIGURATION mode. The switch enters Zoneset CONFIGURATION mode.
6. Add the existing zones to the zoneset with the `member zone-name` command in Zoneset CONFIGURATION mode.
7. Activate the zoneset using the `zoneset activate zoneset-name` command in vfabric CONFIGURATION mode. The members in the zoneset become active.
8. Allow access between all the logged-in FC nodes in the absence of active zoneset configuration using the `zone default-zone permit` command in vfabric CONFIGURATION mode. A default zone advertises a maximum of 255 members in the registered state change notification (RSCN) message.

NOTE: The default-zone allows or denies access to the FC nodes when an active zoneset is not available. When the default-zone action is set to `permit`, the switch allows communication between all the possible pairs of FC nodes. When the default-zone action is not configured, the switch denies any communication between FC nodes.

To configure the vfabric on FC interfaces, you need to associate a VLAN ID to the vfabric and add an FC map. See [Virtual fabric](#) on page 118 for more information.

Configure FC zoning

```
OS10(config)# fc zone hba1
OS10(config-fc-zone-hba1)# member wwn 10:00:00:90:fa:b8:22:19
OS10(config-fc-zone-hba1)# member wwn 21:00:00:24:ff:7b:f5:c8
OS10(config-fc-zone-hba1)# exit

OS10(config)# fc zoneset set
OS10(conf-fc-zoneset-set)# member hba1
OS10(conf-fc-zoneset-set)# exit

OS10(config)# vfabric 100
OS10(conf-vfabric-100)# zoneset activate set
OS10(conf-vfabric-100)# zone default-zone permit
```

View FC zone configuration

```
OS10(config-fc-zone-hba1)# show configuration
!
fc zone hba1
member wwn 21:00:00:24:ff:7b:f5:c8
member wwn 10:00:00:90:fa:b8:22:19
```

```
OS10# show fc zone

Zone Name                Zone Member
=====
hba1                      21:00:00:24:ff:7b:f5:c8
                          10:00:00:90:fa:b8:22:19

hba2                      20:01:00:0e:1e:e8:e4:99
                          50:00:d3:10:00:ec:f9:1b
                          50:00:d3:10:00:ec:f9:05
                          50:00:d3:10:00:ec:f9:1f
                          20:35:78:2b:cb:6f:65:57
```

View FC zoneset configuration

```
OS10(conf-fc-zoneset-set)# show configuration
!  
fc zoneset set  
  member hba1  
  member hba2
```

```
OS10# show fc zoneset active  
  
vFabric id: 100  
Active Zoneset: set  
ZoneName          ZoneMember  
=====
```

hba2	*20:01:00:0e:1e:e8:e4:99
	20:35:78:2b:cb:6f:65:57
	50:00:d3:10:00:ec:f9:05
	50:00:d3:10:00:ec:f9:1b
	50:00:d3:10:00:ec:f9:1f
hba1	*10:00:00:90:fa:b8:22:19
	*21:00:00:24:ff:7b:f5:c8

```
OS10# show fc zoneset set  
ZoneSetName      ZoneName          ZoneMember  
=====
```

set	hba1	21:00:00:24:ff:7b:f5:c8
		10:00:00:90:fa:b8:22:19
		21:00:00:24:ff:7f:ce:ee
		21:00:00:24:ff:7f:ce:ef
hba2	20:01:00:0e:1e:e8:e4:99	
	50:00:d3:10:00:ec:f9:1b	
	50:00:d3:10:00:ec:f9:05	
	50:00:d3:10:00:ec:f9:1f	
	20:35:78:2b:cb:6f:65:57	

F_Port on Ethernet

OS10 supports configuring F_Port mode on an Ethernet port that is connected to converged network adapters (CNA).

After enabling F_Port mode, configure a vfabric and apply the vfabric to Ethernet ports connected to CNA.

You can configure only one vfabric in F_Port mode.

You can apply the configured vfabric to multiple Ethernet interfaces. You can also add the Ethernet interfaces to a port-channel and apply the vfabric to the port-channel.

Example configuration

```
OS10(config)# feature fc domain-id 100  
OS10(config)# vfabric 100  
OS10(conf-vfabric-100)# name 100  
OS10(conf-vfabric-100)# vlan 1023  
OS10(conf-vfabric-100)# fcoe fcmmap 0xEFC64  
OS10(conf-vfabric-100)# zoneset activate set  
OS10(conf-vfabric-100)# zone default-zone permit  
OS10(conf-vfabric-100)# exit  
OS10(config)# interface ethernet 1/1/30  
OS10(conf-if-eth1/1/30)# vfabric 100
```

F_Port commands

The following commands are supported on F_Port mode:

fc alias

Creates an FC alias. After creating the alias, you can add members to the FC alias. An FC alias can have a maximum of 255 unique members.

Syntax	<code>fc alias <i>alias-name</i></code>
Parameters	<i>alias-name</i> — Enter a name for the FC alias.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes the FC alias. To delete an FC alias, first remove it from the FC zone.
Example	<pre>OS10(config)# fc alias test OS10(config-fc-alias-test)# member wwn 21:00:00:24:ff:7b:f5:c9 OS10(config-fc-alias-test)# member wwn 20:25:78:2b:cb:6f:65:57</pre>
Supported Releases	10.3.1E or later

fc zone

Creates an FC zone and adds members to the zone. An FC zone can have a maximum of 255 unique members.

Syntax	<code>fc zone <i>zone-name</i></code>
Parameters	<i>zone-name</i> — Enter a name for the zone.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes the FC zone. To delete an FC zone, first remove it from the FC zoneset.
Example	<pre>OS10(config)# fc zone hba1 OS10(config-fc-zone-hba1)# member wwn 10:00:00:90:fa:b8:22:19 OS10(config-fc-zone-hba1)# member wwn 21:00:00:24:ff:7b:f5:c8</pre>
Supported Releases	10.3.1E or later

fc zoneset

Creates an FC zoneset and adds the existing FC zones to the zoneset.

Syntax	<code>fc zoneset <i>zoneset-name</i></code>
Parameters	<i>zoneset-name</i> — Enter a name for the FC zoneset. The name must start with a letter and may contain characters: A-Z, a-z, 0-9, \$, _, -, ^
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the FC zoneset.
Example	<pre>OS10(config)# fc zoneset set OS10(conf-fc-zoneset-set)# member hba1</pre>

Supported Releases 10.3.1E or later

feature fc

Enables the F_Port globally.

Syntax `feature fc domain-id domain-id`

Parameters `domain-id` — Enter the domain ID of the F_Port, from 1 to 239.

Defaults Disabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables the F_Port. You can disable the F_Port only when vfabric and zoning configurations are not available. Before disabling the F_Port, remove the vfabric and zoning configurations.

Example

```
OS10(config)# feature fc domain-id 100
```

Supported Releases 10.3.1E or later

member (alias)

Add members to existing FC aliases. Identify a member by an FC alias, a World Wide Name (WWN), or an FC ID.

Syntax `member {wwn wwn-ID | fc-id fc-id}`

Parameters

- `wwn-ID` — Enter the WWN name.
- `fc-id` — Enter the FC ID name.

Defaults Not configured

Command Mode Alias CONFIGURATION

Usage Information The `no` version of this command removes the member from the FC alias.

Example

```
OS10(config)# fc alias test
OS10(config-fc-alias-test)# member wwn 21:00:00:24:ff:7b:f5:c9
OS10(config-fc-alias-test)# member wwn 20:25:78:2b:cb:6f:65:57
```

Supported Releases 10.3.1E or later

member (zone)

Adds members to existing zones. Identify a member by an FC alias, a World Wide Name (WWN), or an FC ID.

Syntax `member {alias-name alias-name | wwn wwn-ID | fc-id fc-id}`

Parameters

- `alias-name` — Enter the FC alias name.
- `wwn-ID` — Enter the WWN name.
- `fc-id` — Enter the FC ID name.

Defaults Not configured

Command Mode Zone CONFIGURATION

Usage Information The `no` version of this command removes the member from the zone.

Example

```
OS10(config)# fc zone hba1
OS10(config-fc-zone-hba1)# member wwn 10:00:00:90:fa:b8:22:19
OS10(config-fc-zone-hba1)# member wwn 21:00:00:24:ff:7b:f5:c8
```

Supported Releases 10.3.1E or later

member (zoneset)

Adds zones to an existing zoneset.

Syntax `member zone-name`

Parameters `zone-name` — Enter an existing zone name.

Defaults Not configured

Command Mode Zoneset CONFIGURATION

Usage Information The `no` version of this command removes the zone from the zoneset.

Example

```
OS10(config)# fc zoneset set
OS10(config-fc-zoneset-set)# member hba1
```

Supported Releases 10.3.1E or later

show fc alias

Displays the details of a FC alias and its members.

Syntax `show fc alias [alias-name]`

Parameters `alias-name` — (Optional) Enter the FC alias name.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fc alias

Alias Name                Alias Member
=====
test                      21:00:00:24:ff:7b:f5:c9
                          20:25:78:2b:cb:6f:65:57

OS10#
```

Supported Releases 10.3.1E or later

show fc interface-area-id mapping

Displays the FC ID to interface mapping details.

Syntax `show fc interface-area-id mapping`

Parameters None

Default Not configured
Command Mode EXEC
Usage Information None

Example

```
OS10# show fc interface-area-id mapping
Intf Name                      FC-ID                      Status
=====
ethernet1/1/40                 0a:02:00                 Active
```

Supported Releases 10.4.1.0 or later

show fc ns switch

Displays the details of FC NS switch parameters.

Syntax show fc ns switch [brief]
Parameters None
Default Not configured
Command Mode EXEC
Usage Information None

Example

```
OS10# show fc ns switch

Total number of devices = 2

Switch Name          10:00:14:18:77:20:8d:cf
Domain Id            100
Switch Port          fibrechannel1/1/25:1
FC-Id                64:64:00
Port Name            10:00:00:90:fa:b8:22:19
Node Name            20:00:00:90:fa:b8:22:19
Class of Service     12
Symbolic Port Name
Symbolic Node Name
Port Type             N_PORT
Registered with NameServer Yes
Registered for SCN   Yes

Switch Name          10:00:14:18:77:20:8d:cf
Domain Id            100
Switch Port          fibrechannel1/1/29
FC-Id                64:74:00
Port Name            21:00:00:24:ff:7b:f5:c8
Node Name            20:00:00:24:ff:7b:f5:c8
Class of Service     8
Symbolic Port Name   QLogic Port0 WWPN 21:00:00:24:ff:7b:f5:c8
Symbolic Node Name   QLE2742 FW:v8.03.05 DVR:v9.2.3.20
Port Type             N_PORT
Registered with NameServer Yes
Registered for SCN   Yes
```

Example (brief)

```
OS10# show fc ns switch brief
Total number of devices = 2

Intf#           Domain  FC-ID           Enode-WWPN
  Enode-WWNN
-----
fibrechannel1/1/25:1  100    64:64:00       10:00:00:90:fa:b8:22:19
```

```

20:00:00:90:fa:b8:22:19
fibrechannel1/1/29      100      64:74:00      21:00:00:24:ff:7b:f5:c8
20:00:00:24:ff:7b:f5:c8

```

Supported Releases 10.3.1E or later

show fc zone

Displays the FC zones and the zone members.

Syntax `show fc zone [zone-name]`

Parameters `zone-name` — Enter the FC zone name.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```

OS10# show fc zone

Zone Name                Zone Member
=====
hba1                    21:00:00:24:ff:7b:f5:c8
                        10:00:00:90:fa:b8:22:19
                        21:00:00:24:ff:7f:ce:ee
                        21:00:00:24:ff:7f:ce:ef
hba2                    20:01:00:0e:1e:e8:e4:99
                        50:00:d3:10:00:ec:f9:1b
                        50:00:d3:10:00:ec:f9:05
                        50:00:d3:10:00:ec:f9:1f
                        20:35:78:2b:cb:6f:65:57

```

Example (with zone name)

```

OS10# show fc zone hba1

Zone Name                Zone Member
=====
hba1                    21:00:00:24:ff:7b:f5:c8
                        10:00:00:90:fa:b8:22:19
                        21:00:00:24:ff:7f:ce:ee
                        21:00:00:24:ff:7f:ce:ef

```

Supported Releases 10.3.1E or later

show fc zoneset

Displays the FC zonesets, the zones in the zoneset, and the zone members.

Syntax `show fc zoneset [active | zoneset-name]`

Parameters `zoneset-name` — Enter the FC zoneset name.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fc zoneset
ZoneSetName      ZoneName      ZoneMember
=====
set              hba1          21:00:00:24:ff:7b:f5:c8
                10:00:00:90:fa:b8:22:19
                21:00:00:24:ff:7f:ce:ee
                21:00:00:24:ff:7f:ce:ef

                hba2          20:01:00:0e:1e:e8:e4:99
                50:00:d3:10:00:ec:f9:1b
                50:00:d3:10:00:ec:f9:05
                50:00:d3:10:00:ec:f9:1f
                20:35:78:2b:cb:6f:65:57

vFabric id: 100
Active Zoneset: set
ZoneName          ZoneMember
=====
hba2              20:01:00:0e:1e:e8:e4:99
                20:35:78:2b:cb:6f:65:57
                50:00:d3:10:00:ec:f9:05
                50:00:d3:10:00:ec:f9:1b
                50:00:d3:10:00:ec:f9:1f

hba1              *10:00:00:90:fa:b8:22:19
                *21:00:00:24:ff:7b:f5:c8
                21:00:00:24:ff:7f:ce:ee
                21:00:00:24:ff:7f:ce:ef
```

Example (active zoneset)

```
OS10# show fc zoneset active

vFabric id: 100
Active Zoneset: set
ZoneName          ZoneMember
=====
hba2              20:01:00:0e:1e:e8:e4:99
                20:35:78:2b:cb:6f:65:57
                50:00:d3:10:00:ec:f9:05
                50:00:d3:10:00:ec:f9:1b
                50:00:d3:10:00:ec:f9:1f

hba1              *10:00:00:90:fa:b8:22:19
                *21:00:00:24:ff:7b:f5:c8
                21:00:00:24:ff:7f:ce:ee
                21:00:00:24:ff:7f:ce:ef
```

Example (with zoneset name)

```
OS10# show fc zoneset set
ZoneSetName      ZoneName      ZoneMember
=====
set              hba1          21:00:00:24:ff:7b:f5:c8
                10:00:00:90:fa:b8:22:19
                21:00:00:24:ff:7f:ce:ee
                21:00:00:24:ff:7f:ce:ef

                hba2          20:01:00:0e:1e:e8:e4:99
                50:00:d3:10:00:ec:f9:1b
                50:00:d3:10:00:ec:f9:05
                50:00:d3:10:00:ec:f9:1f
                20:35:78:2b:cb:6f:65:57
```

Supported Releases

10.3.1E or later

zone default-zone permit

Enables access between all logged-in FC nodes of vfabric in the absence of an active zoneset configuration. A default zone advertises a maximum of 255 members in the registered state change notification (RSCN) message.

Syntax	<code>zone default-zone permit</code>
Parameters	None
Defaults	Not configured
Command Mode	Vfabric CONFIGURATION
Usage Information	The <code>no</code> version of this command disables access between FC nodes in the absence of an active zoneset.
Example	<pre>OS10(config)# vfabric 100 OS10(conf-vfabric-100)# zone default-zone permit</pre>
Supported Releases	10.3.1E or later

zoneset activate

Activates an existing zoneset. You can activate only one zoneset in a vfabric.

Syntax	<code>zoneset activate zoneset-name</code>
Parameters	<code>zoneset-name</code> — Enter an existing zoneset name.
Defaults	Not configured
Command Mode	Vfabric CONFIGURATION
Usage Information	The <code>no</code> version of this command deactivates the zoneset. After you disable an active zoneset, the <code>zone default-zone permit</code> command configuration takes effect. Based on this configuration, the default zone allows or denies access between all the logged-in FC nodes of the vfabric.
Example	<pre>OS10(config)# vfabric 100 OS10(conf-vfabric-100)# zoneset activate set</pre>
Supported Releases	10.3.1E or later

NPG commands

The following commands are supported on NPG mode:

fc port-mode F

Configures port mode on Fibre Channel interfaces.

Syntax	<code>fc port-mode F</code>
Parameters	None
Defaults	N_Port
Command Mode	Fibre Channel INTERFACE
Usage Information	Configure the port mode when the port is in <code>shut</code> mode and when NPG mode is enabled. The <code>no</code> version of this command returns the port mode to default.

Example

```
OS10(config)# interface fibrechannel 1/1/1
OS10(conf-if-fc1/1/1)# fc port-mode F
```

Supported Releases

10.4.1.0 or later

feature fc npg

Enables the NPG mode globally.

Syntax

feature fc npg

Parameters

None

Defaults

Disabled

Command Mode

CONFIGURATION

Usage Information

The no version of this command disables the NPG mode. You can enable only any one of the following at a time: F_Port, FIP snooping bridge, or NPG.

Example

```
OS10(config)# feature fc npg
```

Supported Releases

10.4.0E(R1) or later

show npg devices

Displays the NPG devices connected to the switch.

Syntax

show npg devices [brief]

Parameters

None

Default

Not configured

Command Mode

EXEC

Usage Information

Use the brief option to display minimum details.

Example

```
OS10# show npg devices
Node[0]:
Node MAC :d4:ae:52:1a:ee:54
Node Interface :Eth 1/1/31
FCF MAC :14:18:77:20:7c:e3
Fabric Interface :Fc 1/1/20
FCoE Vlan :100
Vfabric Id :10
ENode WWPN :20:01:d4:ae:52:1a:ee:54
ENode WWNN :20:00:d4:ae:52:1a:ee:54
FCoE MAC :0e:fc:00:01:04:02
FC-ID :01:04:02
Login Method :FLOGI
Time since discovered(in Secs) :6253
Status :LOGGED_IN
```

```
OS10# show npg devices
Node[0]:
Node MAC :d4:ae:52:1a:ee:54
Node Interface :Eth 1/1/31
FCF MAC :14:18:77:20:7c:e3
Fabric Interface :Fc 1/1/20
FCoE Vlan :100
```

```

Vfabric Id :10
ENode WWPN :20:01:d4:ae:52:1a:ee:54
ENode WWNN :20:00:d4:ae:52:1a:ee:54
FCoE MAC :0e:fc:00:01:04:02
FC-ID :01:04:02
Login Method :FLOGI
Time since discovered(in Secs) :6253
Status :LOGGED_IN

FC Node[1]:
Node Interface :Fc 1/1/6
Fabric Interface :Fc 1/1/5
Vlan :100
Vfabric Id :10
WWPN :20:07:00:11:0d:a8:d4:00
WWNN :20:07:00:11:0d:a8:d4:00
FC-ID :02:34:01
Login Method :FLOGI
Time since discovered(in Secs) :23
Status :LOGGED_IN

```

Example (brief)

```

OS10# show npg devices brief

Total NPG Devices = 3
ENode-Interface ENode-WWPN FCoE-Vlan Fabric-Intf Vfabric-Id LoginMethod Status
-----
Eth 1/1/31 20:01:d4:ae:52:1a:ee:54 100 Fc 1/1/20 10 FLOGI LOGGED_IN
Eth 1/1/31 20:01:d4:ae:52:1a:ee:5f 100 Fc 1/1/20 10 FLOGI LOGGED_IN
Eth 1/1/31 20:01:d4:ae:52:1a:f8:9c 100 Fc 1/1/20 10 FLOGI LOGGED_IN

```

```

OS10# show npg devices brief
Total NPG Devices = 4
ENode-Interface ENode-WWPN FCoE-Vlan Fabric-Intf Vfabric-Id LoginMethod Status
-----
Eth 1/1/31 20:01:d4:ae:52:1a:ee:54 100 Fc 1/1/20 10 FLOGI LOGGED_IN
Eth 1/1/31 20:01:d4:ae:52:1a:ee:5f 100 Fc 1/1/20 10 FLOGI LOGGED_IN
Eth 1/1/31 20:01:d4:ae:52:1a:f8:9c 100 Fc 1/1/20 10 FLOGI LOGGED_IN

Node-Interface      WWPN                      Vlan      Fabric-Intf      Vfabric-Id L
-----
Fc 1/1/6            20:07:00:11:0d:a8:d4:00  100       Fc 1/1/5         10         F

```

Supported Releases 10.4.0E(R1) or later

F_Port and NPG commands

The following commands are supported on both F_Port and NPG modes:

clear fc statistics

Clears FC statistics for specified vfabric or fibre channel interface.

Syntax `clear fc statistics [vfabric vfabric-ID | interface fibrechannel]`

- Parameters**
- *vfabric-ID* — Enter the vfabric ID.
 - *fibrechannel* — Enter the fibre channel interface name.

Default Not configured

Command Mode EXEC

Usage None

Information

Example

```
OS10# clear fc statistics vfabric 100
OS10# clear fc statistics interface fibrechannel1/1/25
```

Supported Releases

10.4.1.0 or later

fcoe

Adds FCoE parameters to vfabric.

Syntax

```
fcoe {fcmmap fc-map | fcf-priority fcf-priority-value | fka-adv-period adv-period | vlan-priority vlan-priority-value | keep-alive}
```

Parameters

- *fc-map* — Enter the FC map ID, ranging from 0x0efc00-0x0efcff.
- *fcf-priority-value* — Enter the FCF priority value, ranging from 1 to 255.
- *adv-period* — Enter the FCF keepalive advertisement period ranging from 8 to 90 seconds.
- *vlan-priority-value* — Enter the VLAN priority value, ranging from 0 to 7.

Defaults

- *fcmmap*—0x0EFC00
- *fcf-priority*—128
- *fka-adv-period*—8
- *vlan-priority*—3
- *keep-alive*—True

Command Mode

Vfabric CONFIGURATION

Usage Information

The no version of this command disables the FCoE parameters.

Example

```
OS10(config)# vfabric 10
OS10(conf-vfabric-10)# name 10
OS10(conf-vfabric-10)# fcoe fcmmap 0x0efc01
OS10(conf-vfabric-10)# fcoe fcf-priority 128
OS10(conf-vfabric-10)# fcoe fka-adv-period 8
OS10(conf-vfabric-10)# fcoe vlan-priority 3
```

Supported Releases

10.3.1E or later

name

Configures a vfabric name.

Syntax

```
name vfabric-name
```

Parameters

vfabric-name — Enter a name for the vfabric.

Defaults

Not configured

Command Mode

Vfabric CONFIGURATION

Usage Information

The no version of this command removes the vfabric name..

Example

```
OS10(config)# vfabric 100
OS10(conf-vfabric-100)# name test_vfab
```

Supported Releases

10.3.1E or later

show fc statistics

Displays the FC statistics.

Syntax `show fc statistics {vfabric vfabric-ID | interface fibrenchannel}`

- Parameters**
- *vfabric-ID* — Enter the vfabric ID.
 - *fibrenchannel* — Enter the fibre channel interface name.

Default Not configured

Command Mode EXEC

Usage Information None

Example (vfabric)

```
OS10# show fc statistics vfabric 100
Number of FLOGI                : 43
Number of FDISC                : 6
Number of FLOGO                : 0
Number of FLOGI Accepts       : 43
Number of FLOGI Rejects       : 0
Number of FDISC Accepts       : 6
Number of FDISC Rejects       : 0
Number of FLOGO Accepts       : 0
Number of FLOGO Rejects       : 0
```

Example (interface)

```
OS10# show fc statistics interface fibrenchannel1/1/25:1
Number of FLOGI                : 1
Number of FDISC                : 0
Number of FLOGO                : 0
Number of FLOGI Accepts       : 1
Number of FLOGI Rejects       : 0
Number of FDISC Accepts       : 0
Number of FDISC Rejects       : 0
Number of FLOGO Accepts       : 0
Number of FLOGO Rejects       : 0
```

Supported Releases 10.3.1E or later

show fc switch

Displays the FC switch parameters.

Syntax `show fc switch`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fc switch
Switch Mode : FPORT
Switch WWN  : 10:00:14:18:77:20:8d:cf
```

Supported Releases 10.3.1E or later

show running-config vfabric

Displays the running configuration for vfabric.

Syntax show running-config vfabric

Parameters None

Defaults Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show running-configuration vfabric
!
vfabric 10
vlan 100
fcoe fcmmap 0xEFC00
fcoe fcf-priority 140
fcoe fka-adv-period 13
```

Supported Releases 10.4.0E(R1) or later

show vfabric

Displays vfabric details.

Syntax show vfabric

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show vfabric
Fabric Name          100
Fabric Type          FPORT
Fabric Id            100
Vlan Id              1023
FC-MAP               0xEFC64
Config-State        ACTIVE
Oper-State           UP
=====
Switch Config Parameters
=====
Domain ID            100
=====
Switch Zoning Parameters
=====
Default Zone Mode:   Allow
Active ZoneSet:      set
=====
Members
fibrechannell1/1/1
fibrechannell1/1/2
fibrechannell1/1/3
fibrechannell1/1/4
fibrechannell1/1/5
fibrechannell1/1/6
fibrechannell1/1/7
fibrechannell1/1/8
```

```

fibrechannell1/1/9
fibrechannell1/1/10
fibrechannell1/1/11
fibrechannell1/1/12
fibrechannell1/1/15
fibrechannell1/1/17
fibrechannell1/1/18
fibrechannell1/1/19
fibrechannell1/1/20
fibrechannell1/1/21
fibrechannell1/1/22
fibrechannell1/1/23
fibrechannell1/1/24
fibrechannell1/1/25:1
fibrechannell1/1/29:1
fibrechannell1/1/30:1
fibrechannell1/1/30:3
=====

```

Supported Releases 10.3.1E or later

vfabric

Configures a virtual fabric (vfabric). Enable the F_Port before configuring a vfabric. You can configure only one vfabric in F_Port mode. The vfabric becomes active only when you configure the vfabric with a valid VLAN and FC map. Do not use spanned VLAN as vfabric VLAN.

Syntax `vfabric fabric-ID`

Parameters `fabric-ID` — Enter the fabric ID, from 1 to 255.

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the vfabric. You can remove a vfabric only when it is not applied on any interfaces.

Example

```
OS10(config)# vfabric 100
```

Supported Releases 10.3.1E or later

vfabric (interface)

Applies an existing vfabric to an Ethernet or FC interface.

Syntax `vfabric fabric-ID`

Parameters `fabric-ID` — Enter the fabric ID, from 1 to 255.

Defaults Not configured

Command Mode INTERFACE

Usage Information The `no` version of this command removes the vfabric from the interface.

Example

```
OS10(config)# interface fibrechannel 1/1/1
OS10(conf-if-fc1/1/1)# vfabric 100
```

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# vfabric 200
```

Supported Releases 10.3.1E or later

vlan

Associate an existing VLAN ID to the vfabric to carry traffic. Create the VLAN ID before associating it to the vfabric. Do not use spanned VLAN as vfabric VLAN.

Syntax `vlan vlan-ID`

Parameters *vlan-ID* — Enter an existing VLAN ID.

Defaults Not configured

Command Mode Vfabric CONFIGURATION

Usage Information The `no` version of this command removes the VLAN ID from the vfabric.

Example

```
OS10(config)# interface vlan 1023
100OS10(conf-if-vl-1023)# exit
OS10(config)# vfabric 100
OS10(conf-vfabric-100)# vlan 1023
```

Supported Releases 10.3.1E or later

FIP-snooping commands

The following commands are supported on FIP-snooping mode:

feature fip-snooping

Enables the FIP snooping feature globally.

Syntax `feature fip-snooping`

Parameters None

Defaults Disabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables FIP snooping.

Example

```
OS10(config)# feature fip-snooping
```

Supported Releases 10.4.0E(R1) or later

fip-snooping enable

Enables FIP snooping on specified VLAN.

Syntax `fip-snooping enable`

Parameters None

Defaults Disabled

Command Mode VLAN INTERFACE

Usage Information	The <code>no</code> version of this command disables FIP snooping on the VLAN. You can enable FIP snooping on a VLAN only after enabling the FIP snooping feature globally using the <code>feature fip-snooping</code> command. OS10 supports FIP snooping on a maximum of 12 VLANs.
Example	<pre>OS10(config)# interface vlan 3 OS10(config-if-vl-3)# fip-snooping enable</pre>
Supported Releases	10.4.0E(R1) or later

fip-snooping fc-map

Configure the FC map value for specific VLAN.

Syntax	<code>fip-snooping fc-map <i>fc-map</i></code>
Parameters	<i>fc-map</i> — Enter the FC map ID, ranging from 0xefc00 to 0xefc0ff.
Defaults	Not configured
Command Mode	VLAN INTERFACE
Usage Information	The <code>no</code> version of this command disables the FC map configuration.
Example	<pre>OS10(config)# interface vlan 3 OS10(config-if-vl-3)# fip-snooping fc-map 0xEFC64</pre>
Supported Releases	10.4.0E(R1) or later

fip-snooping port-mode fcf

Sets the FIP snooping port mode to FCF for interfaces.

Syntax	<code>fip-snooping port-mode fcf</code>
Parameters	None
Defaults	ENode port mode
Command Mode	INTERFACE
Usage Information	By default, the port mode of an interface is set to ENode. Use this command to change the port mode to FCF. You can set the port mode to FCF only after enabling the FIP snooping feature. The <code>no</code> version of this command resets the port mode to ENode.
Example	<pre>OS10(config)# interface ethernet 1/1/32 OS10(config-if-eth1/1/32)# fip-snooping port-mode fcf</pre>
Supported Releases	10.4.0E(R1) or later

FCoE commands

The following commands are supported on all the three modes: F_Port, NPG, and FSB.

clear fcoe database

Clears the FCoE database for the specified VLAN.

Syntax	<code>clear fcoe database vlan <i>vlan-id</i> {<i>enode enode-mac-address</i> <i>fcf fcf-mac-address</i> <i>session fcoe-mac-address</i>}</code>
Parameters	<ul style="list-style-type: none">• <i>vlan-id</i> — Enter the VLAN ID.• <i>enode-mac-address</i> — Enter the MAC address of ENode.• <i>fcf-mac-address</i> — Enter the MAC address of FCF.• <i>fcoe-mac-address</i> — Enter the MAC address of FCoE session.
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	<pre>OS10# clear fcoe database vlan 100 enode aa:bb:cc:00:00:00</pre>
Supported Releases	10.4.0E(R1) or later

clear fcoe statistics

Clears FCoE statistics for specified interface.

Syntax	<code>clear fcoe statistics [<i>interface interface-type</i>]</code>
Parameters	<i>interface-type</i> — (Optional) Enter the interface type. The interface may be ethernet, VLAN, or port-channel.
Default	Not configured
Command Mode	EXEC
Usage Information	If you do not specify the <i>interface interface-type</i> information, then the command clears the statistics for all the interfaces and VLANs.
Example	<pre>OS10# clear fcoe statistics interface ethernet 1/1/1 OS10# clear fcoe statistics interface port-channel 5</pre>
Supported Releases	10.4.0E(R1) or later

fcoe max-sessions-per-enodemac

Configures the maximum number of sessions allowed for an ENode.

Syntax	<code>fcoe max-sessions-per-enodemac <i>max-session-number</i></code>
Parameters	<i>max-session-number</i> — Enter the maximum number of sessions to be allowed, ranging from 1 to 64.
Defaults	32
Command Mode	CONFIGURATION
Usage Information	The no version of this command resets the number of sessions to the default value.
Example	<pre>OS10(config)# fcoe max-sessions-per-enodemac 64</pre>

Supported Releases 10.4.0E(R1) or later

fcoe priority-bits

Configures the priority bits for FCoE application TLVs.

Syntax `fcoe priority-bits priority-value`

Parameter *priority-value* — Enter PFC priority value advertised in FCoE application TLV. You can enter one of the following values: 0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, or 0x80.

Default 0x08

Command Mode CONFIGURATION

Usage Information You can configure only one PFC priority at a time. The `no` version of this command returns the configuration to default value.

Example

```
OS10(config)# fcoe priority-bits 0x08
```

Supported Releases 10.4.0E(R3) or later

lldp tlv-select dcbxp-appln fcoe

Enables FCoE application TLV for an interface.

Syntax `lldp tlv-select dcbxp-appln fcoe`

Parameter None

Default Enabled

Command Mode INTERFACE

Usage Information The default priority value advertised in FCoE application TLV is 3. If the PFC configuration in an interface matches 3, then the FCoE application TLV is advertised as 3. Otherwise, FCoE application TLV is not advertised.

When you configure the application priority using `fcoe priority-bits` command, the configured value is advertised in the TLV, which is not dependent on PFC configuration.

The `no` version of this command disables the FCoE application TLV.

Example

```
OS10(conf-if-eth1/1/1)# lldp tlv-select dcbx-appln fcoe
```

Supported Releases 10.4.0E(R3) or later

show fcoe enode

Displays the details of ENodes connected to the switch.

Syntax `show fcoe enode [enode-mac-address]`

Parameters *enode-mac-address* — (Optional) Enter the MAC address of ENode. This option displays details pertaining to the specified ENode.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fcoe enode
Enode MAC          Enode Interface  VLAN FCFs Sessions
-----
d4:ae:52:1b:e3:cd  ethernet1/1/54   100  1     5
```

Supported Releases 10.4.0E(R1) or later

show fcoe fcf

Displays the details of FCFs connected to the switch.

Syntax `show fcoe [fcf-mac-address]`

Parameters `fcf-mac-address` — (Optional) Enter the MAC address of FCF. This option displays details of specified FCF.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fcoe fcf
FCF MAC          FCF Interface  VLAN FC-MAP    FKA_ADV_PERIOD No. of
Enodes
-----
54:7f:ee:37:34:40 port-channel5  100  0e:fc:00  4000          2
```

Supported Releases 10.4.0E(R1) or later

show fcoe sessions

Displays the details of established FCoE sessions.

Syntax `show fcoe sessions [interface vlanvlan-id]`

Parameters `vlan-id` — (Optional) Enter the VLAN ID. This option displays the sessions established on the specified VLAN.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fcoe sessions
Enode MAC          Enode Interface  FCF MAC          FCF interface  VLAN
FCoE MAC          FC-ID    PORT  WWPN          PORT  WWNN
-----
aa:bb:cc:00:00:00 ethernet1/1/54   aa:bb:cd:00:00:00 port-channel5
100    0e:fc:00:01:00:01  01:00:01  31:00:0e:fc:00:00:00:00
21:00:0e:fc:00:00:00
aa:bb:cc:00:00:00 ethernet1/1/54   aa:bb:cd:00:00:00 port-channel5
100    0e:fc:00:01:00:02  01:00:02  31:00:0e:fc:00:00:00:00
21:00:0e:fc:00:00:00
```

Supported Releases 10.4.0E(R1) or later

show fcoe statistics

Displays the statistical details of FCoE control plane.

Syntax `show fcoe statistics [interface interface-type]`

Parameters *interface-type* — (Optional) Enter the type of interface. This option displays statistics of the specified interface.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fcoe statistics interface vlan 100
Number of Vlan Requests                :0
Number of Vlan Notifications           :0
Number of Multicast Discovery Solicits  :2
Number of Unicast Discovery Solicits    :0
Number of FLOGI                        :2
Number of FDISC                         :16
Number of FLOGO                         :0
Number of Enode Keep Alive              :9021
Number of VN Port Keep Alive            :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts                 :2
Number of FLOGI Rejects                 :0
Number of FDISC Accepts                 :16
Number of FDISC Rejects                 :0
Number of FLOGO Accepts                 :0
Number of FLOGO Rejects                 :0
Number of CVL                           :0
Number of FCF Discovery Timeouts         :0
Number of VN Port Session Timeouts      :0
Number of Session failures due to Hardware Config :0
```

Supported Releases 10.4.0E(R1) or later

show fcoe system

Displays the system information related to FCoE.

Syntax `show fcoe system`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fcoe system
Mode: FIP Snooping Bridge
FCOE VLAN List (Operational) : 1, 100
FCFs                          : 1
```

```
Enodes           : 2
Sessions         : 17
```

Supported Releases 10.4.0E(R1) or later

show fcoe vlan

Displays the details of FIP snooping operational VLANs and the attributes.

Syntax show fcoe vlan

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show fcoe vlan
* = Default VLAN
VLAN FC-MAP FCFs Enodes Sessions
---- - - - - -
*1 - - - - -
100 0X0EFC00 1 2 17
```

Supported Releases 10.4.0E(R1) or later

Layer 2

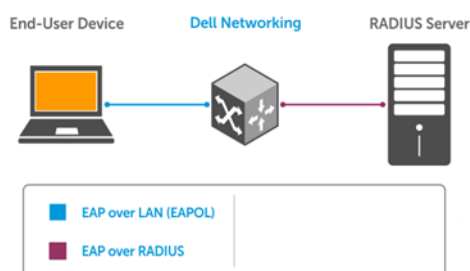
802.1X	Verifies device credentials prior to sending or receiving packets using the Extensible Authentication Protocol (EAP) (see 802.1X Commands).
Link Aggregation Control Protocol (LACP)	Exchanges information between two systems and automatically establishes a LAG between the systems (see LACP Commands).
Link Layer Discovery Protocol (LLDP)	Enables a LAN device to advertise its configuration and receive configuration information from adjacent LLDP-enabled infrastructure devices (see LLDP Commands).
Media Access Control (MAC)	Configures limits, redundancy, balancing, and failure detection settings for devices on your network using tables (see MAC Commands).
Multiple Spanning-Tree (MST)	Mapping of MST instances and allows you to map many VLANs to a single spanning-tree instance, reducing the total number of required instances (see MST Commands).
Rapid Per-VLAN Spanning-Tree Plus (RPVST+)	Combination of rapid spanning-tree and per-VLAN spanning-tree plus for faster convergence and interoperability (see RPVST+ Commands).
Rapid Spanning-Tree Protocol (RSTP)	Faster convergence and interoperability with devices configured with the Spanning-Tree and Multiple Spanning-Tree Protocols (STPs and MSTPs) (see RSTP Commands).
Virtual LANs (VLANs)	Improved security to isolate groups of users into different VLANs and the ability to create a single VLAN across multiple devices (see VLAN Commands).
Port Monitoring (Local/Remote)	Port monitoring of ingress or egress traffic, or both ingress and egress traffic, on specified port(s). Monitoring methods include port-mirroring, remote port monitoring, and encapsulated remote-port monitoring (see Local/Remote Commands).

802.1X

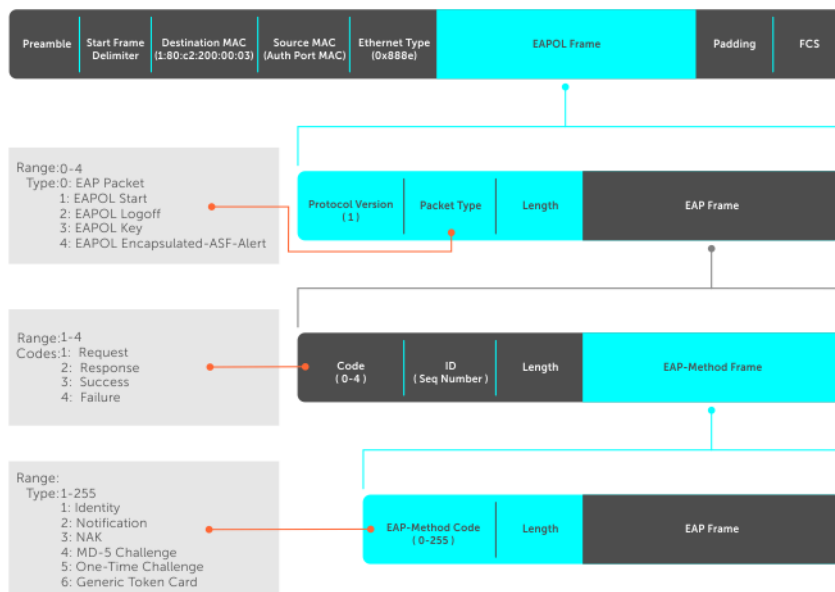
The IEEE 802.1X standard defines a client and server-based access control that prevents unauthorized clients from connecting to a LAN through publicly accessible ports. Authentication is only required in OS10 for inbound traffic. Outbound traffic is transmitted regardless of the authentication state.

802.1X employs EAP to provide device credentials to an authentication server, typically RADIUS, using an intermediary network access device. The network access device mediates all communication between the end user device and the authentication server so the network remains secure.

The network access device uses EAP-over-Ethernet (also known as EAPOL — EAP over LAN) to communicate with the end user device and EAP-over-RADIUS to communicate with the server.



NOTE: OS10 supports only RADIUS as the back-end authentication server.



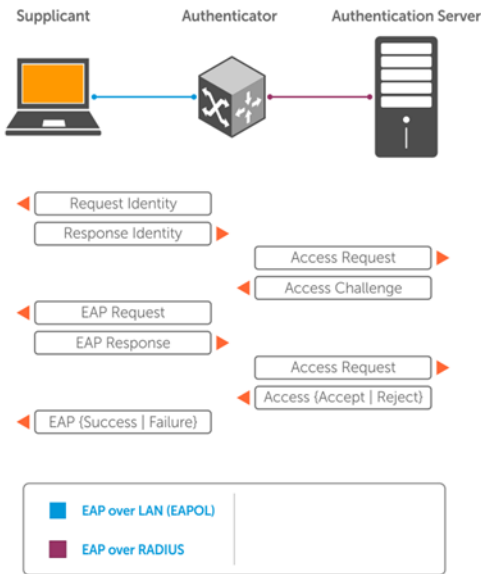
The authentication process involves three devices:

- **Supplicant** — The device attempting to access the network performs the role of supplicant. Regular traffic from this device does not reach the network until the port associated to the device is authorized. Prior to that, the supplicant can only exchange 802.1x messages (EAPOL frames) with the authenticator.
- **Authenticator** — The authenticator is the gate keeper of the network, translating and forwarding requests and responses between the authentication server and the supplicant. The authenticator also changes the status of the port based on the results of the authentication process. The authenticator is executed on the Dell device.
- **Authentication-server** — The authentication-server selects the authentication method, verifies the information the supplicant provides, and grants network access privileges.

Port authentication

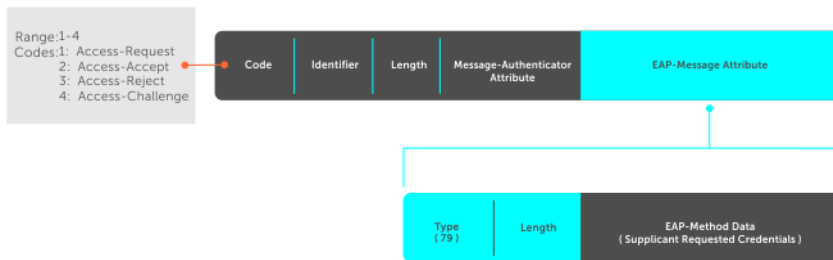
The process begins when the authenticator senses a link status change from down to up:

1. The authenticator requests that the supplicant identify itself using an EAP *Request Identity* frame.
2. The supplicant responds with its identity in an EAP *Response Identity* frame.
3. The authenticator decapsulates the EAP response from the EAPOL frame, encapsulates it in a RADIUS *Access Request* frame, and forwards the frame to the authentication server.
4. The authentication server replies with an *Access Challenge* frame who requests that the supplicant verifies its identity using an EAP-Method. The authenticator translates and forwards the challenge to the supplicant.
5. The supplicant negotiates the authentication method and the supplicant provides the EAP *Request* information in an EAP *Response*. Another *Access Request* frame translates and forwards the response to the authentication server.
6. If the identity information the supplicant provides is valid, the authentication server sends an *Access Accept* frame in which network privileges are specified. The authenticator changes the port state to authorize and forwards an EAP *Success* frame. If the identity information is invalid, the server sends an *Access Reject* frame. If the port state remains unauthorized, the authenticator forwards an EAP *Failure* frame.



EAP over RADIUS

802.1X uses RADIUS to transfer EAP packets between the authenticator and the authentication server. EAP messages are encapsulated in RADIUS packets as an attribute of type, length, value (TLV) format — the type value for EAP messages is 79.

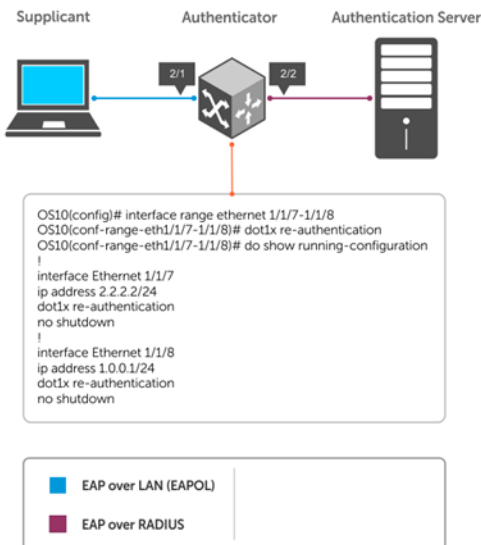


Configure 802.1X

You can configure and enable 802.1X on a port in a single process. OS10 supports 802.1X with EAP-MD5, EAP-OTP, EAP-TLS, EAP-TTLS, PEAPv0, PEAPv1, and MS-CHAPv2 with PEAP and all platforms support RADIUS as the authentication server.

If the primary RADIUS server becomes unresponsive, the authenticator begins using a secondary RADIUS server if configured.

NOTE: 802.1X is not supported on port-channels or port-channel members.



Enable 802.1X

1. Enable 802.1X globally in CONFIGURATION mode.

```
dot1x system-auth-control
```

2. Enter an interface or a range of interfaces in INTERFACE mode.

```
interface range
```

3. Enable 802.1X on the supplicant interface only in INTERFACE mode.

```
dot1x port-control auto
```

Configure and verify 802.1X configuration

```

OS10(config)# dot1x system-auth-control
OS10(config)# interface range 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# dot1x port-control auto
OS10(conf-range-eth1/1/7-1/1/8)# dot1x re-authentication
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7

```

```
802.1x information on ethernet1/1/7
```

```

-----
Dot1x Status:          Enable
Port Control:         AUTO
Port Auth Status:     UNAUTHORIZED
Re-Authentication:    Enable
Tx Period:            60 seconds
Quiet Period:         60 seconds
Supplicant Timeout:   30 seconds
Server Timeout:       30 seconds
Re-Auth Interval:    3600 seconds
Max-EAP-Req:         2
Host Mode:            MULTI_HOST
Auth PAE State:       Initialize
Backend State:        Idle

```

Identity retransmissions

If the authenticator sends a *Request Identity* frame but the supplicant does not respond, the authenticator waits 30 seconds and then re-transmits the frame. There are several reasons why the supplicant might fail to respond — the supplicant may have been booting when the request arrived, there may be a physical layer problem, and so on.

1. Configure the amount of time that the authenticator waits before re-transmitting an EAP *Request Identity* frame in INTERFACE mode (1 to 65535 – 1 year, default 60).

```
dot1x timeout tx-period seconds
```

2. Configure a maximum number of times the authenticator re-transmits a *Request Identity* frame in INTERFACE mode (1 to 10, default 2).

```
dot1x max-req retry-count
```

Configure and verify retransmission time

```
OS10(config)# dot1x system-auth-control
OS10(config)# interface range 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout tx-period 120
OS10(conf-range-eth1/1/7-1/1/8)# dot1x max-req 5
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7
```

```
802.1x information on ethernet1/1/7
-----
Dot1x Status:          Enable
Port Control:          AUTO
Port Auth Status:      UNAUTHORIZED
Re-Authentication:     Enable
Tx Period:             120 seconds
Quiet Period:          60 seconds
Supplicant Timeout:    30 seconds
Server Timeout:        30 seconds
Re-Auth Interval:     3600 seconds
Max-EAP-Req:           5
Host Mode:             MULTI_HOST
Auth PAE State:        Initialize
Backend State:         Idle
```

View interface running configuration

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
 no shutdown
 dot1x max-req 5
 dot1x port-control auto
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
!
interface ethernet1/1/8
 no shutdown
 dot1x max-req 5
 dot1x port-control auto
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
...
```

Failure quiet period

If the supplicant fails the authentication process, the authenticator sends another Request Identity frame after 30 seconds by default. The quiet period is a transmit interval time after a failed authentication.

The Request Identity Re-transmit interval is for an unresponsive supplicant. You can configure the interval for a maximum of 10 times for an unresponsive supplicant.

1. Configure the amount of time that the authenticator waits to re-transmit a *Request Identity* frame after a failed authentication in INTERFACE mode (1 to 65535, default 60 seconds).

```
dot1x timeout quiet-period seconds
```

Configure and verify port authentication

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout quiet-period 120
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7
802.1x information on ethernet1/1/7
-----
Dot1x Status:          Enable
Port Control:         AUTO
Port Auth Status:     UNAUTHORIZED
Re-Authentication:    Enable
Tx Period:            120 seconds
Quiet Period:         120 seconds
Supplicant Timeout:   30 seconds
Server Timeout:       30 seconds
Re-Auth Interval:     3600 seconds
Max-EAP-Req:          5
Host Mode:             MULTI_HOST
Auth PAE State:       Initialize
Backend State:        Idle
```

View interface running configuration

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
 no shutdown
 dot1x max-req 5
 dot1x port-control auto
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
!
interface ethernet1/1/8
 no shutdown
 dot1x max-req 5
 dot1x port-control auto
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
...

```

Port control mode

802.1X requires a port to be in one of three states — force-authorized, force-unauthorized, or auto.

- force-authorized (default)** This is an *authorized state*. A device connected to this port does not use the authentication process but can communicate on the network. Placing the port in this state is same as disabling 802.1X on the port. *force-authorized* is the default mode.
- force-unauthorized** This is an *unauthorized state*. A device connected to a port does not use the authentication process but is *not* allowed to communicate on the network. Placing the port in this state is the same as shutting down the port. Any attempt by the supplicant to initiate authentication is ignored.
- auto** This is an *unauthorized state* by default. A device connected to this port is subject to the authentication process. If the process is successful, the port is authorized and the connected device communicates on the network.

- Place a port in the Auto, Force-authorized (default), or Force-unauthorized state in INTERFACE mode.

```
dot1x port-control {auto | force-authorized | force-unauthorized}
```

Configure and verify force-authorized state

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x port-control force-authorized
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7

802.1x information on ethernet1/1/7
-----
Dot1x Status:          Enable
Port Control:          AUTHORIZED
Port Auth Status:      UNAUTHORIZED
Re-Authentication:    Enable
Tx Period:             120 seconds
Quiet Period:          120 seconds
Supplicant Timeout:    30 seconds
Server Timeout:        30 seconds
Re-Auth Interval:      3600 seconds
Max-EAP-Req:           5
Host Mode:              MULTI_HOST
Auth PAE State:         Initialize
Backend State:          Initialize
```

View interface running configuration

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
 no shutdown
 dot1x max-req 5
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
!
interface ethernet1/1/8
 no shutdown
 dot1x max-req 5
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
...

```

Reauthenticate port

Configures the time period for reauthentication. After the supplicant is authenticated and the port is authorized, configure the authenticator to reauthenticate the supplicant. If you enable reauthentication, the supplicant reauthenticates every 3600 seconds.

- Re-authenticate the supplicant in INTERFACE mode (1 to 65535, default 3600).

```
dot1x timeout re-authperiod seconds
```

Configure and verify reauthentication time period

```
OS10(config)# interface range ethernet 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# dot1x re-authentication
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout re-authperiod 3600
OS10(conf-range-eth1/1/7-1/1/8)# show dot1x interface ethernet 1/1/7

802.1x information on ethernet1/1/7
-----
Dot1x Status:          Enable
Port Control:          AUTHORIZED
Port Auth Status:      UNAUTHORIZED
Re-Authentication:    Enable
```

```

Tx Period:          120 seconds
Quiet Period:       120 seconds
Supplicant Timeout: 30 seconds
Server Timeout:     30 seconds
Re-Auth Interval:  3600 seconds
Max-EAP-Req:        5
Host Mode:          MULTI_HOST
Auth PAE State:     Initialize
Backend State:      Initialize

```

View interface running configuration

```

OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
 no shutdown
 dot1x max-req 5
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout re-authperiod 3600
 dot1x timeout tx-period 120
!
interface ethernet1/1/8
 no shutdown
 dot1x max-req 5
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout re-authperiod 3600
 dot1x timeout tx-period 120
...

```

Configure timeouts

If the supplicant or the authentication server is unresponsive, the authenticator terminates the authentication process after 30 seconds by default. Configure the amount of time the authenticator waits for a response before termination.

- Terminate the authentication process due to an unresponsive supplicant in INTERFACE mode (1 to 65535, default 30).

```
dot1x timeout supp-timeout seconds
```

- Terminate the authentication process due to an unresponsive authentication server in INTERFACE mode (1 to 65535, default 30).

```
dot1x timeout server-timeout seconds
```

Configure and verify server timeouts

```

OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout supp-timeout 45
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout server-timeout 60
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7

802.1x information on ethernet1/1/7
-----
Dot1x Status:          Enable
Port Control:          AUTHORIZED
Port Auth Status:      UNAUTHORIZED
Re-Authentication:     Enable
Tx Period:             120 seconds
Quiet Period:          120 seconds
Supplicant Timeout:    45 seconds
Server Timeout:        60 seconds
Re-Auth Interval:     3600 seconds
Max-EAP-Req:           5
Host Mode:             MULTI_HOST
Auth PAE State:        Initialize
Backend State:         Initialize

```

View interface running configuration

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
  no shutdown
  dot1x max-req 5
  dot1x re-authentication
  dot1x timeout quiet-period 120
  dot1x timeout re-authperiod 3600
  dot1x timeout server-timeout 60
  dot1x timeout supp-timeout 45
  dot1x timeout tx-period 120
!
interface ethernet1/1/8
  no shutdown
  dot1x max-req 5
  dot1x re-authentication
  dot1x timeout quiet-period 120
  dot1x timeout re-authperiod 3600
  dot1x timeout server-timeout 60
  dot1x timeout supp-timeout 45
  dot1x timeout tx-period 120
...

```

802.1X commands

dot1x host-mode

Allows 802.1X authentication for either a single supplicant or multiple supplicants on an interface.

Syntax	<code>dot1x host-mode {multi-host multi-auth}</code>
Parameters	<ul style="list-style-type: none">• <code>multi-host</code> — Allows attachment of multiple hosts to a single 802.1X-enabled port. You can only authorize one of the attached clients for all clients to grant network access. If the port becomes unauthorized (re-authentication fails or receives an EAPOL-logoff message), the device denies network access to all of the attached clients.• <code>multi-auth</code> — Allows 802.1X authentication for each connected host.
Default	Multi-host
Command Mode	INTERFACE
Usage Information	The no version of this command resets the value to the default.
Example	<pre>OS10(conf-range-eth1/1/7-1/1/8)# dot1x host-mode multi-auth</pre>
Supported Releases	10.2.0E or later

dot1x max-req

Changes the maximum number of requests that the device sends to a supplicant before restarting 802.1X authentication.

Syntax	<code>dot1x max-req <i>retry-count</i></code>
Parameters	<code>max-req <i>retry-count</i></code> — Enter the retry count for the request sent to the supplicant before restarting 802.1X reauthentication (1 to 10).
Default	2
Command Mode	INTERFACE

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x max-req 4
```

Supported Releases 10.2.0E or later

dot1x port-control

Controls the 802.1X authentication performed on the interface.

Syntax dot1x port-control {force-authorized | force-unauthorized | auto}

Parameters

- `force-authorized` — Disables 802.1X authentication on the interface and allows all traffic on the interface without authentication.
- `force-unauthorized` — Keeps the port in unauthorized state, ignoring all attempts by the client to authenticate.
- `auto` — Enables the 802.1X authentication on the interface.

Default Force-authorized

Command Mode INTERFACE

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(config)# interface range ethernet 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# dot1x port-control auto
```

Supported Releases 10.2.0E or later

dot1x re-authentication

Enables periodic re-authentication of 802.1X supplicants.

Syntax dot1x re-authentication

Parameters None

Default Disabled

Command Mode INTERFACE

Usage Information The no version of this command disables the periodic re-authentication of 802.1X supplicants.

Example

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x re-authentication
```

Supported Releases 10.2.0E or later

dot1x timeout quiet-period

Sets the number of seconds that the device remains in quiet state following a failed authentication exchange with a supplicant.

Syntax dot1x timeout quiet-period *seconds*

Parameters quiet period *seconds* — Enter the number of seconds for the 802.1X quiet period timeout (1 to 65535).

Default 60 seconds

Command Mode INTERFACE

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout quiet-period 120
```

Supported Releases 10.2.0E or later

dot1x timeout re-authperiod

Sets the number of seconds between re-authentication attempts.

Syntax dot1x timeout re-authperiod *seconds*

Parameters re-authperiod *seconds* — Enter the number of seconds for the 802.1X re-authentication timeout (1 to 65535).

Default 3600 seconds

Command Mode INTERFACE

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout re-authperiod 7200
```

Supported Releases 10.2.0E or later

dot1x timeout server-timeout

Sets the number of seconds that the device waits before retransmitting a packet to the authentication server.

Syntax dot1x timeout server-timeout *seconds*

Parameters server-timeout *seconds* — Enter the number of seconds for the 802.1X server timeout (1 to 65535).

Default 30 seconds

Command Mode INTERFACE

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x server-timeout 60
```

Supported Releases 10.2.0E or later

dot1x timeout supp-timeout

Sets the number of seconds that the device waits for the supplicant to respond to an EAP request frame before the device retransmits the frame.

Syntax dot1x timeout supp-timeout *seconds*

Parameters supp-timeout *seconds* — Enter the number of seconds for the 802.1X supplicant timeout (1 to 65535).

Default 30 seconds

Command Mode INTERFACE

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout supp-timeout 45
```

Supported Releases 10.2.0E or later

dot1x timeout tx-period

Sets the number of seconds that the device waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request.

Syntax dot1x timeout tx-period *seconds*

Parameters tx-period *seconds* — Enter the number of seconds for the 802.1X transmission timeout (1 to 65535).

Default 60 seconds

Command Mode INTERFACE

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout tx-period 120
```

Supported Releases 10.2.0E or later

show dot1x

Displays global 802.1X configuration information.

Syntax show dot1x

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show dot1x
PAE Capability:      Authenticator only
Protocol Version:   2
System Auth Control: Enable
Auth Server:        Radius
```

Supported Releases 10.2.0E or later

show dot1x interface

Displays 802.1X configuration information.

Syntax show dot1x interface ethernet *node/slot/port[:subport]*

Parameters ethernet *node/slot/port[:subport]* — Enter the Ethernet interface information.

Command Mode EXEC

Usage Information Use this command to view the dot1x interface configuration for a specific interface.

Example

```
OS10# show dot1x interface
802.1x information on ethernet1/1/1
-----
Dot1x Status:          Enable
802.1x information on ethernet1/1/2
-----
Dot1x Status:          Enable
802.1x information on ethernet1/1/3
-----
Dot1x Status:          Enable
802.1x information on ethernet1/1/4
-----
Dot1x Status:          Enable
802.1x information on ethernet1/1/5
-----
Dot1x Status:          Enable
802.1x information on ethernet1/1/6
-----
Dot1x Status:          Enable
802.1x information on ethernet1/1/7
-----
Dot1x Status:          Enable
Port Control:          AUTO
Port Auth Status:      UNAUTHORIZED
--more--
```

Example (when dot1x is not enabled globally)

```
OS10# show dot1x interface
802.1x not enabled in the system
OS10#
```

Example (Ethernet)

```
OS10# show dot1x interface ethernet 1/1/7
802.1x information on ethernet1/1/7
-----
Dot1x Status:          Enable
Port Control:          AUTO
Re-Authentication:     Enable
Tx Period:              120 seconds
Quiet Period:           120 seconds
Supplicant Timeout:     45 seconds
Server Timeout:         60 seconds
Re-Auth Interval:       3600 seconds
Max-EAP-Req:            4
Host Mode:              MULTI_AUTH
Port status and State info for Supplicant: 01:80:c2:00:01:1c
Port Auth Status:      UNAUTHORIZED
Untagged VLAN id:       1
Auth PAE State:         Initialize
Backend State:          Idle
```

Supported Releases 10.2.0E or later

Link Aggregation Control Protocol

Group Ethernet interfaces to form a single link layer interface called a LAG or port-channel. Aggregating multiple links between physical interfaces creates a single logical LAG, which balances traffic across the member links within an aggregated Ethernet bundle and increases the uplink bandwidth. If one member link fails, the LAG continues to carry traffic over the remaining links.

You can use LACP to create dynamic LAGs exchanging information between two systems (also called Partner Systems) and automatically establishing the LAG between the systems. LACP permits the exchange of messages on a link to:

- Reach an agreement on the identity of the LAG to which the link belongs.
- Move the link to that LAG.
- Enable the transmission and reception functions.

LACP functions by constantly exchanging custom MAC PDUs across LAN Ethernet links. The protocol only exchanges packets between ports you configure as LACP-capable.

Modes

A LAG includes three configuration modes — on, active, and passive.

- On** Sets the Channeling mode to Static. The interface acts as a member of the static LAG.
- Active** Sets the interface in the Active Negotiating state. LACP runs on any link configured in this mode. A port in Active mode automatically initiates negotiations with other ports by using LACP packets. A port in Active mode can set up a port-channel (LAG) with another port in Active mode or Passive mode.
- Passive** Sets the interface in an Inactive Negotiating state, but LACP runs on the link. A port in Passive mode also responds to negotiation requests (from ports in Active mode). Ports in Passive mode respond to LACP packets. A port in Passive mode cannot set up a LAG with another port in Passive mode.

- There is no dual-membership in static and dynamic LAGs:
 - If a physical interface is a part of a static LAG, the `channel-group id mode active` command is rejected on that interface.
 - If a physical interface is a part of a dynamic LAG, the `channel-group id` command is rejected on that interface.
- You cannot add static and dynamic members to the same LAG.
- There is a difference between the `shutdown` and `no interface port-channel` commands:
 - The `shutdown` command on LAG xyz disables the LAG and retains the user commands.
 - The `no interface port-channel channel-number` command deletes the specified LAG, including a dynamically created LAG. The interfaces restore and are ready for configuration.
- A maximum of 128 port-channels with up to 16 members per channel are allowed.

Configuration

LACP is enabled globally by default. You can configure aggregated ports with compatible active and passive LACP modes to automatically link them.

1. Configure the system priority in CONFIGURATION mode (1 to 65535; the higher the number, the lower the priority; default 32768).

```
lacp system-priority priority-value
```

2. Configure the LACP port priority in INTERFACE mode (1 to 65535; the higher the number, the lower the priority; default 32768).

```
lacp port-priority priority-value
```

3. Configure the LACP rate in INTERFACE mode (default normal).

```
lacp rate [fast | normal]
```

Configure LACP

```
OS10(config)# lacp system-priority 65535
OS10(config)# interface range ethernet 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# lacp port-priority 4096
OS10(conf-range-eth1/1/7-1/1/8)# lacp rate fast
```

Verify LACP configuration

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration
...
!
interface ethernet1/1/7
```

```

lacp port-priority 4096
lacp rate fast
no shutdown
!
interface ethernet1/1/8
lacp port-priority 4096
lacp rate fast
no shutdown
!
...

```

Interfaces

Create a LAG and then add LAG member interfaces. By default, all interfaces are in `no shutdown` and `switchport` modes.

1. Create a LAG in CONFIGURATION mode.

```
interface port-channel port-channel number
```

2. Enter INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
```

3. Set the channel group mode to Active in INTERFACE mode.

```
channel-group number mode active
```

Configure dynamic LAG interfaces

```

OS10(config)# interface port-channel 10
OS10(config-if-po-10)# exit
OS10(config)# interface ethernet 1/1/10
OS10(config-if-eth1/1/10)# no switchport
OS10(config-if-eth1/1/10)# channel-group 10 mode active
OS10(config-if-eth1/1/10)# exit
OS10(config)# interface ethernet 1/1/11
OS10(config-if-eth1/1/11)# no switchport
OS10(config-if-eth1/1/11)# channel-group 10 mode active

```

Rates

Protocol data units (PDUs) are exchanged between port-channel (LAG) interfaces to maintain LACP sessions. PDUs are transmitted at either a slow or fast transmission rate, depending on the LACP timeout value. The timeout value is the amount of time that a LAG interface waits for a PDU from the remote system before bringing the LACP session down.

By default, the LACP rate is `normal` (long timeout). If you configure a `fast` LACP rate, a short timeout sets.

- Set the LACP rate in CONFIGURATION mode.

```
lacp rate [fast | normal]
```

Configure LACP timeout

```
OS10(config-if-eth1/1/29)# lacp rate fast
```

View port status

```

OS10# show lacp port-channel

Port-channel 20 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address f8:b1:56:00:02:33
Partner System ID: Priority 4096, Address 10:11:22:22:33:33
Actor Admin Key 20, Oper Key 20, Partner Oper Key 10
LAG ID 20 is an aggregatable link
A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC,

```

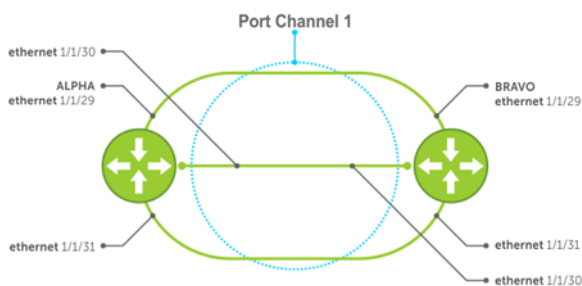
```

I - Collection enabled, J - Collection disabled, K - Distribution enabled,
L - Distribution disabled, M - Partner Defaulted, N - Partner Non-defaulted,
O - Receiver is in expired state, P - Receiver is not in expired state
Port ethernet1/1/14 is Enabled, LACP is enabled and mode is lacp
  Actor Admin: State BCFHJKNO Key 20 Priority 32768
  Oper: State BDEGIKNO Key 20 Priority 32768
  Partner Admin: State BCEGIKNP Key 0 Priority 0
  Oper: State BDEGIKNO Key 10 Priority 32768
Port ethernet1/1/16 is Enabled, LACP is enabled and mode is lacp
  Actor Admin: State BCFHJKNO Key 20 Priority 32768
  Oper: State BDEGIKNO Key 20 Priority 32768
  Partner Admin: State BCEGIKNP Key 0 Priority 0
  Oper: State BDEGIKNO Key 10 Priority 32768

```

Sample configuration

This sample topology is based on two routers — Alpha and Bravo.



Alpha LAG configuration summary

```

OS10(config)# interface port-channel 1
OS10(config-if-po-1)# exit
OS10(config)# interface ethernet 1/1/49
OS10(config-if-eth1/1/49)# no switchport
OS10(config-if-eth1/1/49)# channel-group 1 mode active
OS10(config-if-eth1/1/49)# interface ethernet 1/1/50
OS10(config-if-eth1/1/50)# no switchport
OS10(config-if-eth1/1/50)# channel-group 1 mode active
OS10(config-if-eth1/1/50)# interface ethernet 1/1/51
OS10(config-if-eth1/1/51)# no switchport
OS10(config-if-eth1/1/51)# channel-group 1 mode active

```

Bravo LAG configuration summary

```

OS10(config)# interface port-channel 1
OS10(config-if-po-1)# exit
OS10(config)# interface ethernet 1/1/49
OS10(config-if-eth1/1/49)# no switchport
OS10(config-if-eth1/1/49)# channel-group 1 mode active
OS10(config-if-eth1/1/49)# interface ethernet 1/1/50
OS10(config-if-eth1/1/50)# no switchport
OS10(config-if-eth1/1/50)# channel-group 1 mode active
OS10(config-if-eth1/1/50)# interface ethernet 1/1/51
OS10(config-if-eth1/1/51)# no switchport
OS10(config-if-eth1/1/51)# channel-group 1 mode active

```

Alpha verify LAG port configuration

```

OS10# show lacp port-channel

Port-channel 1 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address 34:17:eb:f2:c7:c4
Partner System ID: Priority 32768, Address 34:17:eb:f2:9b:c4
Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
LACP LAG ID 1 is an aggregatable link

```

```

A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC,
I - Collection enabled, J - Collection disabled, K - Distribution enabled,
L - Distribution disabled, M - Partner Defaulted, N - Partner Non-defaulted,
O - Receiver is in expired state, P - Receiver is not in expired state
Port ethernet1/1/49 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 1 Priority 32768
Port ethernet1/1/50 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 1 Priority 32768
Port ethernet1/1/51 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 1 Priority 32768

```

Bravo verify LAG port configuration

```

bravo# show interface ethernet 1/1/29

Ethernet 1/1/29 is up, line protocol is up
Port is part of Port-channel
Hardware is Dell EMC Eth, address is 90:b1:1c:f4:9b:a2
Current address is 90:b1:1c:f4:9b:a2
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
Wavelength is 25
SFP receive power reading is 0.0
Interface index is 16866812
Internet address is not set
Mode of IPv4 Address Assignment : not set
MTU 1532 bytes, IP MTU bytes
LineSpeed auto
Flowcontrol rx tx
ARP type: ARPA, ARP Timeout: 240
Last clearing of show "interface" counters :
Queuing strategy : fifo
Input statistics:
  466 packets, 45298 octets
  224 64-byte pkts, 1 over 64-byte pkts, 241 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  466 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 465 discarded
Output statistics:
  7840 packets, 938965 octets
  0 64-byte pkts, 1396 over 64-byte pkts, 6444 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  7840 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
  Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
  Output 0 Mbits/sec, 1 packets/sec, 0% of line rate
Time since last interface status change : 01:25:29

```

Verify LAG 1

```

OS10# show interface port-channel 1

Port-channel 1 is up, line protocol is up
Hardware address is Current address is
Interface index is 85886081
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IPv4 Address Assignment : not set
Lag MTU is 1500 ,IP MTU bytes
Linespeed AUTO
Members in this channel ethernet1/1/29 ethernet1/1/30 ethernet1/1/31

```

```

ARP type: ARPA      Arp timeout: 240
Last clearing of "show interface" counters :
Queuing strategy :fifo
Input statistics:
1388 packets, 135026 octets
666 64-byte pkts,1 over 64-byte pkts, 721 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
1388 Multicasts, 0 Broadcasts
0 runs, 0 giants, 0 throttles
0 CRC, 0 overrun, 1387 discarded
Output statistics:
2121444503 packets, 135773749275 octets
2121421152 64-byte pkts,4182 over 64-byte pkts, 19169 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
23351 Multicasts, 0 Broadcasts,2121421152 Unicasts
0 throttles, 143426 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
Output 0 Mbits/sec, 3 packets/sec, 0% of line rate
Time since last interface status change : 01:24:43

```

Verify LAG status

```

OS10# show lacp port-channel

Port-channel 1 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address 90:b1:1c:f4:9b:8a
Partner System ID: Priority 32768, Address 00:01:e8:8a:fd:9e
Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
LACP LAG ID 1 is an aggregatable link

A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC,
I - Collection enabled, J - Collection disabled, K - Distribution enabled,
L - Distribution disabled, M - Partner Defaulted, N - Partner Non-defaulted,
O - Receiver is in expired state, P - Receiver is not in expired state

Port ethernet1/1/29 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State Key 1 Priority 32768
Oper: State Key 1 Priority 32768
Partner Admin: State Key 0 Priority 0
Oper: State Key 1 Priority 32768
Port ethernet1/1/30 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State Key 1 Priority 32768
Oper: State Key 1 Priority 32768
Partner Admin: State Key 0 Priority 0
Oper: State Key 1 Priority 32768
Port ethernet1/1/31 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State Key 1 Priority 32768
Oper: State Key 1 Priority 32768
Partner Admin: State Key 0 Priority 0
Oper: State Key 1 Priority 32768

```

Verify LAG membership

```

OS10# show lacp interface ethernet 1/1/29

Interface ethernet1/1/29 is up
Channel group is 1 port channel is po1
PDUS sent: 17
PDUS rcvd: 11
Marker sent: 0
Marker rcvd: 0
Marker response sent: 0
Marker response rcvd: 0
Unknown packetse rcvd: 0
Illegal packetse rcvd: 0
Local Port:      MAC Address=74:e6:e2:f5:b5:80
System Identifier=32768,32768
Port Identifier=32768,32768
Operational key=1
LACP_Activity=passive

```



```

LACP_Timeout=Long Timeout(30s)
Synchronization=IN_SYNC
Collecting=true
Distributing=true
Partner information refresh timeout=Long Timeout(90s)
Actor Admin State=BCFHJKNO
Actor Oper State=BDEGIKNO
Neighbor: 276
MAC Address=00:00:00:00:00:00
System Identifier=,00:00:00:00:00:00
Port Identifier=0,14:18:77:7a:2d:00
Operational key=1
LACP_Activity=passive
LACP_Timeout=Long Timeout(30s)
Synchronization=IN_SYNC
Collecting=true
Distributing=true
Partner Admin State=BCEGIKNP
Partner Oper State=BDEGIKNO

```

LACP fallback

LACP fallback allows an active LACP interface to establish a port-channel before receiving LACP PDUs from the peer.

This feature is useful in environments where Preboot Execution Environment (PXE) servers are connected to switch with LACP port-channel.

Whenever a PXE server reboots, both the port-channel and ports go down. While rebooting, the ports come up, but not the port-channel. LACP fallback enables the port-channel to be up and keeps sending packets to the PXE server.

The LACP fallback feature adds a member port to LACP port-channel if it does not receive LACP PDUs from the peer for a particular period of time. You can set the timer using the `lacp fallback timeout timer-value` command.

The member port becomes active and sends packets to the PXE server.

When the switch starts receiving LACP PDU, OS10 ungroups the statically added member port from LACP port-channel and resumes with normal LACP functionality..

When you enable LACP fallback, the port that comes up is selected based on the following:

- LACP port priority configuration allows deterministic port allocation. The port with the least priority is placed in the active state when a port-channel is in LACP fallback mode.
- If all the ports in a port-channel have same port priority, the switch internally compares the interface names by base name, module number, port number, and then selects the lowest one to be active. For example, Ethernet 1 is less than Ethernet 2 and hence Ethernet 1 becomes active.
- In a VLT network, if the interface name is the same on both the VLT peers, then the port in switch with lower system MAC address becomes active.

Limitations

- OS10 switches cannot be a PXE client irrespective of whether it acts as a VLT peer or ToR switch.
- If you are configuring LACP fallback in a VLT domain, configure `lacp fallback` commands in both the VLT peers.
- If you do not enable LACP fallback in one of the VLT peers, or configure different time-out values in the peers, then the switch might behave differently.
- The LACP fallback feature adds or groups a member port to the port channel only when the switch does not receive LACP PDUs from the peer, to make the link connected to the PXE client device as operational. As PXE clients handle untagged DHCP request, you need to configure the LACP fallback only on an untagged VLAN to reach the DHCP/PXE server.
- After the LACP fallback election, if a port with lower priority port is configured to be part of the same port-channel, it would trigger re-election.

Configure LACP fallback

1. Enable LACP fallback with the `lacp fallback enable` in port-channel INTERFACE mode.
2. Set a timer for receiving LACP PDUs using `lacp fallback timeout timer-value` in port-channel INTERFACE mode.

Example configuration

```

OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# lacp fallback enable
OS10(conf-if-po-1)# lacp fallback timeout 20

```

View LACP fallback configuration

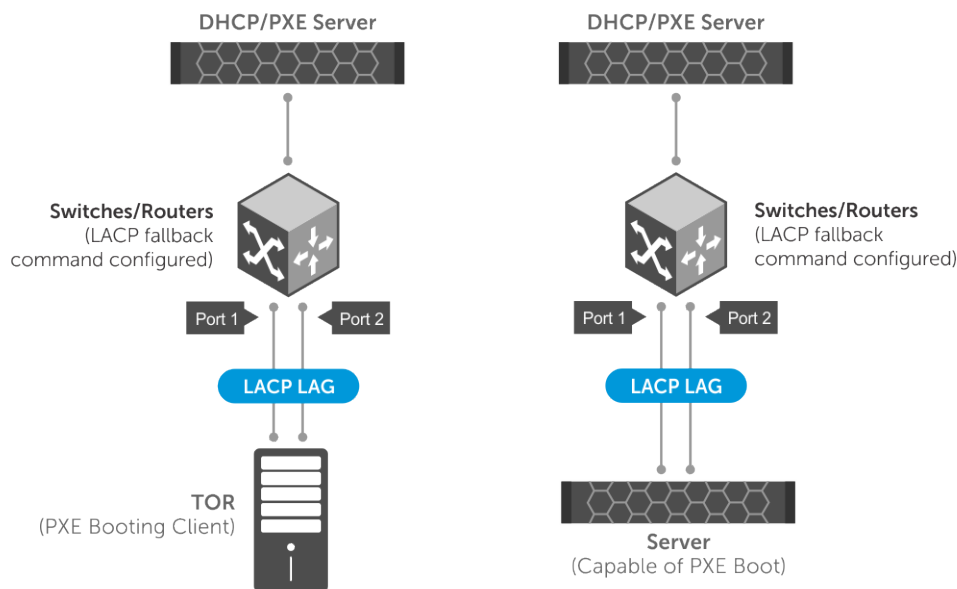
```
OS10# show port-channel summary
```

```
Flags:  D - Down      I - member up but inactive    P - member up and active
        U - Up (port-channel) F - Fallback enabled
```

Group	Port-Channel	Type	Protocol	Member	Ports
1	port-channel1	(UF) Eth	DYNAMIC	1/1/10 (P)	1/1/11 (I)

LACP fallback in non-VLT network

In a non-VLT network, LACP fallback enables rebooting of ToR or server connected to the switch through normal LACP. The other end of the switch is connected to a DHCP/PXE server, as shown in the following illustration:

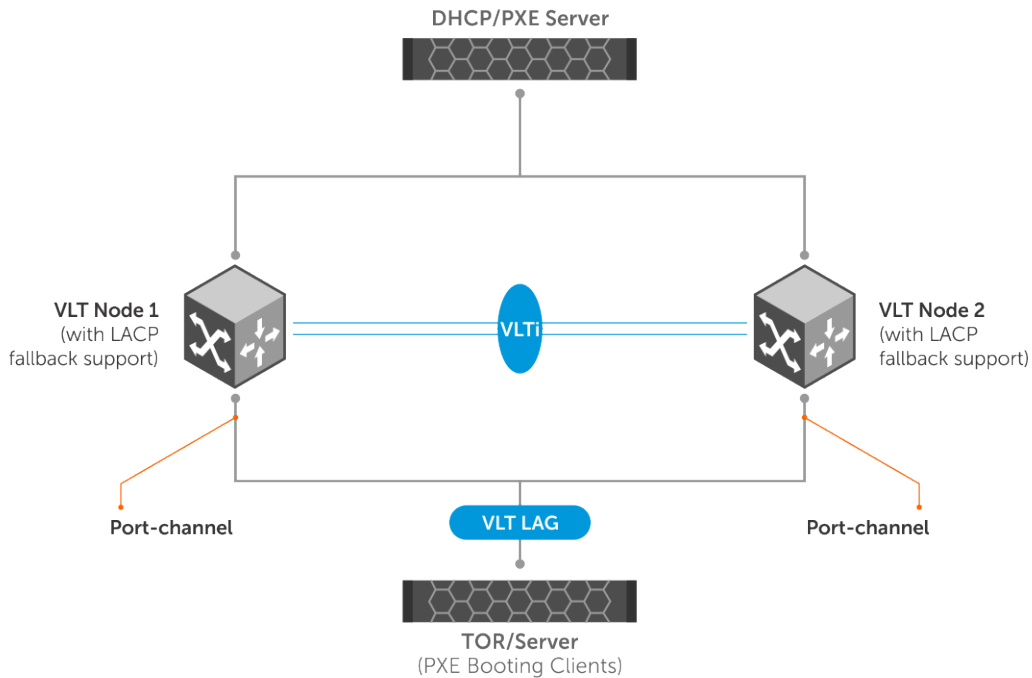


In the above scenario, LACP fallback works as follows:

1. The ToR/server boots up.
2. The switch detects the link that is up and checks fallback enabled status. If fallback is enabled, the device waits for the time-out period for any LACP BPDUs. If there are no LACP BPDUs received within the time period, then the LAG enters into fallback mode and adds the first operationally UP port to the port-channel instead of placing it in an inactive state.
3. Now the ToR/server has one port up and active. The active port sends packets to the DHCP/PXE server.
4. After receiving response from the DHCP server, the ToR/server proceeds to boot from the TFTP/NFS server.
5. When the ToR/server is fully loaded with the boot image and configurations, the server starts sending LACP PDUs.
6. When the switch receives LACP PDUs from ToR/server, the device comes out of the fallback mode and activates the LAG through normal LACP process.

LACP fallback in VLT domain

In a VLT domain, LACP fallback enables rebooting of ToR or server connected to VLT nodes through VLT port-channel. The other end of the VLT nodes are connected to a DHCP/PXE server, as shown in the following illustration:



In the above scenario, LACP fallback works as follows:

1. The ToR/server boots up.
2. One of the VLT peers takes care of controlling the LACP fallback mode. All events are sent to the controlling VLT peer for deciding the port that should be brought up and then the decision is passed on to peer devices.
3. The controlling VLT peer can decide to bring up one of the ports in either the local port-channel or in the peer VLT port-channel.
4. One of the ports, local or peer, becomes active based on the decision of the controlling VLT peer.
5. Now the ToR/server has one port up and active. The active port sends packets to the DHCP/PXE server.
6. After receiving response from the DHCP server, the ToR/server proceeds to boot from the TFTP/NFS server.
7. When the ToR/server is fully loaded with the boot image and configurations, the server starts sending LACP PDUs.
8. When the switch receives LACP PDUs from ToR/server, the controlling VLT peer makes the LACP port to come out of the fallback mode and to resume the normal functionality.

LACP commands

channel-group

Assigns and configures a physical interface to a port-channel group.

Syntax	<code>channel-group <i>number</i> mode {active on passive}</code>
Parameters	<ul style="list-style-type: none"> • <i>number</i> — Enter the port-channel group number (1 to 128). The maximum number of port-channels is 128. The maximum physical port/maximum NPU is supported. • <i>mode</i> — Enter the interface port-channel mode. • <i>active</i> — Enter to enable the LACP interface. The interface is in the Active Negotiating state when the port starts negotiations with other ports by sending LACP packets. • <i>on</i> — Enter so that the interface is not part of a dynamic LAG but acts as a static LAG member. • <i>passive</i> — Enter to only enable LACP if it detects a device. The interface is in the Passive Negotiation state when the port responds to the LACP packets that it receives but does not initiate negotiation until it detects a device.
Default	Not configured
Command Mode	INTERFACE

Usage Information When you delete the last physical interface from a port-channel, the port-channel remains. Configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, OS10 suspends that port in the port-channel. The member ports in a port-channel must have the same setting for link speed capability and duplex capability. The `no` version of this command removes the interface from the port-channel.

Example

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# channel-group 10 mode active
OS10(conf-if-eth1/1/10)# exit
OS10(config)# interface ethernet 1/1/11
OS10(conf-if-eth1/1/11)# channel-group 10 mode active
```

Supported Releases 10.2.0E or later

clear lacp counters

Clears the statistics for all interfaces for LACP groups.

Syntax `clear lacp counters [interface port-channel channel-number]`

Parameters

- `interface port-channel` — (Optional) Enter the interface port-channel number.
- `channel-number` — (Optional) Enter the LACP port-channel number (1 to 128).

Default Not configured

Command Mode EXEC

Usage Information If you use this command for a static port-channel group without enabling the aggregation protocol, the device ignores the command. If you do not enter a port-channel number, the LACP counters for all LACP port groups clear.

Example

```
OS10# clear lacp counters
```

Example (Port-Channel)

```
OS10# clear lacp counters interface port-channel 20
```

Supported Releases 10.2.0E or later

lacp fallback enable

Enables LACP fallback mode.

Syntax `lacp fallback enable`

Parameters None

Default Disabled

Command Mode Port-channel INTERFACE

Usage Information The `no` version of this command disables LACP fallback mode.

Example

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# lacp fallback enable
```

Supported Releases 10.3.2E(R3) or later

lacp fallback preemption

Enables or disables LACP fallback port preemption.

Syntax	<code>lacp fallback preemption {enable disable}</code>
Parameters	<ul style="list-style-type: none">• <code>enable</code>—Enables preemption on the port-channel.• <code>disable</code>—Disables preemption on the port-channel.
Default	Enabled
Command Mode	Port-channel INTERFACE
Usage Information	<p>When you enable preemption, the fallback port election preempts the already elected fallback port and elects a new fallback port.</p> <p>The new port is elected based on the following events:</p> <ul style="list-style-type: none">• When a non-fallback port configured with low priority.• When a low-priority port becomes operationally UP.• When a port with the least numbering is operationally UP.• A port with the lowest priority is elected as fallback port, if non-default LACP port priority is configured on a port even though preemption is disabled.• The <code>lacp fallback preemption disable</code> command is not applicable on port priority events that you have configured or triggered.

Example

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# lacp fallback preemption enable
```

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# lacp fallback preemption disable
```

Supported Releases 10.4.1.0 or later

lacp fallback timeout

Configures LACP fallback time out period.

Syntax	<code>lacp fallback timeout <i>timer-value</i></code>
Parameters	<i>timer-value</i> —Enter the timer values in seconds, ranging from 0 to 100 seconds.
Default	15 seconds
Command Mode	Port-channel INTERFACE
Usage Information	The <code>no</code> version of this command returns the timer to default value.

Example

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# lacp fallback timeout 20
```

Supported Releases 10.3.2E(R3) or later

lacp max-bundle

Configures the maximum number of active members allowed in a port-channel.

Syntax	<code>lacp max-bundle <i>max-bundle-number</i></code>
---------------	---

Parameters	<i>max-bundle-number</i> — Enter the maximum bundle size (1 to 32).
Default	32
Command Mode	INTERFACE
Usage Information	The <code>no</code> version of this command resets the maximum bundle size to the default value.
Example	<pre>OS10(conf-if-po-10)# lacp max-bundle 10</pre>
Supported Releases	10.2.0E or later

lacp port-priority

Sets the priority for the physical interfaces for LACP.

Syntax	<code>lacp port-priority <i>priority</i></code>
Parameters	<i>priority</i> — Enter the priority for the physical interfaces (0 to 65535).
Default	32768
Command Mode	INTERFACE
Usage Information	LACP uses the port priority with the port number to create the port identifier. The port priority decides which ports are put into Standby mode when there is a hardware limitation that prevents all compatible ports from aggregating, or when you have more than eight ports configured for the channel group. When setting the priority, a higher number means a lower priority. The <code>no</code> version of this command returns the port priority to the default value.
Example	<pre>OS10(conf-range-eth1/1/7-1/1/8)# lacp port-priority 32768</pre>
Supported Releases	10.2.0E or later

lacp rate

Sets the rate at which LACP sends control packets.

Syntax	<code>lacp rate {fast normal}</code>
Parameters	<ul style="list-style-type: none"> <code>fast</code> — Enter the fast rate of 1 second. <code>normal</code> — Enter the default rate of 30 seconds.
Default	30 seconds
Command Mode	INTERFACE
Usage Information	Change the LACP timer rate to modify the duration of the LACP timeout. The <code>no</code> version of this command resets the rate to the default value.
Example	<pre>OS10(conf-range-eth1/1/7-1/1/8)# lacp rate fast</pre>
Supported Releases	10.2.0E or later

lacp system-priority

Sets the system priority of the device for LACP.

Parameters	<i>priority</i> — Enter the priority value for physical interfaces (0 to 65535).
-------------------	--

Default	32768
Command Mode	CONFIGURATION
Usage Information	Each device that runs LACP has an LACP system priority value. LACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems. The system ID is unique for each device. The <code>no</code> version of this command resets the system priority to the default value.
Example	<pre>OS10(config)# lacp system-priority 32768</pre>
Supported Releases	10.2.0E or later

show lacp counter

Displays information about LACP statistics.

Syntax	<code>show lacp counter [interface port-channel <i>channel-number</i>]</code>																																																																																																																																																									
Parameters	<ul style="list-style-type: none"> • <code>interface port-channel</code> — (Optional) Enter the interface port-channel. • <code>channel-number</code> — (Optional) Enter the LACP channel group number (1 to 128). 																																																																																																																																																									
Default	Not configured																																																																																																																																																									
Command Mode	EXEC																																																																																																																																																									
Usage Information	All channel groups display if you do not enter the <code>channel-number</code> parameter.																																																																																																																																																									
Example	<pre>OS10# show lacp counter interface port-channel 1</pre> <table border="1"> <thead> <tr> <th>LACPDU Port</th> <th>Marker Sent</th> <th>Marker Recv</th> <th>Response Sent</th> <th>Response Recv</th> <th>LACPDUs Sent</th> <th>LACPDUs Recv</th> <th>Pkts</th> <th>Err</th> </tr> </thead> <tbody> <tr> <td colspan="9">-----</td> </tr> <tr> <td colspan="9">port-channell</td> </tr> <tr> <td>Ethernet1/1</td> <td>554</td> <td>536</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/2</td> <td>527</td> <td>514</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/3</td> <td>535</td> <td>520</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/4</td> <td>515</td> <td>502</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/5</td> <td>518</td> <td>505</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/6</td> <td>540</td> <td>529</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/7</td> <td>541</td> <td>530</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/8</td> <td>547</td> <td>532</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/9</td> <td>544</td> <td>532</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/10</td> <td>513</td> <td>501</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/11</td> <td>497</td> <td>485</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/12</td> <td>493</td> <td>486</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Ethernet1/13</td> <td>492</td> <td>485</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td colspan="9">--more--</td> </tr> </tbody> </table>	LACPDU Port	Marker Sent	Marker Recv	Response Sent	Response Recv	LACPDUs Sent	LACPDUs Recv	Pkts	Err	-----									port-channell									Ethernet1/1	554	536	0	0	0	0	0	0	Ethernet1/2	527	514	0	0	0	0	0	0	Ethernet1/3	535	520	0	0	0	0	0	0	Ethernet1/4	515	502	0	0	0	0	0	0	Ethernet1/5	518	505	0	0	0	0	0	0	Ethernet1/6	540	529	0	0	0	0	0	0	Ethernet1/7	541	530	0	0	0	0	0	0	Ethernet1/8	547	532	0	0	0	0	0	0	Ethernet1/9	544	532	0	0	0	0	0	0	Ethernet1/10	513	501	0	0	0	0	0	0	Ethernet1/11	497	485	0	0	0	0	0	0	Ethernet1/12	493	486	0	0	0	0	0	0	Ethernet1/13	492	485	0	0	0	0	0	0	--more--								
LACPDU Port	Marker Sent	Marker Recv	Response Sent	Response Recv	LACPDUs Sent	LACPDUs Recv	Pkts	Err																																																																																																																																																		

port-channell																																																																																																																																																										
Ethernet1/1	554	536	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/2	527	514	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/3	535	520	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/4	515	502	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/5	518	505	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/6	540	529	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/7	541	530	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/8	547	532	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/9	544	532	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/10	513	501	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/11	497	485	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/12	493	486	0	0	0	0	0	0																																																																																																																																																		
Ethernet1/13	492	485	0	0	0	0	0	0																																																																																																																																																		
--more--																																																																																																																																																										

Supported Releases	10.2.0E or later
---------------------------	------------------

show lacp interface

Displays information about specific LACP interfaces.

Syntax	<code>show lacp interface ethernet <i>node/slot/port</i></code>
Parameters	<code>node/slot/port</code> — Enter the interface information.
Default	Not configured
Command Mode	EXEC
Usage Information	The <code>LACP_activity</code> field displays if you configure the link in Active or Passive port-channel mode. The <code>Port Identifier</code> field displays the port priority as part of the information including the port number. For

example, Port Identifier=0x8000,0x101, where the port priority value is 0x8000 and the port number value is 0x101.

Example

```
OS10# show lacp interface ethernet 1/1/129
Invalid Port id, Max. Port Id is: 32
OS10# show lacp interface ethernet 1/1/29

Interface ethernet1/1/29 is up
  Channel group is 1 port-channel is po1
  PDUS sent: 365
  PDUS rcvd: 17
  Marker sent: 0
  Marker rcvd: 0
  Marker response sent: 0
  Marker response rcvd: 0
  Unknown packetse rcvd: 0
  Illegal packetse rcvd: 0
Local Port: ethernet1/1/29      MAC Address=90:b1:1c:f4:9b:8a
  System Identifier=32768,32768
  Port Identifier=32768,32768
  Operational key=1
  LACP_Activity=passive
  LACP_Timeout=Long Timeout(30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
  Partner information refresh timeout=Long Timeout(90s)
Actor Admin State=BCFHJKNO
Actor Oper State=BDEGIKNO
Neighbor: 178
  MAC Address=00:00:00:00:00:00
  System Identifier=,00:00:00:00:00:00
  Port Identifier=0,00:01:e8:8a:fd:9e
  Operational key=1
  LACP_Activity=passive
  LACP_Timeout=Long Timeout(30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
  Partner Admin State=BCEGIKNP
  Partner Oper State=BDEGIKMO
```

Supported Releases 10.2.0E or later

show lacp neighbor

Displays information about LACP neighbors.

Syntax show lacp neighbor [interface port-channel *channel-number*]

- Parameters**
- interface port-channel — (Optional) Enter the interface port-channel.
 - *channel-number* — (Optional) Enter the port-channel number for the LACP neighbor (1 to 128).

Default Not configured

Command Mode EXEC

Usage Information All channel groups display if you do not enter the *channel-number* parameter.

Example

```
OS10# show lacp neighbor interface port-channel 1

Flags:S-Device is sending Slow LACPDUs F-Device is sending Fast LACPDus
      A-Device is in Active mode      P-Device is in Passive mode
Port-channel port-channell neighbors
Port: ethernet1/1/29
Partner System Priority: 32768
```



```
Partner System ID: 00:01:e8:8a:fd:9e
Partner Port: 178
Partner Port Priority: 32768
Partner Oper Key: 1
Partner Oper State:aggregation synchronization collecting distributing
defaulted expired
```

Supported Releases 10.2.0E or later

show lacp port-channel

Displays information about LACP port-channels.

Syntax `show lacp port-channel [interface port-channel channel-number]`

Parameters

- `interface port-channel` — (Optional) Enter the interface port-channel.
- `channel-number` — (Optional) Enter the port-channel number for the LACP neighbor (1 to 128).

Default Not configured

Command Mode EXEC

Usage Information All channel groups display if you do not enter the *channel-number* parameter.

Example

```
OS10# show lacp port-channel 1

Port-channel 1 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address 90:b1:1c:f4:9b:8a
Partner System ID: Priority 32768, Address 00:01:e8:8a:fd:9e
Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
LACP LAG ID 1 is an aggregatable link
A-Active LACP, B-Passive LACP, C-Short Timeout, D-Long Timeout
E-Aggregatable Link, F-Individual Link, G-IN_SYNC, H-OUT_OF_SYNC,
I-Collection enabled, J-Collection disabled, K-Distribution enabled,
L-Distribution disabled, M-Partner Defaulted, N-Partner Non-defaulted,
O-Receiver is in expired state, P-Receiver is not in expired state
Port ethernet1/1/29 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
  Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
  Oper: State BDEGIKMO Key 1 Priority 32768
```

Supported Releases 10.2.0E or later

show lacp system-identifier

Displays the LACP system identifier for a device.

Syntax `show lacp system-identifier`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information The LACP system ID is a combination of the configurable LACP system priority value and the MAC address. Each system that runs LACP has an LACP system priority value. The default value is 32768 or configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and uses the system priority during negotiation with other devices. A higher system priority value means a lower priority. The system ID is different for each device.

Example

```
OS10# show lacp system-identifier
Actor System ID: Priority 32768, Address 90:b1:1c:f4:9b:8a
```

Supported Releases

10.2.0E or later

Link Layer Discovery Protocol

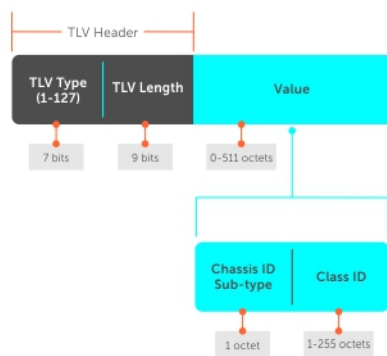
LLDP enables a LAN device to advertise its system and receive system information from adjacent LAN devices.

- LLDP is enabled by default on OS10 interfaces.
- An LLDP-enabled interface can support up to eight neighbors. An OS10 switch supports a maximum of 250 total neighbors per system.
- OS10 devices receive and periodically transmit Link Layer Discovery Protocol Data Units (LLDPDUs), which are data packets. The default transmission interval is 30 seconds.
- LLDPDU information received from a neighbor expires after the default time to live (TTL) value (120 seconds).
- Spanning-tree *blocked* ports allow LLDPDUs.
- 802.1X-controlled ports do not allow LLDPDUs until the connected device is authenticated.
- Link layer discovery protocol-media endpoint discovery (LLDP-MED) is enabled on all interfaces by default.

Protocol data units

LLDP devices exchange system information represented as type, length, and value (TLV) segments:

Type	Information included in the TLV.
Length	Value (in bytes) of the TLV after the Length field.
Value	System information the agent is advertising.



LAN devices transmit LLDPDUs, which encapsulate TLVs, to neighboring LAN devices. LLDP is a one-way protocol and LAN devices (LLDP agents) transmit and/or receive advertisements but they cannot solicit and do not respond to advertisements.

There are three mandatory TLVs followed by zero or more optional TLVs and the end of the LLDPDU TLV. The three mandatory TLVs must be located at the beginning of the LLDPDU in the following order:

- Chassis ID TLV
- Port ID TLV
- Time-to-live TLV

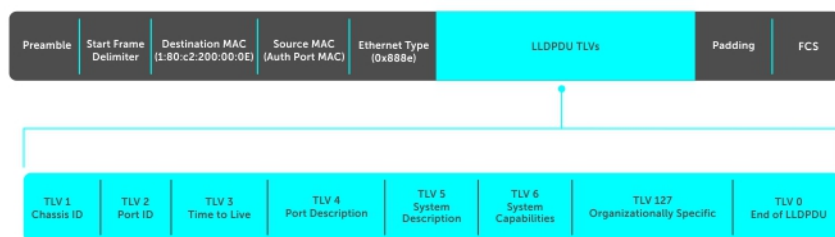
0 — End of LLDPDU Marks the end of an LLDPDU.

1 — Chassis ID Identifies the LAN agent.

2 — Port ID Identifies a port through which the LAN device transmits LLDPDUs.

3 — Time-to-live Number of seconds that the recipient LLDP agent considers the information associated with this MAP identifier to be valid.

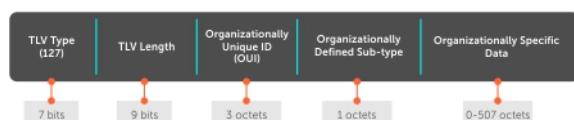
— Optional Includes sub-types of TLVs that advertise specific configuration information. These sub-types are management TLVs, IEEE 802.1, IEEE 802.3, and TIA-1057 organization-specific TLVs.



Optional TLVs

OS10 supports basic TLVs, IEEE 802.1, and 802.3 organizationally-specific TLVs, and TIA-1057 organizationally-specific TLVs. A basic TLV is an optional TLV sub-type. This kind of TLV contains essential management information about the sender.

A professional organization or vendor can define organizationally-specific TLVs. They have two mandatory fields, in addition to the basic TLV fields.



Organizationally-specific TLVs

There are eight TLV types defined by the 802.1 and 802.3 working groups as a basic part of LLDP. Configure OS10 to advertise any or all of these TLVs.

Optional TLVs

4 — Port description User-defined alphanumeric string that describes the port.

5 — System name User-defined alphanumeric string that identifies the system.

6 — System description Detailed description of all components of the system.

7 — System capabilities Determines the capabilities of the system.

8 — Management address Network address of the management interface.

802.1X Organizationally-specific TLVs

127 — Link aggregation Indicates whether the link (associated with the port on which the LLDPDU is transmitted) can be aggregated. Also indicates whether the link is currently aggregated and provides the aggregated port identifier if the link is aggregated.

127 — Port-VLAN ID Untagged VLAN to which a port belongs.

127 — Protocol identity Not supported.

802.3 Organizationally-specific TLVs

127 — MAC/PHY configuration/status Indicates duplex and bit rate capability and the current duplex and bit rate settings of the sending device. Also indicates whether the current settings are due to auto-negotiation or due to manual configuration.

127 — Power via MDI Not supported.

127 — Maximum frame size Maximum frame size capability of the MAC and PHY.


Media endpoint discovery

LLDP media endpoint discovery (LLDP-MED) provides additional organizationally-specific TLVs to allow endpoint devices and network connectivity devices to advertise their characteristics and configuration information.

LLDP-MED endpoint devices are located at the IEEE 802 LAN network edge and participate in IP communication service using the LLDP-MED framework, such as IP phones and conference bridges. LLDP-MED network connectivity devices provide access to the IEEE 802-based LAN infrastructure for LLDP-MED endpoint devices, such as IP phones. An OS10 device acts as an LLDP-MED network connectivity device.

LLDP-MED provides network connectivity devices to:

- Manage inventory
- Manage PoE
- Identify physical location
- Identify network policy

 **NOTE:** Only the Rx function is supported for managing PoE and identifying the physical location. LLDP-MED is designed for but not limited to VoIP endpoints.

Network connectivity device

OS10 can act as an LLDP-MED network connectivity device (Type 4). Network connectivity devices transmit an LLDP-MED capability TLV to endpoint devices and store information that endpoint devices advertise.

127/1 — LLDP-MED capabilities

- If the transmitting device supports LLDP-MED
- What LLDP-MED TLVs are supported
- LLDP device class

127/2 — Network policy Application type, VLAN ID, L2 priority, and DSCP value.

127/3 — Local identification Physical location of the device expressed in one of three formats:

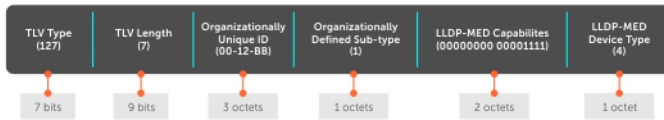
- Coordinate-based LCI
- Civic address LCI
- Emergency call services ELIN

127/4 — Extended power-via-MDI Power requirements, priority, and power status.

LLDP-MED capabilities TLV

The LLDP-MED capabilities TLV communicates the types of TLVs that the endpoint device and the network connectivity device support. The value of the LLDP-MED capabilities field in the TLV is a 2-octet bitmap. Each bit represents an LLDP-MED capability.

LLDP-MED is enabled by default on an interface. If you disable LLDP-MED, use the `lldp med enable` command to re-enable it on an interface. The device transmits MED PDUs only when it receives a TLV from a peer. The device does not otherwise send PDUs — even if MED is enabled on an interface.



LLDP-MED capabilities

Bit 0	LLDP-MED capabilities
Bit 1	Network policy
Bit 2	Location ID
Bit 3	Extended power via MDI-PSE
Bit 4	Extended power via MDI-PD
Bit 5	Inventory
Bits 6-15	Reserved

LLDP-MED device types

0	Type not defined
1	Endpoint class 1
2	Endpoint class 2
3	Endpoint class 3
4	Network connectivity
5-255	Reserved

Network policies TLVs

A network policy in the context of LLDP-MED is a device's VLAN configuration and associated Layer 2 and Layer 3 configurations.

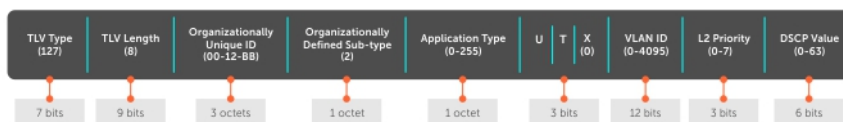
LLDP-MED network policies TLV include:

- VLAN ID
- VLAN tagged or untagged status
- Layer 2 priority
- DSCP value

An integer represents the application type (the Type integer shown in the following table), which indicates a device function for which a unique network policy is defined. An individual LLDP-MED network policy TLV is generated for each application type that you use with OS10 commands (see [Advertise LLDP-MED TLVs](#)).

NOTE: Signaling is a series of control packets that are exchanged between an endpoint device and a network connectivity device to establish and maintain a connection. These signal packets might require a different network policy than the media packets for which a connection is made. In this case, configure the signaling application.

- 0 — Reserved** —
- 1 — Voice** Used for dedicated IP telephony handsets and other appliances supporting interactive voice services.
- 2 — Voice signaling** Used only if voice control packets use a separate network policy than voice data.
- 3 — Guest voice** Used only for a separate limited voice service for guest users with their own IP telephony handsets and other appliances supporting interactive voice services.
- 4 — Guest voice signaling** Used only if guest voice control packets use a separate network policy than voice data.
- 5 — SoftPhone voice** Used for softphone application on a device like PC or laptop. This class does not support multiple VLANs and if required, is configured to use untagged VLAN or a single tagged data specific VLAN.
- 6 — Video conferencing** Used only for dedicated video conferencing and other similar appliances supporting real-time interactive video.
- 7 — Streaming video** Used for broadcast or multicast based video content distribution and similar applications supporting streaming video services that require specific network policy treatment.
- 8 — Video signaling** Used only if video control packets use a separate network policy than video data.
- 9-255 — Reserved** —



Define network policies

You can manually define LLDP-MED network policies. LLDP commands that you configure at CONFIGURATION level are global and affect all interfaces. LLDP commands you configure at INTERFACE level affect only the specific interface.

Create up to 32 network policies and attach the LLDP-MED network policies to a port in CONFIGURATION mode.

- Define the LLDP-MED network policy in CONFIGURATION mode.

```
lldp-med network-policy number app {voice | voice-signaling | guest-voice |
guestvoice-signaling | softphone-voice | streaming-video | video-conferencing | video-
signaling}{vlan vlan-id vlan-type {tag | untag} priority priority dscp dscp value}
```

Configure LLDP-MED network policy for voice applications

```
OS10(config)# lldp med network-policy 10
OS10(config)# lldp med network-policy 10 app
OS10(config)# lldp med network-policy 10 app voice
OS10(config)# lldp med network-policy 1 app voice vlan 10 vlan-type tag
OS10(config)# lldp med network-policy 1 app voice-signaling vlan 10 vlan-type tag
priority 2 dscp 1
```

Packet timer values

LLDPDUs are transmitted periodically. You can configure LLDP packet timer values for LLDPDU transmission.

1. Configure the LLDP packet timer value in CONFIGURATION mode.

```
lldp timer
```

2. Enter the multiplier value for the hold time in CONFIGURATION mode.

```
lldp holdtime-multiplier
```

3. Enter the delay (in seconds) for LLDP initialization on any interface in CONFIGURATION mode.

```
lldp reinit
```

Configure LLDPDU timer

```
OS10(config)# lldp timer 60
OS10(config)# do show lldp timers
LLDP Timers:
Holdtime in seconds: 120
Reinit-time in seconds: 2
Transmit interval in seconds: 60
```

Configure LLDPDU intervals

```
OS10(config)# lldp holdtime-multiplier 2
OS10(config)# do show lldp timers
LLDP Timers:
Holdtime in seconds: 60
Reinit-time in seconds: 2
Transmit interval in seconds: 30
```

Disable and re-enable LLDP

By default, LLDP is enabled for each interface and globally. You can disable LLDP on an interface or globally. If you disable LLDP globally, LLDP is disabled on all interfaces irrespective of whether LLDP is previously enabled or disabled on an interface. When you enable LLDP globally, the LLDP configuration at the interface level takes precedence over the global LLDP configuration.

1. Disable the LLDPDU transmit or receive in INTERFACE mode.

```
no lldp transmit
no lldp receive
```

2. Disable the LLDP holdtime multiplier value in CONFIGURATION mode.

```
no lldp holdtime-multiplier
```

3. Disable the LLDP initialization in CONFIGURATION mode.

```
no lldp reinit
```

4. Disable the LLDP MED in CONFIGURATION or INTERFACE mode.

```
no lldp med
```

5. Disable LLDP TLV in INTERFACE mode.

```
no lldp tlv-select
```

6. Disable LLDP globally in CONFIGURATION mode.

```
no lldp enable
```

Disable LLDP

```
OS10(config)# no lldp timer 100
OS10(config)# no lldp holdtime-multiplier 10
OS10(config)# no lldp reinit 8
```

Disable LLDP interface

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# no lldp med
OS10(config-if-eth1/1/4)# no lldp tlv-select
OS10(config-if-eth1/1/4)# no lldp transmit
OS10(config-if-eth1/1/4)# no lldp receive
```

Enable LLDP

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# lldp transmit
OS10(config-if-eth1/1/1)# lldp receive
```

Disable LLDP globally

```
OS10(config)# no lldp enable
```

Disable and re-enable LLDP on management ports

By default, LLDP is enabled on management ports. You can disable or enable the following LLDP configurations on management ports.

1. Disable the LLDPDU transmit or receive.

```
no lldp transmit
no lldp receive
```

2. Disable LLDP TLVs.

```
no lldp tlv-select basic-tlv {port-description | system-name | system-description |
system-capabilities | management-address}
no lldp tlv-select dot1tlv port-vlan-id
```

Disable LLDP transmit or receive

```
OS10(config)# interface mgmt 1/1/1
OS10(config-if-ma-1/1/1)# no lldp transmit
OS10(config-if-ma-1/1/1)# no lldp receive
```

Enable LLDP transmit or receive

```
OS10(config)# interface mgmt 1/1/1
OS10(config-if-ma-1/1/1)# lldp transmit
OS10(config-if-ma-1/1/1)# lldp receive
```

Disable LLDP TLVs

```
OS10(config)# interface mgmt 1/1/1
OS10(config-if-ma-1/1/1)# no lldp tlv-select basic-tlv system-name system-description
OS10(config-if-ma-1/1/1)# no lldp tlv-select dot1tlv port-vlan-id
```

Enable LLDP TLVs

```
OS10(config)# interface mgmt 1/1/1
OS10(config-if-ma-1/1/1)# lldp tlv-select basic-tlv system-name system-description
OS10(config-if-ma-1/1/1)# lldp tlv-select dot1tlv port-vlan-id
```

Advertise TLVs

Configure the system to advertise TLVs out of all interfaces or specific interfaces. If you configure an interface, only the interface sends LLDPDUs with the specified TLVs.

1. Enable basic TLVs attributes to transmit and receive LLDP packets in INTERFACE mode.

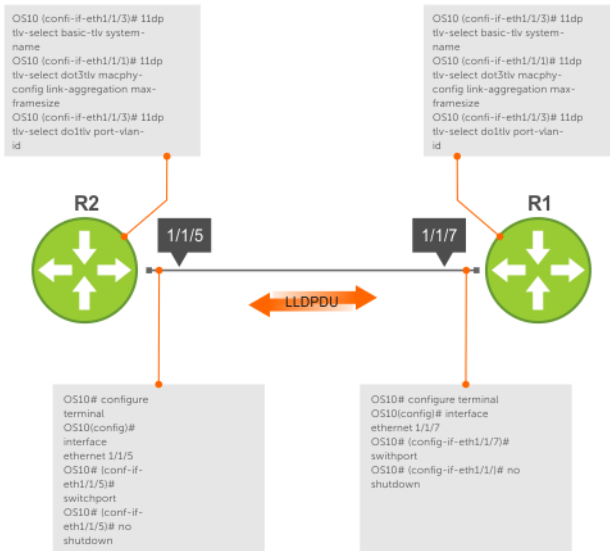
```
lldp tlv-select basic-tlv {port-description | system-name | system-description |
system-capabilities | management-address}
```

2. Enable dot3 TLVs to transmit and receive LLDP packets in INTERFACE mode.

```
lldp tlv-select dot3tlv {macphy-config | max-framesize}
```

3. Enable dot1 TLVs to transmit and receive LLDP packets in INTERFACE mode.

```
lldp tlv-select dot1tlv { port-vlan-id | link-aggregation}
```



Configure advertise TLVs

```
OS10(conf-if-eth1/1/3)# lldp tlv-select basic-tlv system-name
OS10(conf-if-eth1/1/1)# lldp tlv-select dot3tlv macphy-config max-framesize
OS10(conf-if-eth1/1/3)# lldp tlv-select dot1tlv link-aggregation
```

Network policy advertisement

LLDP-MED is enabled on all interfaces by default. Configure OS10 to advertise LLDP-MED TLVs out of configured interfaces. Define LLDP-MED network policies before applying the policies to an interface. Attach only one network policy per interface.

- Define an LLDP-MED network-policy on an interface in CONFIGURATION mode.

```
lldp-med network-policy {add | remove} number
```

- add — Attach the network policy to an interface.
- remove — Remove the network policy from an interface.
- number — Enter a network policy index number (1 to 32).

Configure advertise LLDP-MED network policies

```
OS10(conf-if-eth1/1/5)# lldp-med network-policy add 1
```

Fast start repeat count

Fast start repeat count enables a network connectivity device to advertise itself at a faster rate for a limited amount of time. The fast start timer starts when a network connectivity device receives the first LLDP frame from a newly detected endpoint.

When an LLDP-MED endpoint is newly detected or connected to the network, the `lldp-med fast-start-repeat-count` command enables the network to quickly detect the endpoint. The LLDP-MED fast start repeat count specifies the number of LLDP packets that are sent during the LLDP-MED fast start period. By default, the device sends three packets per interval. Change the number of packets a device sends per second — up to 10.

Rapid availability is crucial for applications such as emergency call service location (E911).

- Enable fast start repeat count which is the number of packets sent during activation in CONFIGURATION mode (1 to 10, default 3).

```
lldp-med fast-start-repeat-count number
```

Configure fast start repeat count

```
OS10(config)# lldp med fast-start-repeat-count 5
```

View LLDP configuration

- View the LLDP configuration in EXEC mode.

```
show running-configuration
```

- View LLDP error messages in EXEC mode.

```
show lldp errors
```

- View LLDP timers in EXEC mode.

```
show lldp timers
```

- View the LLDP traffic in EXEC mode.

```
show lldp traffic
```

View running configuration

```
OS10# show running-configuration
```

View LLDP errors

```
OS10# show lldp errors
Total Memory Allocation Failures : 0
Total Input Queue Overflows : 0
Total Table Overflows : 0
```

View LLDP timers

```
OS10# show lldp timers
LLDP Timers:
Holdtime in seconds: 120
Reinit-time in seconds: 2
Transmit interval in seconds: 30
```

View LLDP global traffic

```
OS10# show lldp traffic
LLDP traffic statistics:
Total Frames Out           : 0
Total Entries Aged         : 0
Total Frames In           : 0
Total Frames Received In Error : 0
Total Frames Discarded     : 0
Total TLVs Unrecognized    : 0
Total TLVs Discarded       : 0
```

View LLDP interface traffic

```
OS10# show lldp traffic interface ethernet 1/1/1
LLDP Traffic Statistics:
Total Frames Out           : 0
Total Entries Aged         : 0
Total Frames In           : 0
Total Frames Received In Error : 0
Total Frames Discarded     : 0
Total TLVS Unrecognized    : 0
Total TLVs Discarded      : 0

LLDP MED Traffic Statistics:
Total Med Frames Out       : 0
Total Med Frames In       : 0
Total Med Frames Discarded : 0
Total Med TLVS Discarded   : 0
Total Med Capability TLVS Discarded: 0
Total Med Policy TLVS Discarded : 0
Total Med Inventory TLVS Discarded : 0
```

Adjacent agent advertisements

- View brief information about adjacent devices in EXEC mode.

```
show lldp neighbors
```

- View all information that neighbors are advertising in EXEC mode.

```
show lldp neighbors detail
```

- View all interface-specific information that neighbors are advertising in EXEC mode.

```
show lldp neighbors interface ethernetnode/slot/port[:subport]
```

View LLDP neighbors

```
OS10# show lldp neighbors
Loc PortID          Rem Host Name      Rem Port Id        Rem Chassis Id
-----
ethernet1/1/2      Not Advertised    fortyGigE 0/56     00:01:e8:8a:fd:35
ethernet1/1/20:1   Not Advertised    GigabitEthernet 1/0 00:01:e8:05:db:05
```

View LLDP neighbors detail

```
OS10# show lldp neighbors interface ethernet 1/1/1 detail

Remote Chassis ID Subtype: Mac address (4)
Remote Chassis ID: 00:13:21:57:ca:40
Remote Port Subtype: Interface name (5)
Remote Port ID: ethernet1/1/10
Remote Port Description: Ethernet port 1
Local Port ID: ethernet1/1/1
Locally assigned remote Neighbor Index: 3
Remote TTL: 120
Information valid for next 105 seconds
Time since last information change of this neighbor: 00:00:15
Remote System Name: LLDP-pkt-gen
Remote Management Address (IPv4): 10.1.1.1
Remote System Desc: LLDP packet generator using scapy
Existing System Capabilities: Repeater, Bridge, Router
Enabled System Capabilities: Repeater, Bridge, Router
Remote Max Frame Size: 0
Remote Aggregation Status: false
MAC PHY Configuration:
  Auto-neg supported: 1
  Auto-neg enabled: 1
  Auto-neg advertised capabilities:
    10BASE-T half duplex mode,
```

```

    10BASE-T full duplex mode,
    100BASE-TX half duplex mode,
    100BASE-TX full duplex mode
MED Capabilities:
  Supported:
    LLDP-MED Capabilities,
    Network Policy,
    Location Identification,
    Extended Power via MDI - PSE,
    Extended Power via MDI - PD,
    Inventory Management
  Current:
    LLDP-MED Capabilities,
    Network Policy,
    Location Identification,
    Extended Power via MDI - PD,
    Inventory Management
  Device Class: Endpoint Class 3
Network Policy:
  Application: voice, Tag: Tagged, Vlan: 50, L2 Priority: 6, DSCP Value: 46
Inventory Management:
  H/W Revision   : 12.1.1
  F/W Revision   : 10.1.9750B
  S/W Revision   : 10.1.9750B
  Serial Number  : B11G152
  Manufacturer   : Dell
  Model          : S6010-ON
  Asset ID       : E1001
Power-via-MDI:
  Power Type: PD Device
  Power Source: Local and PSE
  Power Priority: Low
  Power required: 6.5
Location Identification:
  Civic-based:
    2C:02:49:4E:01:02:54:4E:03:07:43:68:65:6E:6E:61:69:04:06:47:75:69:
    6E:64:79:05:0B:53:49:44:43:4F:49:6E:64:45:73:74:17:05:4F:54:50:2D:
    31
  ECS-ELIN:
    39:39:36:32:30:33:35:38:32:34

```

View LLDP neighbors interface

```

OS10# show lldp neighbors interface ethernet 1/1/1
Loc PortID          Rem Host Name          Rem Port Id          Rem Chassis Id
-----
ethernet1/1/1      OS10                   ethernet1/1/2      4:17:eb:f7:06:c4

```

Time to live

The information received from a neighbor expires after a specific amount of time (in seconds) called TTL. The TTL is the LLDPDU transmit interval (hello) and an integer is called a multiplier. For example, LLDPDU transmit interval (30) times the multiplier (4), (30 x 4 = 120). The default multiplier is 4, with a default TTL of 120 seconds.

1. Adjust the TTL value in CONFIGURATION mode.

```
lldp holdtime-multiplier
```

2. Return to the default multiplier value in CONFIGURATION mode.

```
no lldp holdtime-multiplier
```

Configure TTL

```
OS10(config)# lldp holdtime-multiplier 2
```

Return multiplier value

```
OS10(config)# no lldp holdtime-multiplier
```

LLDP commands

clear lldp counters

Clears LLDP and LLDP-MED transmit, receive, and discard statistics from all the physical interfaces.

Syntax	clear lldp counters
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	The counter default value resets to zero for all physical interfaces.

Example

```
OS10# clear lldp counters
```

Supported Releases 10.2.0E or later

clear lldp table

Clears LLDP neighbor information for all interfaces.

Syntax	clear lldp table
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	Neighbor information clears on all interfaces.

Example

```
OS10# clear lldp table
```

Supported Releases 10.2.0E or later

lldp enable

Enables or disables LLDP globally.

Syntax	lldp enable
Parameters	None
Default	Enabled
Command Mode	CONFIGURATION
Usage Information	This command enables LLDP globally for all Ethernet (PHY) interfaces, except on those interfaces where LLDP is manually disabled. The <code>no</code> version of this command disables LLDP globally irrespective of whether LLDP is manually enabled on an interface.

Example

```
OS10(config)# lldp enable
```

Supported Releases

10.3.1E or later

lldp holdtime-multiplier

Configures the multiplier value for the hold time (in seconds).

Syntax

```
lldp holdtime-multiplier integer
```

Parameters

integer — Enter the holdtime-multiplier value in seconds (2 to 10).

Default

4 seconds

Command Mode

CONFIGURATION

Usage Information

Hold time is the amount of time (in seconds) that a receiving system waits to hold the information before discarding it. Formula: Hold Time = (Updated Frequency Interval) X (Hold Time Multiplier). The `no` version of this command resets the value to the default.

Example

```
OS10(config)# lldp holdtime-multiplier 2
```

Supported Releases

10.2.0E or later

lldp med fast-start-repeat-count

Configures the number of packets sent during the activation of the fast start mechanism.

Syntax

```
lldp-med fast-start-repeat-count number
```

Parameters

number — Enter the number of packets sent during the activation of the fast start mechanism (1 to 10).

Default

3

Command Mode

CONFIGURATION

Usage Information

None

Example

```
OS10(config)# lldp med fast-start-repeat-count 5
```

Supported Releases

10.2.0E or later

lldp med

Enables or disables LLDP-MED on an interface.

Syntax

```
lldp med {enable | disable}
```

Parameters

- `enable` — Enable LLDP-MED on the interface.
- `disable` — Disable LLDP-MED on the interface.

Default

Enabled with network-policy TLV

Command Mode

INTERFACE

Usage Information

LLDP-MED communicates the types of TLVs that the endpoint device and the network connectivity device support. Use the `no lldp med` or `lldp med disable` command to disable LLDP-MED on a specific interface.

Example

```
OS10(conf-if-eth1/1/1)# lldp med disable
```

Supported Releases

10.2.0E or later

lldp med network-policy

Manually defines an LLDP-MED network policy.

Syntax

```
lldp-med network-policy number app {voice | voice-signaling | guest-voice | guestvoice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling} {vlan vlan-id vlan-type {tag | untag} priority priority dscp dscp value}
```

Parameters

- *number* — Enter a network policy index number (1 to 32).
- *app* — Enter the type of the applications available for the network policy:
 - *voice* — Voice network-policy application.
 - *voice-signaling* — Voice-signaling network-policy application.
 - *guest-voice* — Guest voice network-policy application.
 - *guestvoice-signaling* — Guest voice signaling network policy application.
 - *softphone-voice* — SoftPhone voice network policy application.
 - *streaming-video* — Streaming video network-policy application.
 - *video-conferencing* — Voice conference network-policy application.
 - *video-signaling* — Video signaling network-policy application.
- *vlan vlan-id* — Enter the VLAN number for the selected application (1 to 4093).
- *vlan-type* — Enter the type of VLAN the application is using.
- *tag* — Enter a tagged VLAN number.
- *untag* — Enter an untagged VLAN number.
- *priority priority* — Enter the user priority set for the application.
- *dscp dscp value* — Enter the DSCP value set for the application.

Default

Not configured

Command Mode

CONFIGURATION

Usage Information

You can create up to 32 network policies and attach the LLDP-MED network policies to a port.

Example

```
OS10(config)# lldp med network-policy 10 app voice vlan 10 vlan-type tag priority 2 dscp 1
```

Supported Releases

10.2.0E or later

lldp med network-policy (Interface)

Attaches or removes an LLDP-MED network policy to or from an interface.

Syntax

```
lldp-med network-policy {add | remove} number
```

Parameters

- *add* — Attach the network policy to an interface.
- *remove* — Remove the network policy from an interface.
- *number* — Enter a network policy index number (1 to 32).

Default

Not configured

Command Mode

INTERFACE

Usage Information

Attach only one network policy for per interface.

Example

```
OS10(conf-if-eth1/1/5)# lldp med network-policy add 1
```

Supported Release

10.2.0E or later

lldp med tlv-select

Configures the LLDP-MED TLV type to transmit or receive.

Syntax

```
lldp med tlv-select {network-policy | inventory}
```

Parameters

- `network-policy` — Enable or disable the port description TLV.
- `inventory` — Enable or disable the system TLV.

Default

Enabled

Command Mode

INTERFACE

Usage

None

Information**Example**

```
OS10(conf-if-eth1/1/3)# lldp med tlv-select network-policy
```

Supported Releases

10.2.0E or later

lldp receive

Enables or disables the LLDP packet reception on a specific interface.

Syntax

```
lldp receive
```

Parameters

None

Default

Not configured

Command Mode

INTERFACE

Usage**Information**

Enable LLDP globally on the system before using the `lldp receive` command. The `no` version of this command disables the reception of LLDP packets.

Example

```
OS10(conf-if-eth1/1/3)# lldp receive
```

Supported Releases

10.2.0E or later

lldp reinit

Configures the delay time (in seconds) for LLDP to initialize on any interface.

Syntax

```
lldp reinit seconds
```

Parameters

seconds — Enter the delay timer value in seconds (1 to 10).

Default

2 seconds

Command Mode

CONFIGURATION

Usage**Information**

The `no` version of this command resets the value to the default.

Example

```
OS10(config)# lldp reinit 5
```


Supported Releases 10.2.0E or later

lldp timer

Configures the rate (in seconds) at which LLDP packets send to the peers.

Syntax `lldp timer seconds`

Parameters `seconds` — Enter the LLDP timer rate in seconds (5 to 254).

Default 30 seconds

Command Mode CONFIGURATION

Usage Information The `no` version of this command sets the LLDP timer back to its default value.

Example

```
OS10(config)# lldp timer 25
```

Supported Releases 10.2.0E or later

lldp tlv-select basic-tlv

Enables or disables TLV attributes to transmit and receive LLDP packets.

Syntax `lldp tlv-select basic-tlv {port-description | system-name | system-description | system-capabilities | management-address}`

Parameters

- `port-description` — Enable or disable the port description TLV.
- `system-name` — Enable or disable the system TLV.
- `system-description` — Enable or disable the system description TLV.
- `system-capabilities` — Enable or disable the system capabilities TLV.
- `management-address` — Enable or disable the management address TLV.

Default Enabled

Command Mode INTERFACE

Usage Information None

Example

```
OS10(conf-if-eth1/1/3)# lldp tlv-select basic-tlv system-name
```

Supported Releases 10.2.0E or later

lldp tlv-select dot1tlv

Enables or disables the dot.1 TLVs to transmit in LLDP packets.

Syntax `lldp tlv-select dot1tlv { port-vlan-id | link-aggregation}`

Parameters

- `port-vlan-id` — Enter the port VLAN ID.
- `link-aggregation` — Enable the link aggregation TLV.

Default Enabled

Command Mode INTERFACE

Usage Information The `lldp tlv-select dot1tlv link-aggregation` command advertises link aggregation as a dot1 TLV in the LLDPDUs. The `no` version of this command disables TLV transmissions.

Example (Port)

```
OS10(conf-if-eth1/1/3)# lldp tlv-select dot1tlv port-vlan-id
```

Example (Link Aggregation)

```
OS10(conf-if-eth1/1/3)# lldp tlv-select dot1tlv link-aggregation
```

Supported Releases

10.2.0E or later

lldp tlv-select dot3tlv

Enables or disables the dot3 TLVs to transmit in LLDP packets.

Syntax

```
lldp tlv-select dot3tlv {macphy-config | max-framesize}
```

Parameters

- `macphy-config` — Enable the port VLAN ID TLV.
- `max-framesize` — Enable maximum frame size TLV.

Default

Enabled

Command Mode

INTERFACE

Usage Information

The `no` version of this command disables TLV transmission.

Example

```
OS10(conf-if-eth1/1/3)# lldp tlv-select dot3tlv macphy-config
```

Supported Releases

10.2.0E or later

lldp transmit

Enables the transmission of LLDP packets on a specific interface.

Syntax

```
lldp transmit
```

Parameters

None

Default

Not configured

Command Mode

INTERFACE

Usage Information

The `no` version of this command disables the transmission of LLDP packets on a specific interface.

Example

```
OS10(conf-if-eth1/1/9)# lldp transmit
```

Supported Releases

10.2.0E or later

show lldp interface

Displays the LLDP information advertised from a specific interface.

Syntax

```
show lldp interface ethernet node/slot/port[:subport] [med | local-device]
```

Parameters

- `ethernet node/slot/port[:subport]` — Enter the Ethernet interface information.
- `med` — Enter the interface to view the MED information.
- `local-device` — Enter the interface to view the local-device information.

Default

None

Command Mode

EXEC

Usage Information

Use the `med` parameter to view MED information for a specific interface, and use the `local-device` parameter to view inventory details.

Example

```
OS10# show lldp interface ethernet 1/1/5
ethernet1/1/5
Tx State           : Enabled
Rx State           : Enabled
Tx SEM State       : initialize
Rx SEM State       : wait-port-operational
Notification Status : Disabled
Notification Type   : mis-configuration
DestinationMacAddr : 01:80:c2:00:00:0e
```

Example (Local Device)

```
OS10# show lldp interface ethernet 1/1/1 local-device
Device ID: 00:0c:29:e5:aa:f4
Port ID: ethernet1/1/1
System Name: OS10
Capabilities: Bridge Router
System description: Dell networking Operating system
Port description: Connected to end point device
Time To Live: 120
LLDP MED Capabilities: Capabilities, Network Policy
LLDP MED Device Type: Network connectivity
```

Example (MED)

```
OS10# show lldp interface ethernet 1/1/20:1 med
Port | Capabilities | Network Policy | Location | Inventory | POE
-----|-----|-----|-----|-----|---
ethernet1/1/20:1 | Yes | Yes | No | No | No
Network Polices :
```

Supported Releases

10.2.0E or later

show lldp errors

Displays the LLDP errors related to memory allocation failures, queue overflows, and table overflows.

Syntax `show lldp errors`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show lldp errors
Total Memory Allocation Failures: 0
Total Input Queue Overflows: 0
Total Table Overflows: 0
```

Supported Release

10.2.0E or later

show lldp med

Displays the LLDP MED information for all the interfaces.

Syntax `show lldp med`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information Use the `show lldp interface` command to view MED information for a specific interface.

Example

```
OS10# show lldp med
Fast Start Repeat Count: 3
LLDP MED Device Type: Network Connectivity
Port | Capabilities | Network Policy | Location | Inventory | POE
-----|-----|-----|-----|-----|-----
ethernet1/1/1 | Yes | Yes | No | No | No
ethernet1/1/2 | Yes | Yes | No | No | No
ethernet1/1/3 | Yes | Yes | No | No | No
ethernet1/1/4 | Yes | Yes | No | Yes | No
ethernet1/1/5 | Yes | Yes | No | No | No
ethernet1/1/6 | Yes | Yes | No | No | No
ethernet1/1/7 | Yes | Yes | No | Yes | No
ethernet1/1/8 | Yes | Yes | No | No | No
ethernet1/1/9 | Yes | Yes | No | No | No
ethernet1/1/10 | Yes | Yes | No | No | No
ethernet1/1/11 | Yes | Yes | No | No | No
ethernet1/1/12 | Yes | Yes | No | No | No
ethernet1/1/13 | Yes | Yes | No | No | No
ethernet1/1/14 | Yes | Yes | No | No | No
ethernet1/1/15 | Yes | Yes | No | No | No
ethernet1/1/16 | Yes | Yes | No | No | No
ethernet1/1/17 | Yes | Yes | No | No | No
ethernet1/1/18 | Yes | Yes | No | No | No
ethernet1/1/19 | Yes | Yes | No | No | No
ethernet1/1/20 | Yes | Yes | No | No | No
ethernet1/1/21 | Yes | Yes | No | No | No
ethernet1/1/22 | Yes | Yes | No | No | No
ethernet1/1/23 | Yes | Yes | No | No | No
ethernet1/1/24 | Yes | Yes | No | No | No
ethernet1/1/25 | Yes | Yes | No | No | No
ethernet1/1/26 | Yes | Yes | No | No | No
ethernet1/1/27 | Yes | Yes | No | No | No
ethernet1/1/28 | Yes | Yes | No | No | No
ethernet1/1/29 | Yes | Yes | No | No | No
ethernet1/1/30 | Yes | Yes | No | No | No
ethernet1/1/31 | Yes | Yes | No | No | No
ethernet1/1/32 | Yes | Yes | No | No | No
```

Supported Releases 10.2.0E or later

show lldp neighbors

Displays the status of the LLDP neighbor system information.

Syntax `show lldp neighbors [detail | interface ethernet node/slot/port[:subport]]`

- Parameters**
- `detail` — View LLDP neighbor detailed information.
 - `interface ethernet node/slot/port[:subport]` — Enter the Ethernet interface information.

Command Mode EXEC

Usage Information This command status information includes local port ID, remote host name, remote port ID, and remote node ID.

Example

```
OS10# show lldp neighbors
Loc PortID      Rem Host Name      Rem Port Id      Rem Chassis Id
-----|-----|-----|-----|-----
ethernet1/1/2   Not Advertised     fortyGigE 0/56   00:01:e8:8a:fd:35
ethernet1/1/20:1 Not Advertised     GigabitEthernet 1/0 00:01:e8:05:db:05
```

Example (Detail)

```

OS10# show lldp neighbors interface ethernet 1/1/1 detail

Remote Chassis ID Subtype: Mac address (4)
Remote Chassis ID: 00:13:21:57:ca:40
Remote Port Subtype: Interface name (5)
Remote Port ID: ethernet1/1/10
Remote Port Description: Ethernet port 1
Local Port ID: ethernet1/1/1
Locally assigned remote Neighbor Index: 3
Remote TTL: 120
Information valid for next 105 seconds
Time since last information change of this neighbor: 00:00:15
Remote System Name: LLDP-pkt-gen
Remote Management Address (IPv4): 10.1.1.1
Remote System Desc: LLDP packet generator using scapy
Existing System Capabilities: Repeater, Bridge, Router
Enabled System Capabilities: Repeater, Bridge, Router
Remote Max Frame Size: 0
Remote Aggregation Status: false
MAC PHY Configuration:
  Auto-neg supported: 1
  Auto-neg enabled: 1
  Auto-neg advertised capabilities:
    10BASE-T half duplex mode,
    10BASE-T full duplex mode,
    100BASE-TX half duplex mode,
    100BASE-TX full duplex mode
MED Capabilities:
  Supported:
    LLDP-MED Capabilities,
    Network Policy,
    Location Identification,
    Extended Power via MDI - PSE,
    Extended Power via MDI - PD,
    Inventory Management
  Current:
    LLDP-MED Capabilities,
    Network Policy,
    Location Identification,
    Extended Power via MDI - PD,
    Inventory Management
  Device Class: Endpoint Class 3
Network Policy:
  Application: voice, Tag: Tagged, Vlan: 50, L2 Priority: 6, DSCP
  Value: 46
Inventory Management:
  H/W Revision : 12.1.1
  F/W Revision : 10.1.9750B
  S/W Revision : 10.1.9750B
  Serial Number : B11G152
  Manufacturer : Dell
  Model : S6010-ON
  Asset ID : E1001
Power-via-MDI:
  Power Type: PD Device
  Power Source: Local and PSE
  Power Priority: Low
  Power required: 6.5
Location Identification:
  Civic-based:

2C:02:49:4E:01:02:54:4E:03:07:43:68:65:6E:6E:61:69:04:06:47:75:69:
6E:64:79:05:0B:53:49:44:43:4F:49:6E:64:45:73:74:17:05:4F:54:50:2D:
31
ECS-ELIN:
39:39:36:32:30:33:35:38:32:34

```

Example (Interface)

```

OS10# show lldp neighbors interface ethernet 1/1/1
Loc PortID          Rem Host Name      Rem Port Id      Rem Chassis Id

```

```
-----  
ethernet1/1/1          OS10          ethernet1/1/2  4:17:eb:f7:06:c4
```

Supported Releases 10.2.0E or later

show lldp timers

Displays the LLDP hold time, delay time, and update frequency interval configuration information.

Syntax `show lldp timers`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show lldp timers  
LLDP Timers:  
Holdtime in seconds: 120  
Reinit-time in seconds: 6  
Transmit interval in seconds: 30
```

Supported Releases 10.2.0E or later

show lldp tlv-select interface

Displays the TLVs enabled for an interface.

Syntax `show lldp tlv-select interface ethernet node/slot/port[:subport]`

Parameters `ethernet node/slot/port[:subport]` — Enter the Ethernet interface information (1 to 253).

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show lldp tlv-select interface ethernet 1/1/4  
port-description  
system-name  
system-description  
system-capabilities  
management-address  
port-vlan  
mac-phy-config  
link-aggregation  
max-frame-size
```

Supported Releases 10.2.0E or later

show lldp traffic

Displays LLDP traffic information including counters, packets transmitted and received, discarded packets, and unrecognized TLVs.

Syntax	<code>show lldp traffic [interface ethernet <i>node/slot/port[:subport]</i>]</code>
Parameters	<code>interface ethernet <i>node/slot/port[:subport]</i></code> — (Optional) Enter the Ethernet interface information to view the LLDP traffic.
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show lldp traffic
LLDP Traffic Statistics:
Total Frames Out           : 1504
Total Entries Aged         : 2
Total Frames In            : 67
Total Frames Received In Error : 0
Total Frames Discarded     : 0
Total TLVS Unrecognized    : 0
Total TLVS Discarded      : 0
```

Example (Interface)

```
OS10# show lldp traffic interface ethernet 1/1/2
LLDP Traffic Statistics:
Total Frames Out           : 45
Total Entries Aged         : 1
Total Frames In            : 33
Total Frames Received In Error : 0
Total Frames Discarded     : 0
Total TLVS Unrecognized    : 0
Total TLVS Discarded      : 0

LLDP MED Traffic Statistics:
Total Med Frames Out       : 2
Total Med Frames In        : 1
Total Med Frames Discarded : 0
Total Med TLVS Discarded   : 0
Total Med Capability TLVS Discarded: 0
Total Med Policy TLVS Discarded : 0
Total Med Inventory TLVS Discarded : 0
```

Supported Releases	10.2.0E or later
---------------------------	------------------

show network-policy profile

Displays the network policy profiles.

Syntax	<code>show network-policy profile [<i>profile number</i>]</code>
Parameters	<code><i>profile number</i></code> — (Optional) Enter the network policy profile number (1 to 32).
Default	Not configured
Command Mode	EXEC
Usage Information	If you do not enter the network profile ID, all configured network policy profiles display.

Example

```
OS10# show network-policy profile 10
Network Policy Profile 10
voice vlan 17 cos 4
```

```
Interface:
  none
Network Policy Profile 30
  voice vlan 30 cos 5
Interface:
  none
Network Policy Profile 36
  voice vlan 4 cos 3
Interface:
  ethernet 1/1/1, ethernet 1/1/3-5
```

Supported Releases 10.2.0E or later

Media Access Control

All Ethernet switching ports maintain media access control (MAC) address tables. Each physical device in your network contains a MAC address. OS10 devices automatically enter learned MAC addresses as dynamic entries in the MAC address table.

Learned MAC address entries are subject to aging. Set the aging timer to zero (0) to disable MAC aging. For any dynamic entry, if no packet arrives on the device with the MAC address as the source or destination address within the timer period, the address is removed from the table.

- Enter an aging time (in seconds) in CONFIGURATION mode (0 to 1000000, default 1800).

```
mac address-table aging-time seconds
```

Configure Aging Time

```
OS10(config)# mac address-table aging-time 900
```

Disable Aging Time

```
OS10(config)# mac address-table aging-time 0
```

Static MAC Address

A static MAC address entry is one that you manually configure. A static entry is not subject to aging.

- Create a static MAC address entry in the MAC address table in CONFIGURATION mode.

```
mac-address-table static nn:nn:nn:nn:nn vlan vlan-id interface [ethernet node/slot/port[:subport] | port-channel channel-number]
```

Set Static MAC Address

```
OS10(config)# mac address-table static 34:17:eb:f2:ab:c6 vlan 10 interface ethernet 1/1/5
```

MAC Address Table

OS10 maintains a list of MAC address table entries.

- View the contents of the MAC address table in EXEC mode.

```
show mac address-table {dynamic | static} [address mac-address | vlan vlan-id | interface {ethernet node/slot/port[:subport] | port-channel number}] [count [vlan vlan-id] [interface {type node/slot/port[:subport] | port-channel number}]
```

- `dynamic` — (Optional) Displays dynamic MAC address table entry information.
- `static` — (Optional) Displays static MAC address table entry information.

- o `address mac-address` — (Optional) Displays MAC address information.
- o `interface ethernet node/slot/port[:subport]` — (Optional) Displays a list of dynamic and static MAC address entries.
- o `interface port-channel number` — (Optional) Displays port channel information (1 to 128).
- o `count` — (Optional) Displays the number of dynamic and static MAC address entries.
- o `vlan vlan-id` — (Optional) Displays information for a specified VLAN only (1 to 4093).

View MAC Address Table Entries

```
OS10# show mac address-table
VlanId  Mac Address          Type          Interface
1       00:00:15:c6:ca:49      dynamic      ethernet1/1/21
1       00:00:20:2a:25:55      dynamic      ethernet1/1/21
1       90:b1:1c:f4:aa:ce      dynamic      ethernet1/1/21
1       90:b1:1c:f4:aa:c6      dynamic      ethernet1/1/21
10      34:17:eb:02:8c:33      static       ethernet1/1/1
```

View MAC Address Table Count

```
OS10# show mac address-table count
MAC Entries for all vlans :
Dynamic Address Count :      4
Static Address (User-defined) Count : 1
Total MAC Addresses in Use:    5
```

Clear MAC Address Table

You can clear dynamic address entries that are maintained in the MAC address table.

- Clear the MAC address table of dynamic entries in EXEC mode.

```
clear mac address-table dynamic [[all] [address mac_addr] [vlan vlan-id] [interface
{ethernet type node/slot/port[:subport] | port-channel number}]
```

- o `all` — (Optional) Clear all dynamic entries.
- o `address mac_addr` — (Optional) Clear a MAC address entry.
- o `vlan vlan-id` — (Optional) Clear a MAC address table entry from a VLAN number (1 to 4093).
- o `ethernet node/slot/port[:subport]` — (Optional) Clear an Ethernet interface entry.
- o `port-channel number` — (Optional) Clear a port-channel number (1 to 128).

Clear MAC Address Table

```
OS10# clear mac address-table dynamic vlan 20 interface ethernet 1/2/20
```

MAC Commands

clear mac address-table dynamic

Clears L2 dynamic address entries from the MAC address table.

Syntax `clear mac address-table dynamic {all | address mac_addr | vlan vlan-id | interface {ethernet node/slot/port[:subport] | port-channel number}}`

- Parameters**
- `all` — (Optional) Delete all MAC address table entries.
 - `address mac_addr` — (Optional) Delete a configured MAC address from the address table (nn:nn:nn:nn:nn:nn format).
 - `vlan vlan-id` — (Optional) Delete all entries based on the VLAN number from the address table (1 to 4093).
 - `interface` — (Optional) Clear the interface type:

- `ethernet node/slot/port[:subport]` — Delete the Ethernet interface configuration from the address table.
- `port-channel channel-number` — Delete the port-channel interface configuration from the address table (1 to 128).

Default Not configured

Command Mode EXEC

Usage Information Use the `all` parameter to remove all dynamic entries from the address table.

Example

```
OS10# clear mac address-table dynamic all
```

Example (VLAN)

```
OS10# clear mac address-table dynamic vlan 20
```

Supported Releases 10.2.0E or later

mac address-table aging-time

Configures the aging time for entries in the L2 address table.

Syntax `mac address-table aging-time seconds`

Parameters `seconds` — Enter the aging time for MAC table entries in seconds (0 to 1000000).

Default 1800 seconds

Command Mode CONFIGURATION

Usage Information Set the aging timer to zero (0) to disable MAC address aging for all dynamic entries. The aging time counts from the last time that the device detected the MAC address.

Example

```
OS10(config)# mac address-table aging-time 3600
```

Supported Releases 10.2.0E or later

mac address-table static

Configures a static entry for the L2 MAC address table.

Syntax `mac address-table static mac-address vlan vlan-id interface {ethernet node/slot/port[:subport] | port-channel number}`

- Parameters**
- `mac-address` — Enter the MAC address to add to the table in `nn:nn:nn:nn:nn:nn` format.
 - `vlan vlan-id` — Enter the VLAN to apply the static MAC address to (1 to 4093).
 - `interface` — Enter the interface type:
 - `ethernet node/slot/port[:subport]` — Enter the Ethernet information.
 - `port-channel channel-number` — Enter a port-channel interface number (1 to 128).

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command resets the value to the default.

Example (VLAN)

```
OS10(config)# mac address-table static 34:17:eb:f2:ab:c6 vlan 1
interface ethernet 1/1/30
```

Example (Port-Channel)

```
OS10(config)# mac address-table static 34:17:eb:02:8c:33 vlan 10
interface port-channel 1
```

Supported Releases

10.2.0E or later

show mac address-table

Displays information about the MAC address table.

Syntax

```
show mac address-table [address mac-address | aging-time | [count [vlan vlan-id] | dynamic | interface {ethernet node/slot/port[:subport] | port-channel number}]| static [address mac-address] | vlan vlan-id
```

Parameters

- *address mac-address* — (Optional) Displays MAC address table information.
- *aging-time* — (Optional) Displays MAC address table aging-time information.
- *count* — (Optional) Displays the number of dynamic and static MAC address entries.
- *dynamic* — (Optional) Displays dynamic MAC address table entries only.
- *interface* — Set the interface type:
 - *ethernet node/slot/port[:subport]* — Displays MAC address table information for a physical interface.
 - *port-channel channel-number* — Displays MAC address table information for a port-channel interface (1 to 128).
- *static* — (Optional) Displays static MAC address table entries only.
- *vlan vlan-id* — (Optional) Displays VLAN information only (1 to 4093).

Default

Not configured

Command Mode

EXEC

Usage Information

The network device maintains static MAC address entries saved in the startup configuration file, and reboots and flushes dynamic entries.

Example (Address)

```
OS10# show mac address-table address 90:b1:1c:f4:a6:8f
VlanId  Mac Address          Type          Interface
1       90:b1:1c:f4:a6:8f      dynamic      ethernet1/1/3
```

Example (Aging Time)

```
OS10# show mac address-table aging-time
Global Mac-address-table aging time : 1800
```

Example (Count)

```
OS10# show mac address-table count
MAC Entries for all vlans :
Dynamic Address Count : 5
Static Address (User-defined) Count : 0
Total MAC Addresses in Use: 5
```

Example (Dynamic)

```
OS10# show mac address-table dynamic
VlanId  Mac Address          Type          Interface
1       90:b1:1c:f4:a6:8f      dynamic      ethernet1/1/3
```

Example (Ethernet)

```
OS10# show mac address-table interface ethernet 1/1/3
VlanId  Mac Address          Type          Interface
1       66:38:3a:62:31:3a      dynamic      ethernet1/1/3
```

Supported Releases

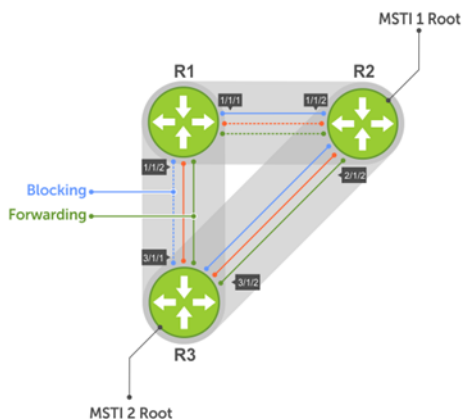
10.2.0E or later

Multiple Spanning-Tree Protocol

Multiple Spanning-Tree Protocol (MSTP) is an RSTP-based spanning-tree variation that improves on per-VLAN RPVST+. You can configure Multiple Spanning-Tree Instances (MSTIs) and map multiple VLANs to one spanning-tree instance to reduce the total number of required instances. RPVST+ allows a spanning-tree instance for each VLAN. This 1:1 approach is not suitable if you have multiple VLANs — each spanning-tree instance costs bandwidth and processing resources.

When you enable MST, all ports in Layer 2 mode participate in MST. Keep in mind that OS10 only supports one MST region.

Load balancing can be achieved using the MSTP. When three VLANs are mapped to two MSTIs, VLAN 100 traffic takes a different path than VLAN 200 and 300 traffic.



Configuring MST is a four-step process:

1. Enable MST, if the current running STP version is not MST.
2. (Optional) Map the VLANs to different instances to achieve load balancing.
3. Ensure the same region name is configured in all the bridges running MST.
4. (Optional) Configure the revision number.

Configure MSTP

When you enable MST globally, all L2 physical, port-channel, and VLAN interfaces are automatically assigned to MSTI zero (0). Within an MSTI, only one path from any one bridge to another is enabled for forwarding.

- Enable MST in CONFIGURATION mode.

```
spanning-tree mode mst
```

Configure and verify MSTP

```
OS10(config)# spanning-tree mode mst
OS10(config)# do show spanning-tree
show spanning-tree mst configuration
Region Name: ravi
Revision: 0
MSTI    VID
0       1,7-4093
1       2
2       3
3       4
4       5
5       6
```

Add or remove interfaces

By default, all interfaces are enabled in L2 switchport mode, and all L2 interfaces are part of spanning-tree.

- Disable spanning-tree on an interface in INTERFACE mode.

```
spanning-tree disable
```

- Enable MST on an interface in INTERFACE mode.

```
no spanning-tree disable
```

Create instances

You can create multiple MSTP instances and map VLANs. A single MSTI provides no more benefit than RSTP. To take full advantage of the MSTP, create multiple MSTIs and map VLANs to them.

1. Enter an instance number in CONFIGURATION mode.

```
spanning tree mst configuration
```

2. Enter the MST instance number in MULTIPLE-SPANNING-TREE mode (0 to 63).

```
instance instance-number
```

3. Enter the VLAN and IDs to participate in the MST instance in MULTIPLE-SPANNING-TREE mode (1 to 4096).

```
instance vlan-id
```

Create MST instances

```
OS10(config)# spanning-tree mst configuration
OS10(conf-mst)# name force10
OS10(conf-mst)# revision 100
OS10(conf-mst)# instance 1 vlan 2-10
OS10(conf-mst)# instance 2 vlan 11-20
OS10(conf-mst)# instance 3 vlan 21-30
```

View VLAN instance mapping

```
OS10# show spanning-tree mst configuration
Region Name: force10
Revision: 100
MSTI    VID
0       1,31-4093
1       2-10
2       11-20
3       21-30
```

View port forwarding/discarding state

```
OS10# show spanning-tree msti 0 brief
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1,31-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID    Priority 32768, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 90b1.1cf4.a523
CIST external path cost 500
Interface
Name          PortID Prio Cost    Sts    Cost Bridge ID    PortID
-----
ethernet1/1/1 128.260 128 2000000000 BLK    0    32768 90b1.1cf4.a523 128.260
ethernet1/1/2 128.264 128 2000000000 BLK    0    32768 90b1.1cf4.a523 128.264
ethernet1/1/3 128.268 128 2000000000 BLK    0    32768 90b1.1cf4.a523 128.268
ethernet1/1/4 128.272 128 2000000000 BLK    0    32768 90b1.1cf4.a523 128.272
ethernet1/1/5 128.276 128 500          FWD    0    32768 3417.4455.667f 128.146
ethernet1/1/6 128.280 128 500          BLK    0    32768 3417.4455.667f 128.150
ethernet1/1/7 128.284 128 2000000000 BLK    0    32768 90b1.1cf4.a523 128.284
ethernet1/1/8 128.288 128 2000000000 BLK    0    32768 90b1.1cf4.a523 128.288
```

ethernet1/1/9	128.292	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.292
ethernet1/1/10	128.296	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.296
ethernet1/1/11	128.300	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.300
ethernet1/1/12	128.304	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.304
ethernet1/1/13	128.308	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.308
ethernet1/1/14	128.312	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.312
ethernet1/1/15	128.316	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.316
ethernet1/1/16	128.320	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.320
ethernet1/1/17	128.324	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.324
ethernet1/1/18	128.328	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.328
ethernet1/1/19	128.332	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.332
ethernet1/1/20	128.336	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.336
ethernet1/1/21	128.340	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.340
ethernet1/1/22	128.344	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.344
ethernet1/1/23	128.348	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.348
ethernet1/1/24	128.352	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.352
ethernet1/1/25	128.356	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.356
ethernet1/1/26	128.360	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.360
ethernet1/1/27	128.364	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.364
ethernet1/1/28	128.368	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.368
ethernet1/1/29	128.372	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.372
ethernet1/1/30	128.376	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.376
ethernet1/1/31	128.380	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.380
ethernet1/1/32	128.384	128	200000000	BLK	0	32768	90b1.1cf4.a523	128.384

Interface								
Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
ethernet1/1/1	Disb	128.260	128	200000000	BLK	0	AUTO	No
ethernet1/1/2	Disb	128.264	128	200000000	BLK	0	AUTO	No
ethernet1/1/3	Disb	128.268	128	200000000	BLK	0	AUTO	No
ethernet1/1/4	Disb	128.272	128	200000000	BLK	0	AUTO	No
ethernet1/1/5	Root	128.276	128	500	FWD	0	AUTO	No
ethernet1/1/6	Altr	128.280	128	500	BLK	0	AUTO	No
ethernet1/1/7	Disb	128.284	128	200000000	BLK	0	AUTO	No
ethernet1/1/8	Disb	128.288	128	200000000	BLK	0	AUTO	No
ethernet1/1/9	Disb	128.292	128	200000000	BLK	0	AUTO	No
ethernet1/1/10	Disb	128.296	128	200000000	BLK	0	AUTO	No

Root selection

MSTP determines the root bridge according to the lowest bridge ID. Assign a lower bridge priority to increase its likelihood of becoming the root bridge.

- Assign a bridge priority number to a specific instance in CONFIGURATION mode (0 to 61440 in increments of 4096, default 32768). Use a lower priority number to increase the likelihood of the bridge to become a root bridge.

```
spanning-tree mst instance-number priority priority
```

Assign root bridge priority

```
OS10(config)# spanning-tree mst 0
```

Verify root bridge priority

```
OS10# show spanning-tree active
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1,31-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 90b1.1cf4.a523
CIST external path cost 500
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID
-----
ethernet1/1/5 128.276 128 500 FWD 0 32768 3417.4455.667f 128.146
ethernet1/1/6 128.280 128 500 BLK 0 32768 3417.4455.667f 128.150
```

Interface Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
ethernet1/1/5	Root	128.276	128	500	FWD	0	AUTO	No
ethernet1/1/6	Altr	128.280	128	500	BLK	0	AUTO	No

Non-Dell hardware

OS10 supports only one MST region. For a bridge to be in the same MST region as another, the three unique attributes (name, revision, and VLAN-to-instance-mapping) must match. The default values for name and revision number match on all Dell hardware. If you have non-Dell hardware that participates in MST, ensure these values match on all devices.

A region is a combination of three unique attributes:

- Name — A mnemonic string you assign to the region (default is the system MAC address).
- Revision — A 2-byte number (default is 0).
- VLAN-to-instance mapping — Placement of a VLAN in an MSTI.

Region name or revision

You can change the MSTP region name or revision.

- Change the region name in MULTIPLE-SPANNING-TREE mode (up to 32 characters).

```
name name
```

- Change the region revision number in MULTIPLE-SPANNING-TREE mode (0 to 65535, default 0).

```
revision number
```

Configure and verify region name

```
OS10(conf-mstp)# name my-mstp-region
OS10(conf-mstp)# do show spanning-tree mst config
MST region name: my-mstp-region
Revision: 0
MSTI    VID
 1      100
 2      200-300
```

Modify parameters

The root bridge sets the values for forward-delay, hello-time, max-age, and max-hops and overwrites the values set on other MST bridges.

- Forward-time** Time an interface waits in the Discarding state and Learning state before it transitions to the Forwarding state.
- Hello-time** Interval in which the bridge sends MST BPDUs.
- Max-age** Length of time the bridge maintains configuration information before it refreshes that information by recomputing the MST topology.
- Max-hops** Maximum number of hops a BPDU travels before a receiving device discards it.

Dell EMC recommends that only experienced network administrators change MST parameters. Poorly planned modification of the MST parameters can negatively affect network performance.

1. Change the forward-time parameter in CONFIGURATION mode (4 to 30, default 15).

```
spanning-tree mst forward-time seconds
```

2. Change the hello-time parameter in CONFIGURATION mode (1 to 10, default 2). Dell EMC recommends increasing the hello-time for large configurations (especially configurations with more ports).

```
spanning-tree mst hello-time seconds
```

3. Change the max-age parameter in CONFIGURATION mode (6 to 40, default 20).

```
spanning-tree mst max-age seconds
```

4. Change the max-hops parameter in CONFIGURATION mode (1 to 40, default 20).

```
spanning-tree mst max-hops number
```

MST configuration

```
OS10(config)# spanning-tree mst
OS10(config)# spanning-tree mst forward-time 16
OS10(config)# spanning-tree mst hello-time 5
OS10(config)# spanning-tree mst max-age 10
OS10(config)# spanning-tree mst max-hops 30
```

View MSTP parameter values

```
OS10# show spanning-tree active
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1,31-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID    Priority 32768, Address 90b1.1cf4.a523
Configured hello time 10, max age 40, forward delay 30, max hops 40
CIST regional root ID Priority 32768, Address 90b1.1cf4.a523
CIST external path cost 500
```

Interface Name	PortID	Prio	Cost	Sts	Cost	Bridge ID	Designated PortID
ethernet1/1/5	128.276	128	500	FWD	0	32768	3417.4455.667f 128.146
ethernet1/1/6	128.280	128	500	BLK	0	32768	3417.4455.667f 128.150

Interface Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
ethernet1/1/5	Root	128.276	128	500	FWD	0	AUTO	No
ethernet1/1/6	Altr	128.280	128	500	BLK	0	AUTO	No

Interface parameters

Adjust two interface parameters to increase or decrease the likelihood that a port becomes a forwarding port.

- Port cost** Value that is based on the interface type. The greater the port cost, the less likely the port is selected to be a forwarding port.
- Port priority** Influences the likelihood that a port is selected to be a forwarding port if several ports have the same port cost.

Default values for port cost by interface:

- 100-Mb/s Ethernet interfaces — 200000
 - 1-Gigabit Ethernet interfaces — 20000
 - 10-Gigabit Ethernet interfaces — 2000
 - Port-channel with 100 Mb/s Ethernet interfaces — 180000
 - Port-channel with 1-Gigabit Ethernet interfaces — 18000
 - Port-channel with 10-Gigabit Ethernet interfaces — 1800
1. Change the port cost of an interface in INTERFACE mode (0 to 200000000).

```
spanning-tree msti number cost cost
```


2. Change the port priority of an interface in INTERFACE mode (0 to 240 in increments of 16, default 128).

```
spanning-tree msti number priority priority
```

View MSTi interface configuration

```
OS10(conf-if-eth1/1/7)# do show spanning-tree msti 0 interface ethernet 1/1/7
ethernet1/1/7 of MSTI 0 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: Yes, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-
violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 69, Received: 0
Interface
Name          PortID  Prio  Cost  Sts  Cost  Bridge ID          PortID
-----
ethernet1/1/7 0.284  0    1    FWD  0    32768  90b1.1cf4.9b8a 0.284
```

Forward traffic

EdgePort allows the interface to forward traffic approximately 30 seconds sooner as it skips the Blocking and Learning states. The `spanning-tree bpduguard enable` command causes the interface hardware to shut down when it receives a BPDU.

⚠ CAUTION: Configure EdgePort only on links connecting to an end station. EdgePort can cause loops if you enable it on an interface connected to a network.

When you implement BPDU guard, although the interface is placed in Error Disabled state when receiving the BPDU, the physical interface remains in the Up state. The hardware discards regular network traffic after a BPDU violation. BPDUs are forwarded to the CPU, where they are discarded as well.

- Enable EdgePort on an interface in INTERFACE mode.

```
spanning-tree port type edge
```

Configure EdgePort

```
OS10(conf-if-eth1/1/4)# spanning-tree port type edge
```

View interface status

```
OS10# show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of MSTI 0 is designated Forwarding
Edge port:yes port guard :none (default)
Link type is point-to-point (auto)
Boundary: YES bpdu filter :disable bpdu guard :disable bpduguard shutdown-on-
violation :disable RootGuard: disable LoopGuard disable
Bpdus (MRecords) sent 610, received 5
Interface
Name          PortID  Prio  Cost  Sts  Cost  Bridge ID          PortID
-----
ethernet1/1/4 128.272 128  500  FWD  0    32768  90b1.1cf4.a911 128.272
=====
```

Spanning-tree extensions

STP extensions provide a means to ensure efficient network convergence by securely enforcing the active network topology. OS10 supports BPDU filtering, BPDU guard, root guard, and loop guard STP extensions.

- BPDU filtering** Protects the network from unexpected flooding of BPDUs from an erroneous device. Enabling BPDU Filtering instructs the hardware to drop BPDUs and prevents flooding from reaching the CPU. BPDU filtering is enabled by default on Edge ports. All BPDUs received on the Edge port are dropped. If you explicitly configure BPDU filtering on a port, that port drops all BPDUs that it receives.

BPDU guard	Blocks the L2 bridged ports and LAG ports connected to end hosts and servers from receiving any BPDUs. When you enable BPDU guard, it places a port (bridge or LAG) in the Error_Disable or Blocking state if the port receives any BPDU frames. In a LAG, all member ports (including new members) are placed in the Blocking state. The network traffic drops but the port continues to forward BPDUs to the CPU that are later dropped. To prevent further reception of BPDUs, configure a port to shut down using the <code>shutdown</code> command. The port can only resume operation from Shutdown state after manual intervention.
Root guard	Avoids bridging loops and preserves the root bridge position during network transitions. STP selects the root bridge with the lowest priority value. During network transitions, another bridge with a lower priority may attempt to become the root bridge and cause unpredictable network behavior. Configure the <code>spanning-tree guard root</code> command to avoid such an attempt and preserve the position of the root bridge. Root guard is enabled on ports that are designated ports. The root guard configuration applies to all VLANs configured on the port.
Loop guard	Prevents L2 forwarding loops caused by a hardware failure (cable failure or an interface fault). When a hardware failure occurs, a participating spanning tree link becomes unidirectional and a port stops receiving BPDUs. When a blocked port stops receiving BPDUs, it transitions to a Forwarding state causing spanning tree loops in the network. Enable loop guard on a port that transitions to the Loop-Inconsistent state until it receives BPDUs using the <code>spanning-tree guard loop</code> command. After BPDUs are received, the port moves out of the Loop-Inconsistent (or blocking) state and transitions to an appropriate state determined by STP. Enabling loop guard on a per-port basis enables it on all VLANs configured on the port. If you disable loop guard on a port, it moves to the Listening state.

If you enable BPDU Filter and BPDU Guard on the same port, the BPDU Filter configuration takes precedence. Root Guard and Loop Guard are mutually exclusive. Configuring one overwrites the other from the active configuration.

1. Enable spanning-tree BPDU filter in INTERFACE mode.

```
spanning-tree bpdudfilter enable
```

- To shut down the port channel interface, all member ports are disabled in the hardware.
- To add a physical port to a port-channel already in the Error Disable state, the new member port is also disabled in the hardware.
- To remove a physical port from a port-channel in Error Disable state, the Error Disabled state clears on this physical port (the physical port is enabled in the hardware).

To clear Error Disabled state:

- Use the `shutdown` command on the interface.
- Use the `spanning-tree bpdudfilter disable` command to disable the BPDU guard on the interface.
- Use the `spanning-tree disable` command to disable STP on the interface.

2. Enable STP BPDU guard in INTERFACE mode.

```
spanning-tree bpduguard enable
```

- To shut down the port channel interface, all member ports are disabled in the hardware.
- To add a physical port to a port-channel already in the Error Disable state, the new member port is also disabled in the hardware.
- To remove a physical port from a port-channel in Error Disable state, the Error Disabled state clears on this physical port (the physical port is enabled in the hardware).

To clear Error Disabled state:

- Use the `shutdown` command on the interface.
- Use the `spanning-tree bpduguard disable` command to disable the BPDU guard on the interface.
- Use the `spanning-tree disable` command to disable STP on the interface.

3. Set the guard types to avoid loops in INTERFACE mode.

```
spanning-tree guard {loop | root | none}
```

- `loop` — Set the guard type to loop.
- `none` — Set the guard type to none.
- `root` — Set the guard type to root.

BPDU filter

```
OS10(conf-if-eth1/1/4)# spanning-tree bpdudfilter enable
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is designated Blocking
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdu filter : Enable bpdu guard : bpduguard shutdown-on-
violation :disable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 134, received 138
Interface
Name          PortID   Prio Cost Sts   Cost  Bridge ID          Designated
-----
ethernet1/1/4 128.272 128  500 BLK  500   32769   90b1.1cf4.a911 128.272
```

BPDU guard

```
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# spanning-tree bpduguard enable
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is designated Blocking
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdu filter : Enable bpdu guard : bpduguard shutdown-on-
violation :enable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 134, received 138
Interface
Name          PortID   Prio Cost Sts   Cost  Bridge ID          Designated
-----
ethernet1/1/4 128.272 128  500 BLK  500   32769   90b1.1cf4.a911 128.272
```

Loop guard

```
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# spanning-tree guard loop
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdu filter : bpdu guard : bpduguard shutdown-on-
violation :disable RootGuard: disable LoopGuard enable
Bpdus (MRecords) sent 7, received 20
Interface
Name          PortID   Prio Cost Sts   Cost  Bridge ID          Designated
-----
ethernet1/1/4 128.272 128  500 FWD  0     32769   90b1.1cf4.9d3b 128.272
```

Root guard

```
OS10(conf-if-eth1/1/4)# spanning-tree guard root
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdu filter : bpdu guard : bpduguard shutdown-on-
violation :disable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 7, received 33
Interface
Name          PortID   Prio Cost Sts   Cost  Bridge ID          Designated
-----
ethernet1/1/4 128.272 128  500 BLK  500   32769   90b1.1cf4.a911 128.272
```

MST commands

instance

Configures MST instances and one or multiple VLANs mapped to the MST instance.

Syntax	<code>instance instance-number {vlan vlan-range}</code>
Parameters	<ul style="list-style-type: none">• <code>instance</code> — Enter an MST instance value (0 to 63).• <code>vlan range</code> — Enter a VLAN range value (1 to 4093).
Default	Not configured
Command Mode	MULTIPLE-SPANNING-TREE
Usage Information	By default, all VLANs map to MST instance zero (0) unless you are using the <code>vlan range</code> command to map the VLANs to a non-zero instance. The <code>no</code> version of this command removes all the instance related configuration.

Example

```
OS10(conf-mst)# instance 1 vlan 2-10
OS10(conf-mst)# instance 2 vlan 11-20
OS10(conf-mst)# instance 3 vlan 21-30
```

Supported Releases 10.2.0E or later

name

Assigns a name to the MST region.

Syntax	<code>name region-name</code>
Parameters	<code>region-name</code> — Enter a name for an MST region (up to 32 characters).
Default	System MAC address
Command Mode	MULTIPLE-SPANNING-TREE
Usage Information	By default, MSTP assigns system MAC as the region name. Two MST devices within the same region must share the same region name, including matching case.

Example

```
OS10(conf-mst)# name my-mst-region
```

Supported Releases 10.2.0E or later

revision

Configures a revision number for the MSTP configuration.

Syntax	<code>revision number</code>
Parameters	<code>number</code> — Enter a revision number for the MSTP configuration (0 to 65535).
Default	0
Command Mode	MULTIPLE-SPANNING-TREE
Usage Information	To have a bridge in the same MST region as another, the default values for the revision number must match on all Dell hardware devices. If there are non-Dell devices, ensure the revision number value matches on all the devices (see Non-Dell Hardware).

Example

```
OS10(conf-mst)# revision 10
```

Supported Releases 10.2.0E or later

spanning-tree bpdufilter

Enables or disables BPDU filtering on an interface.

Syntax `spanning-tree bpdufilter {enable | disable}`

Parameters

- `enable` — Enables the BPDU filtering on an interface.
- `disable` — Disables the BPDU filtering on an interface.

Default Disabled

Command Mode INTERFACE

Usage Information Use the `enable` parameter to enable BPDU filtering.

Example

```
OS10(conf-if-eth1/1/4)# spanning-tree bpdufilter enable
```

Supported Releases 10.2.0E or later

spanning-tree bpduguard

Enables or disables BPDU guard on an interface.

Syntax `spanning-tree bpduguard {enable | disable}`

Parameters

- `enable` — Enables the BPDU guard filter on an interface.
- `disable` — Disables the BPDU guard filter on an interface.

Default Disabled

Command Mode INTERFACE

Usage Information BPDU guard prevents a port from receiving BPDUs. If the port receives a BPDU, it is placed in the Error-Disabled state as a protective measure.

Example

```
OS10(conf-if-eth1/1/4)# spanning-tree bpduguard enable
```

Supported Releases 10.2.0E or later

spanning-tree disable

Disables the spanning-tree mode configured with the `spanning-tree mode` command globally on the switch or on specified interfaces.

Syntax `spanning-tree disable`

Parameters None

Default Not configured.

Usage Information The `no` version of this command re-enables STP and applies the currently configured spanning-tree settings.

Command Mode CONFIGURATION
INTERFACE

Example

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# spanning-tree disable
```

Supported Releases 10.3.0E or later

spanning-tree guard

Enables or disables loop guard or root guard on an interface.

Syntax `spanning-tree guard {loop | root | none}`

Parameters

- `loop` — Enables loop guard on an interface.
- `root` — Enables root guard on an interface.
- `none` — Sets the guard mode to none.

Default Not configured

Usage Information Root guard and loop guard configurations are mutually exclusive. Configuring one overwrites the other from the active configuration.

Command Mode INTERFACE

Example

```
OS10(conf-if-eth1/1/4)# spanning-tree guard root
```

Supported Releases 10.2.0E or later

spanning-tree mode

Enables an STP type (RSTP, Rapid-PVST+, or MST).

Syntax `spanning-tree mode {rstp | mst | rapid-pvst}`

Parameters

- `rstp` — Sets the STP mode to RSTP.
- `mst` — Sets the STP mode to MST.
- `rapid-pvst` — Sets the STP mode to RPVST+.

Default RPVST+

Command Mode CONFIGURATION

Usage Information All STP instances are stopped in the previous STP mode, and are restarted in the new mode. You can also change to RSTP/MST mode.

Example (RSTP)

```
OS10(config)# spanning-tree mode rstp
```

Example (MST)

```
OS10(config)# spanning-tree mode mst
```

Supported Releases 10.2.0E or later

spanning-tree mst

Configures an MST instance and determines root and bridge priorities.

Syntax `spanning-tree mst instance number priority | root {primary | secondary}`

Parameters

- `instance number` — Enter an MST instance number (0 to 63).

- `priority priority value` — Set a bridge priority value in increments of 4096 (0 to 61440). Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
- `root` — Enter a primary or secondary root.
- `primary` — Enter a device as a primary root.
- `secondary` — Enter a device as a secondary root.

Default Not configured

Command Mode CONFIGURATION

Usage Information The MSTP determines the root bridge but you can assign one bridge a lower priority to increase the probability it being the root bridge. A lower *priority-value* increases the probability of the bridge becoming a root bridge. The `no` version of this command resets the value to the default.

Example

```
OS10(config)# spanning-tree mst 0 priority 0
OS10(config)# spanning-tree mst 2 root primary
```

Supported Releases 10.2.0E or later

spanning-tree msti

Configures the MSTI, cost, and priority values for an interface.

Syntax `spanning-tree msti instance {cost cost | priority value}`

- Parameters**
- `msti instance` — Enter the MST instance number (0 to 63).
 - `cost cost` — (Optional) Enter a port cost value (1 to 200000000). Default values:
 - 100 Mb/s Ethernet interface = 200000
 - 1-Gigabit Ethernet interface = 20000
 - 10-Gigabit Ethernet interface = 2000
 - Port-channel interface with one 100 Mb/s Ethernet = 200000
 - Port-channel interface with one 1 Gigabit Ethernet = 20000
 - Port-channel interface with one 10 Gigabit Ethernet = 2000
 - Port-channel with two 1 Gigabit Ethernet = 18000
 - Port-channel with two 10 Gigabit Ethernet = 1800
 - Port-channel with two 100 Mbps Ethernet = 180000
 - `priority value` — Enter a value in increments of 16 as the priority (0 to 240, default 128) .

Default Priority value is 128

Command Mode INTERFACE

Usage Information The `cost` is a value based on the interface type. The greater the `cost` value, the less likely the port is selected to be a forwarding port. The `priority` influences the likelihood that a port is selected to be a forwarding port if several ports have the same cost.

Example

```
OS10(conf-if-eth1/1/1)# spanning-tree msti 1 priority 0
OS10(conf-if-eth1/1/1)# spanning-tree msti 1 cost 3
```

Supported Releases 10.2.0E or later

spanning-tree mst configuration

Enters MST mode to configure MSTP from Configuration mode.

Syntax `spanning-tree mst configuration`

Parameters None

Default	Disabled
Command Mode	CONFIGURATION
Usage Information	Use this command to enter STP MST configuration mode.

Example

```
OS10(config)# spanning-tree mst configuration
OS10(conf-mst)#
```

Supported Releases	10.2.0E or later
---------------------------	------------------

spanning-tree mst disable

Disables spanning tree on the specified MST instance.

Syntax	<code>spanning-tree mst <i>instance-number</i> disable</code>
Parameters	<i>instance-number</i> —Enter the instance number, ranging from 0 to 63.
Default	Enabled
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command enables spanning tree on the specified MST instance.

Example

```
OS10(config)# spanning-tree mst 10 disable
```

Supported Releases	10.4.0E(R1) or later
---------------------------	----------------------

spanning-tree mst force-version

Configures a forced version of STP to transmit BPDUs.

Syntax	<code>spanning-tree mst force-version {stp rstp}</code>
Parameters	<ul style="list-style-type: none"> • <code>stp</code> — Forces the version for the BPDUs transmitted by MST to STP. • <code>rstp</code> — Forces the version for the BPDUs transmitted by MST to RSTP.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	Forces a bridge that supports MST to operate in a STP-compatible mode.

Example

```
OS10(config)# spanning-tree mst force-version
```

Supported Releases	10.2.0E or later
---------------------------	------------------

spanning-tree mst forward-time

Configures a time interval for the interface to wait in the Blocking state or the Learning state before moving to the Forwarding state.

Syntax	<code>spanning-tree mst forward-time <i>seconds</i></code>
Parameters	<i>seconds</i> — Enter the number of seconds an interface waits in the Blocking or Learning States before moving to the Forwarding state (4 to 30).

Default	15 seconds
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# spanning-tree mst forward-time 16</pre>
Supported Releases	10.2.0E or later

spanning-tree mst hello-time

Sets the time interval between generation and transmission of MSTP BPDUs.

Syntax	<code>spanning-tree mst hello-time <i>seconds</i></code>
Parameters	<i>seconds</i> — Enter a hello-time interval value in seconds (1 to 10).
Default	2 seconds
Command Mode	CONFIGURATION
Usage Information	Dell EMC recommends increasing the hello-time for large configurations — especially configurations with multiple ports. The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# spanning-tree mst hello-time 5</pre>
Supported Releases	10.2.0E or later

spanning-tree mst mac-flush-threshold

Sets the threshold value for flushing the MAC addresses.

Syntax	<code>spanning-tree mst <i>instance-number</i> mac-flush-threshold <i>threshold-value</i></code>
Parameters	<ul style="list-style-type: none"> • <i>instance-number</i>—Enter the instance number, ranging from 0 to 63. • <i>threshold-value</i>—Enter the threshold value for the number of flushes, ranging from 0 to 65535. The default value is 5.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the threshold value.
Example	<pre>OS10(config)# spanning-tree mst 10 mac-flush-threshold 255</pre>
Supported Releases	10.4.0E(R1) or later

spanning-tree mst max-age

Configures the time period the bridge maintains configuration information before refreshing the information by recomputing the MST topology.

Syntax	<code>max-age <i>seconds</i></code>
Parameters	<i>seconds</i> — Enter a maximum age value in seconds (6 to 40).
Default	20 seconds

Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# spanning-tree mst max-age 10</pre>
Supported Releases	10.2.0E or later

spanning-tree mst max-hops

Configures the maximum hop count for a BPDU to travel before it is discarded.

Syntax	<code>spanning-tree mst max-hops <i>number</i></code>
Parameters	<i>number</i> — Enter a maximum hop value (6 to 40).
Default	20
Command Mode	CONFIGURATION
Usage Information	A device receiving BPDUs waits until the <code>max-hops</code> value expires before discarding it. When a device receives the BPDUs, it decrements the received value of the remaining hops and uses the resulting value as <code>remaining-hops</code> in the BPDUs. If the remaining MSTP 1333 hops reach zero, the device discards the BPDU and ages out any information that it holds for the port. The command configuration applies to all common IST (CIST) in the MST region.
Example	<pre>OS10(config)# spanning-tree mst max-hops 30</pre>
Supported Releases	10.2.0E or later

spanning-tree port

Sets the port type as the EdgePort.

Syntax	<code>spanning-tree port type edge</code>
Parameters	None
Default	Not configured
Command Mode	INTERFACE
Usage Information	When you configure an EdgePort on a device running STP, the port immediately transitions to Forwarding state. Only configured ports connected to end hosts act as EdgePorts.
Example	<pre>OS10(config)# spanning-tree port type edge</pre>
Supported Releases	10.2.0E or later

show spanning-tree mst

Displays MST configuration information.

Syntax	<code>show spanning-tree mst configuration</code>
Parameters	None
Default	Not configured
Command Mode	EXEC

Usage Information

Enable MSTI prior to using this command.

Example

```
OS10# show spanning-tree mst configuration
Region Name: asia
Revision: 0
MSTI    VID
0       1,7-4093
1       2
2       3
3       4
4       5
5       6
```

Supported Releases

10.2.0E or later

show spanning-tree msti

Displays MST instance information.

Syntax

```
show spanning-tree msti [instance-number [brief | guard | interface interface]]
```

Parameters

- *instance-number* — (Optional) Displays MST instance information (0 to 63).
- *brief* — (Optional) Displays MST instance summary information.
- *guard* — (Optional) Displays which guard is enabled and current port state.
- *interface interface* — (Optional) Displays interface type information:
 - *ethernet node/slot/port[:subport]* — Enter the Ethernet port information (1 to 48).
 - *port-channel* — Enter the port-channel interface information (1 to 128).

Default

Not configured

Command Mode

EXEC

Usage Information

View the MST instance information for a specific MST instance number in detail or brief, or view physical (Ethernet) port or port-channel information.

Example (Brief)

```
OS10# show spanning-tree msti 0 brief
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1-99,101-199,301-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 90b1.1cf4.9b8a
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID    Priority 32768, Address 90b1.1cf4.9b8a
We are the root of MSTI 0
Configured hello time 2, max age 20, forward delay 15, max hops 20
Interface
Name          PortID  Prio  Cost      Sts  Cost Bridge ID  PortID
-----
ethernet1/1/1 132.128 128 200000000 BLK  0 32768 90b1.1cf4.9b8a 128.132
ethernet1/1/2 136.128 128 200000000 BLK  0 32768 90b1.1cf4.9b8a 128.136
ethernet1/1/3 140.128 128 200000000 BLK  0 32768 90b1.1cf4.9b8a 128.140
ethernet1/1/4 144.128 128 200000000 BLK  0 32768 90b1.1cf4.9b8a 128.144
ethernet1/1/5 148.128 128 200000000 BLK  0 32768 90b1.1cf4.9b8a 128.148
ethernet1/1/6 152.128 128 200000000 BLK  0 32768 90b1.1cf4.9b8a 128.152
ethernet1/1/7 156.128 128 200000000 BLK  0 32768 90b1.1cf4.9b8a 128.156
...
Interface
Name          Role  PortID  Prio  Cost      Sts  Cost Link-type Edge
-----
ethernet1/1/1 Disb 128.132 128 200000000 BLK  0  SHARED  No
ethernet1/1/2 Disb 128.136 128 200000000 BLK  0  SHARED  No
ethernet1/1/3 Disb 128.140 128 200000000 BLK  0  SHARED  No
ethernet1/1/4 Disb 128.144 128 200000000 BLK  0  SHARED  No
ethernet1/1/5 Disb 128.148 128 200000000 BLK  0  SHARED  No
ethernet1/1/6 Disb 128.152 128 200000000 BLK  0  SHARED  No
```

```

ethernet1/1/7 Disb 128.156 128 200000000 BLK 0 SHARED No
ethernet1/1/8 Disb 128.160 128 200000000 BLK 0 SHARED No
ethernet1/1/9 Disb 128.164 128 200000000 BLK 0 SHARED No

```

Example (Interface)

```

OS10# show spanning-tree msti 1 interface ethernet 1/1/1
ethernet1/1/1 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary :internal bpdu filter : bpdu guard : bpduguard shutdown-on-
violation :disable RootGuard: disable LoopGuard disable
Bpdus (MRecords) sent 3779, received 7
Interface                               Designated
  Name      PortID  Prio  Cost  Sts Cost Bridge ID      PortID
-----
ethernet1/1/1 128.132 128 20000 FWD 0 32768 74e6.e2f5.dd80 128.132

```

Example (Guard)

```

OS10# show spanning-tree msti 1 guard
Interface
Name              Instance  Sts   Guard Type
-----
ethernet1/1/1     MSTI 1    FWD  root
ethernet1/1/2     MSTI 1    FWD  loop
ethernet1/1/3     MSTI 1    BLK  none
ethernet1/1/4     MSTI 1    FWD  none
ethernet1/1/5     MSTI 1    BLK  none
ethernet1/1/6     MSTI 1    BLK  none
ethernet1/1/7     MSTI 1    BLK  none
ethernet1/1/8     MSTI 1    BLK  none
...

```

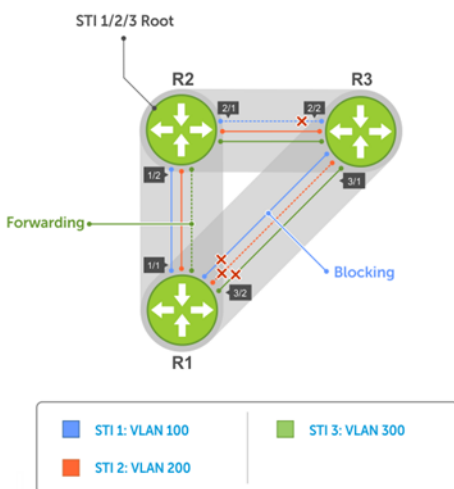
Command History 10.2.0E or later

Rapid per-VLAN spanning-tree plus

RPVST+ is an RSTP to create a single topology per VLAN. RPVST+ is enabled by default, provides faster convergence, and runs on the default VLAN (VLAN 1).

Configuring Rapid-PVST+ is a four-step process:

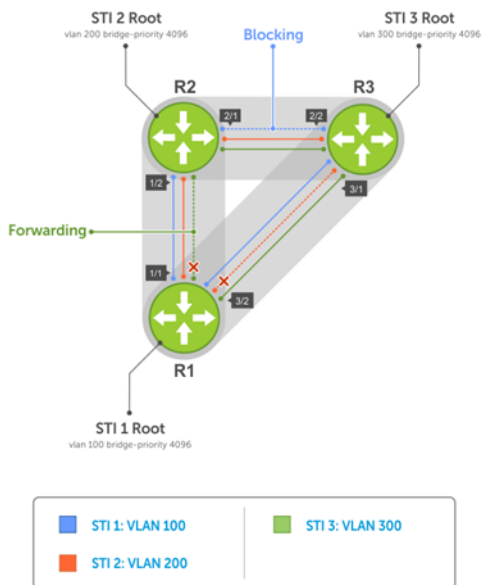
1. Ensure the interfaces are in L2 mode.
2. Place the interfaces in VLANs. By default, switchport interfaces are members of the default (VLAN1).
3. Enable Rapid-PVST+ (only required if another variation of STP is present).
4. (Optional) Select a non-default bridge-priority for the VLAN for load balancing.



By default, each VLAN instance is assigned default bridge priority 32768. For example, all three instances have the same forwarding topology. Traffic load balancing is not achievable with this kind of priority assignment. You must assign each instance a different priority to achieve load balancing, as shown in Load Balancing with RPVST+.

Load balance and root selection

All VLANs use the same forwarding topology — R2 is elected as the root and all 10G Ethernet ports have the same cost. RPVST+ changes the bridge priority of each bridge so that a different forwarding topology generates for each VLAN.



To achieve RPVST+ load balancing, assign a different priority on each bridge.

Enable RPVST+

By default, RPVST+ is enabled and creates an instance only after you add the first member port to a VLAN. Port-channel or physical interfaces must be a member of a VLAN to participate in RPVST+. Add all physical and port-channel interfaces to the default VLAN (VLAN1).

- Enable the Rapid-PVST+ mode in CONFIGURATION mode.

```
spanning-tree mode rapid-pvst
```

Configure RPVST+

```
OS10(config)# spanning-tree mode rapid-pvst
```

View RPVST+ configuration

```
OS10# show spanning-tree active
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32769, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID  Prio Cost Sts  Cost Bridge ID      Designated PortID
-----
ethernet1/1/5 128.276 128 500 FWD 0    32768 3417.4455.667f 128.146
ethernet1/1/6 128.280 128 500 BLK 0    32768 3417.4455.667f 128.150
Interface
Name          Role  PortID  Prio Cost Sts  Cost Link-type Edge
```

```
-----
ethernet1/1/5  Root  128.276  128  500  FWD  0    AUTO    No
ethernet1/1/6  Altr  128.280  128  500  BLK  0    AUTO    No
-----
```

Select root bridge

RPVST+ determines the root bridge. Assign one bridge a lower priority to increase the likelihood that it becomes the root bridge. The `show spanning-tree brief` command displays information about all ports regardless of the operational status.

- Assign a number as the bridge priority or designate it as the root in CONFIGURATION mode (0 to 61440).

```
spanning-tree {vlan vlan-id priority priority-value}
```

- `vlan-id` — Enter a value between 1 to 4093.
- `priority priority-value` — Enter the priority value in increments of 4096, default is 32768. The lower the number assigned, the more likely this bridge becomes the root bridge. The bridge priority the valid values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440. All other values are rejected.

Configure root bridge

```
OS10(config)# spanning-tree vlan 1 priority 4096
```

View active configuration

```
OS10(config)# do show spanning-tree active
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 4097, Address 90b1.1cf4.a523
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 4097, Address 90b1.1cf4.a523
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID   Prio Cost Sts  Cost Bridge ID      Designated
-----
ethernet1/1/5 128.276 128  500 FWD  0    4097  90b1.1cf4.a523 128.276
ethernet1/1/6 128.280 128  500 FWD  0    4097  90b1.1cf4.a523 128.280
Interface
Name          Role   PortID   Prio Cost Sts  Cost Link-type Edge
-----
ethernet1/1/5 Desg  128.276 128  500 FWD  0    AUTO    No
ethernet1/1/6 Desg  128.280 128  500 FWD  0    AUTO    No
```

View brief configuration

```
OS10# show spanning-tree brief
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 4097, Address 90b1.1cf4.a523
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 4097, Address 90b1.1cf4.a523
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID   Prio Cost      Sts  Cost Bridge ID      Designated
-----
ethernet1/1/1 128.260 128  200000000 FWD  0    32769 0000.0000.0000 128.260
ethernet1/1/2 128.264 128  200000000 FWD  0    32769 0000.0000.0000 128.264
ethernet1/1/3 128.268 128  200000000 FWD  0    32769 0000.0000.0000 128.268
ethernet1/1/4 128.272 128  200000000 FWD  0    32769 0000.0000.0000 128.272
ethernet1/1/5 128.276 128  500        FWD  0    4097  90b1.1cf4.a523 128.276
ethernet1/1/6 128.280 128  500        FWD  0    4097  90b1.1cf4.a523 128.280
ethernet1/1/7 128.284 128  200000000 FWD  0    32769 0000.0000.0000 128.284
ethernet1/1/8 128.288 128  200000000 FWD  0    32769 0000.0000.0000 128.288
ethernet1/1/9 128.292 128  200000000 FWD  0    32769 0000.0000.0000 128.292
```

ethernet1/1/10	128.296	128	200000000	FWD	0	32769	0000.0000.0000	128.296
ethernet1/1/11	128.300	128	200000000	FWD	0	32769	0000.0000.0000	128.300
ethernet1/1/12	128.304	128	200000000	FWD	0	32769	0000.0000.0000	128.304
ethernet1/1/13	128.308	128	200000000	FWD	0	32769	0000.0000.0000	128.308
ethernet1/1/14	128.312	128	200000000	FWD	0	32769	0000.0000.0000	128.312
ethernet1/1/15	128.316	128	200000000	FWD	0	32769	0000.0000.0000	128.316
ethernet1/1/16	128.320	128	200000000	FWD	0	32769	0000.0000.0000	128.320
ethernet1/1/17	128.324	128	200000000	FWD	0	32769	0000.0000.0000	128.324
ethernet1/1/18	128.328	128	200000000	FWD	0	32769	0000.0000.0000	128.328
ethernet1/1/19	128.332	128	200000000	FWD	0	32769	0000.0000.0000	128.332
ethernet1/1/20	128.336	128	200000000	FWD	0	32769	0000.0000.0000	128.336
ethernet1/1/21	128.340	128	200000000	FWD	0	32769	0000.0000.0000	128.340
ethernet1/1/22	128.344	128	200000000	FWD	0	32769	0000.0000.0000	128.344
ethernet1/1/23	128.348	128	200000000	FWD	0	32769	0000.0000.0000	128.348
ethernet1/1/24	128.352	128	200000000	FWD	0	32769	0000.0000.0000	128.352
ethernet1/1/25	128.356	128	200000000	FWD	0	32769	0000.0000.0000	128.356
ethernet1/1/26	128.360	128	200000000	FWD	0	32769	0000.0000.0000	128.360
ethernet1/1/27	128.364	128	200000000	FWD	0	32769	0000.0000.0000	128.364
ethernet1/1/28	128.368	128	200000000	FWD	0	32769	0000.0000.0000	128.368
ethernet1/1/29	128.372	128	200000000	FWD	0	32769	0000.0000.0000	128.372
ethernet1/1/30	128.376	128	200000000	FWD	0	32769	0000.0000.0000	128.376
ethernet1/1/31	128.380	128	200000000	FWD	0	32769	0000.0000.0000	128.380
ethernet1/1/32	128.384	128	200000000	FWD	0	32769	0000.0000.0000	128.384

Interface								
Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
ethernet1/1/1	Disb	128.260	128	200000000	FWD	0	AUTO	No
ethernet1/1/2	Disb	128.264	128	200000000	FWD	0	AUTO	No
ethernet1/1/3	Disb	128.268	128	200000000	FWD	0	AUTO	No
ethernet1/1/4	Disb	128.272	128	200000000	FWD	0	AUTO	No
ethernet1/1/5	Desg	128.276	128	500	FWD	0	AUTO	No
ethernet1/1/6	Desg	128.280	128	500	FWD	0	AUTO	No
ethernet1/1/7	Disb	128.284	128	200000000	FWD	0	AUTO	No
ethernet1/1/8	Disb	128.288	128	200000000	FWD	0	AUTO	No
ethernet1/1/9	Disb	128.292	128	200000000	FWD	0	AUTO	No
ethernet1/1/10	Disb	128.296	128	200000000	FWD	0	AUTO	No
ethernet1/1/11	Disb	128.300	128	200000000	FWD	0	AUTO	No

Root assignment

RPVST+ assigns the root bridge according to the lowest bridge ID. Assign one bridge as root bridge and the other as a secondary root bridge.

- Configure the device as the root or secondary root in CONFIGURATION mode.

```
spanning-tree vlan vlan-id root {primary | secondary}
```

- *vlan-id* — Enter the VLAN ID number (1 to 4093).
- *primary* — Enter the bridge as primary or root bridge (primary bridge value is 24576).
- *secondary* — Enter the bridge as secondary or secondary root bridge (secondary bridge value is 28672).

Configure root bridge as primary

```
OS10(config)# spanning-tree vlan 1 root primary
```

Verify root bridge information

```
OS10# show spanning-tree active
```

```
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 24577, Address 90b1.1cf4.a523
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 24577, Address 90b1.1cf4.a523
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID  Prio  Cost  Sts  Cost  Bridge ID          Designated
                                     PortID
```

```
-----
```

ethernet1/1/5	128.276	128	500	FWD	0	24577	90b1.1cf4.a523	128.276
ethernet1/1/6	128.280	128	500	LRN	0	24577	90b1.1cf4.a523	128.280
Interface Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
ethernet1/1/5	Desg	128.276	128	500	FWD	0	AUTO	No
ethernet1/1/6	Desg	128.280	128	500	LRN	0	AUTO	No

```
-----
```

Loop guard

This information explains how to configure loop guard on an interface.

- Enable loop guard on a per-port or port-channel interface in INTERFACE mode.

```
spanning-tree guard {loop | root | none}
```

- `loop` — Enables loop guard on an interface.
- `root` — Enables root on an interface.
- `none` — Enables the guard mode to none.
- Disable loop guard on a port or port-channel interface in INTERFACE mode.

```
no spanning-tree guard loop
```

Port enabled with loop guard conditions

- Loop guard is supported on any STP-enabled port or port-channel interface in RPVST+ mode.
- You cannot enable root guard and loop guard at the same time on an STP port — the loop guard configuration overwrites an existing root guard configuration and vice versa.
- Enabling BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when you configure both Portfast BPDU guard and loop guard:
 - If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic forwards on the port.
 - If no BPDU is received from a remote device which was sending BPDUs, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic forwards on the port.
- When used in a PVST+ network, STP loop guard performs per-port or per port-channel at a VLAN level. If no BPDUs are received on a port-channel interface, the port or port-channel transitions to a Loop-Inconsistent (Blocking) state only for this VLAN.

Global parameters

All non-root bridges accept the timer values on the root bridge.

- Forward-time** Amount of time required for an interface to transition from the Discarding to the Learning state or from the Learning to the Forwarding state.
- Hello-time** Time interval within which the bridge sends BPDUs.
- Max-age** Length of time the bridge maintains configuration information before it refreshes information by recomputing the RPVST+ topology.

- Modify the forward-time (in seconds) in CONFIGURATION mode (4 to 30, default 15).

```
spanning-tree vlan vlan-id forward-time seconds
```

- Modify the hello-time (in seconds) in CONFIGURATION mode (1 to 10, default 2). With large configurations (involving more number of ports), Dell EMC recommends increasing the hello-time.

```
spanning-tree vlan vlan-id hello-time seconds
```

- Modify the max-age (in seconds) in CONFIGURATION mode (6 to 40, default 20).

```
spanning-tree vlan vlan-id max-age seconds
```


View RPVST+ global parameters

```
OS10# show spanning-tree active
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 32769, Address 90b1.1cf4.a523
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID   Priority 32769, Address 90b1.1cf4.a523
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
```

RPVST+ commands

clear spanning-tree counters

Clears the counters for STP.

Syntax `clear spanning-tree counters [interface {ethernet node/slot/port[:subport] | port-channel number}]`

Parameters

- `interface` — Enter the interface type:
 - `ethernet node/slot/port[:subport]` — Deletes the spanning-tree counters from a physical port.
 - `port-channel number` — Deletes the spanning-tree counters for a port-channel interface (1 to 128).

Default Not configured

Command Mode EXEC

Usage Information Clear all STP counters on the device per Ethernet interface or port-channel.

Example

```
OS10# clear spanning-tree counters interface port-channel 10
```

Supported Releases 10.2.0E or later

clear spanning-tree detected-protocol

Forces the MST ports to renegotiate with neighbors.

Syntax `clear spanning-tree detected-protocol [interface {ethernet node/slot/port[:subport] | port-channel number}]`

Parameters

- `interface` — Enter the interface type:
 - `ethernet node/slot/port[:subport]` — Enter the Ethernet interface information (1 to 48).
 - `port-channel number` — Enter the port-channel number (1 to 128).

Default Not configured

Command Mode EXEC

Usage Information Use this command to force the RPVST+ port to re-negotiate with neighbors. If you use this command without parameters, the command applies to each device port.

Example

```
OS10# clear spanning-tree detected-protocol interface ethernet 1/1/1
```

Supported Release 10.2.0E or later

show spanning-tree vlan

Displays RPVST+ status and configuration information by VLAN ID.

Syntax	<code>show spanning-tree vlan <i>vlan-id</i></code>
Parameters	<code>vlan <i>vlan-id</i></code> — Enter the VLAN ID number (1 to 4093)
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show spanning-tree
Spanning tree enabled protocol rapid-pvst
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 32769, Address 74e6.e2f5.bb80
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID   Priority 32769, Address 74e6.e2f5.bb80
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID  Prio Cost      Sts Cost Bridge ID      Designated
-----
ethernet1/1/1 128.260 128 200000000 FWD 0    32769 0000.0000.0000 128.260
ethernet1/1/2 128.264 128 200000000 FWD 0    32769 0000.0000.0000 128.264
ethernet1/1/3 128.268 128 200000000 FWD 0    32769 0000.0000.0000 128.268
ethernet1/1/4 128.272 128 200000000 FWD 0    32769 0000.0000.0000 128.272
ethernet1/1/5 128.276 128 200000000 FWD 0    32769 0000.0000.0000 128.276
ethernet1/1/6 128.280 128 200000000 FWD 0    32769 0000.0000.0000 128.280
ethernet1/1/7 128.284 128 200000000 FWD 0    32769 0000.0000.0000 128.284
ethernet1/1/8 128.288 128 200000000 FWD 0    32769 0000.0000.0000 128.288
ethernet1/1/9 128.292 128 200000000 FWD 0    32769 0000.0000.0000 128.292
ethernet1/1/10 128.296 128 200000000 FWD 0    32769 0000.0000.0000 128.296
ethernet1/1/11 128.300 128 200000000 FWD 0    32769 0000.0000.0000 128.300
ethernet1/1/12 128.304 128 200000000 FWD 0    32769 0000.0000.0000 128.304
```

Supported Releases 10.2.0E or later

spanning-tree bpdudfilter

Enables or disables BPDU filtering on an interface.

Syntax	<code>spanning-tree bpdudfilter {enable disable}</code>
Parameters	<ul style="list-style-type: none">• <code>enable</code> — Enables the BPDU filtering on an interface.• <code>disable</code> — Disables the BPDU filtering on an interface.
Default	Disabled
Command Mode	INTERFACE
Usage Information	Use the <code>enable</code> parameter to enable BPDU filtering.

Example

```
OS10(conf-if-eth1/1/4)# spanning-tree bpdudfilter enable
```

Supported Releases 10.2.0E or later

spanning-tree bpduguard

Enables or disables BPDU guard on an interface.

Syntax	<code>spanning-tree bpduguard {enable disable}</code>
Parameters	<ul style="list-style-type: none">• <code>enable</code> — Enables the BPDU guard filter on an interface.• <code>disable</code> — Disables the BPDU guard filter on an interface.
Default	Disabled
Command Mode	INTERFACE
Usage Information	BPDU guard prevents a port from receiving BPDUs. If the port receives a BPDU, it is placed in the Error-Disabled state as a protective measure.
Example	<pre>OS10(config-if-eth1/1/4)# spanning-tree bpduguard enable</pre>
Supported Releases	10.2.0E or later

spanning-tree disable

Disables the spanning-tree mode configured with the `spanning-tree mode` command globally on the switch or on specified interfaces.

Syntax	<code>spanning-tree disable</code>
Parameters	None
Default	Not configured.
Usage Information	The <code>no</code> version of this command re-enables STP and applies the currently configured spanning-tree settings.
Command Mode	CONFIGURATION INTERFACE
Example	<pre>OS10(config)# interface ethernet 1/1/4 OS10(config-if-eth1/1/4)# spanning-tree disable</pre>
Supported Releases	10.3.0E or later

spanning-tree guard

Enables or disables loop guard or root guard on an interface.

Syntax	<code>spanning-tree guard {loop root none}</code>
Parameters	<ul style="list-style-type: none">• <code>loop</code> — Enables loop guard on an interface.• <code>root</code> — Enables root guard on an interface.• <code>none</code> — Sets the guard mode to none.
Default	Not configured
Usage Information	Root guard and loop guard configurations are mutually exclusive. Configuring one overwrites the other from the active configuration.
Command Mode	INTERFACE
Example	<pre>OS10(config-if-eth1/1/4)# spanning-tree guard root</pre>

Supported Releases 10.2.0E or later

spanning-tree mode

Enables an STP type (RSTP, Rapid-PVST+, or MST).

Syntax `spanning-tree mode {rstp | mst | rapid-pvst}`

- Parameters**
- `rstp` — Sets the STP mode to RSTP.
 - `mst` — Sets the STP mode to MST.
 - `rapid-pvst` — Sets the STP mode to RPVST+.

Default RPVST+

Command Mode CONFIGURATION

Usage Information All STP instances are stopped in the previous STP mode, and are restarted in the new mode. You can also change to RSTP/MST mode.

Example (RSTP)

```
OS10(config)# spanning-tree mode rstp
```

Example (MST)

```
OS10(config)# spanning-tree mode mst
```

Supported Releases 10.2.0E or later

spanning-tree port

Sets the port type as the EdgePort.

Syntax `spanning-tree port type edge`

Parameters None

Default Not configured

Command Mode INTERFACE

Usage Information When you configure an EdgePort on a device running STP, the port immediately transitions to Forwarding state. Only configured ports connected to end hosts act as EdgePorts.

Example

```
OS10(config)# spanning-tree port type edge
```

Supported Releases 10.2.0E or later

spanning-tree vlan cost

Sets the path cost of the interface per VLAN for PVST calculations.

Syntax `spanning-tree vlan vlan-id cost {value}`

Parameters *value* — Enter a port cost value to set the path cost of the interface for PVST calculations (1 to 200000000).

- Defaults**
- 100-Mb/s Ethernet interface = 200000
 - 1-Gigabit Ethernet interface = 20000
 - 10-Gigabit Ethernet interface = 2000
 - Port-channel interface with one 100-Mb/s Ethernet = 200000
 - Port-channel interface with one 1-Gigabit Ethernet = 20000

- Port-channel interface with one 10 Gigabit Ethernet = 2000
- Port-channel with two 1 Gigabit Ethernet = 18000
- Port-channel with two 10 Gigabit Ethernet = 1800
- Port-channel with two 100 Mbps Ethernet = 180000

Command Mode INTERFACE

Usage Information The media speed of a LAN interface determines the STP port path cost default value.

Example

```
OS10(conf-if-eth1/1/4)# spanning-tree vlan 10 cost 1000
```

Supported Releases 10.2.0E or later

spanning-tree vlan disable

Disables spanning tree on specified VLAN.

Syntax `spanning-tree vlan vlan-id disable`

Parameters *vlan-id* — Enter the VLAN ID number, ranging from 1 to 4093.

Default Enabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command enables spanning tree on the specified VLAN.

Example

```
OS10(config)# spanning-tree vlan 100 disable
```

Supported Releases 10.4.0E(R1) or later

spanning-tree vlan forward-time

Configures a time interval for the interface to wait in Blocking state or Learning state before moving to Forwarding state.

Syntax `spanning-tree vlan vlan-id forward-time seconds`

Parameters

- *vlan-id* — Enter a VLAN ID number (1 to 4093).
- *seconds* — Enter the forward-delay time in seconds (4 to 30).

Default 15 seconds

Command Mode CONFIGURATION

Usage Information None

Example

```
OS10(config)# spanning-tree vlan 10 forward-time 16
```

Supported Releases 10.2.0E or later

spanning-tree vlan force-version

Configures a forced version of spanning-tree to transmit BPDUs.

Syntax `spanning-tree vlan vlan-id force-version {stp | rstp}`

Parameters

- `stp` — Forces the version for the BPDUs transmitted by RPVST+ to STP.

- `rstp` — Forces the version for the BPDUs transmitted by RPVST+ to RSTP

Default Not configured

Command Mode CONFIGURATION

Usage Information Forces a bridge that supports RPVST+ to operate in a STP-compatible mode.

Example

```
OS10(config)# spanning-tree mst force-version
```

Supported Releases 10.2.0E or later

spanning-tree vlan hello-time

Sets the time interval between generation and transmission of RPVST BPDUs.

Syntax `spanning-tree vlan vlan-id hello-time seconds`

- Parameters**
- `vlan-id` — Enter the VLAN ID number (1 to 4093).
 - `seconds` — Enter a hello-time interval value in seconds (1 to 10).

Default 2 seconds

Command Mode CONFIGURATION

Usage Information Dell EMC recommends increasing the hello-time for large configurations — especially configurations with multiple ports.

Example

```
OS10(config)# spanning-tree vlan 10 hello-time 5
```

Supported Releases 10.2.0E or later

spanning-tree vlan mac-flush-threshold

Sets the threshold value to flush MAC addresses on specified VLAN.

Syntax `spanning-tree vlan vlan-id mac-flush-threshold threshold-value`

- Parameters**
- `vlan-id` — Enter the VLAN ID number, ranging from 1 to 4093.
 - `threshold-value`—Enter the threshold value for the number of flushes, ranging from 0 to 65535. The default value is 0.

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the threshold value.

Example

```
OS10(config)# spanning-tree vlan 100 mac-flush-threshold 255
```

Supported Releases 10.4.0E(R1) or later

spanning-tree vlan max-age

Configures the time period the bridge maintains configuration information before refreshing the information by recomputing RPVST.

Syntax `spanning-tree vlan vlan-id max-age seconds`

Parameters	<code>max-age seconds</code> — Enter a maximum age value in seconds (6 to 40).
Default	20 seconds
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(config)# spanning-tree vlan 10 max-age 10</pre>
Supported Releases	10.2.0E or later

spanning-tree vlan priority

Sets the priority value for RPVST+.

Syntax	<code>spanning-tree vlan <i>vlan-id</i> priority <i>priority value</i></code>
Parameters	<code>priority <i>priority value</i></code> — Enter a bridge-priority value in increments of 4096 (0 to 61440). Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The RPVST+ protocol determines the root bridge but you can assign one bridge a lower priority to increase the probability it being the root bridge. A lower <i>priority value</i> increases the probability of the bridge becoming a root bridge.
Example	<pre>OS10(config)# spanning-tree vlan 10 priority 0</pre>
Supported Releases	10.2.0E or later

spanning-tree vlan priority (Interface)

Sets an interface priority when two bridges compete for position as the root bridge.

Syntax	<code>spanning-tree vlan <i>vlan-id</i> priority <i>value</i></code>
Parameters	<code>value</code> — Enter a priority value in the increments of 16 (0 to 240).
Default	128
Command Mode	INTERFACE
Usage Information	Breaks the tie between the two bridges which compete for root bridge.
Example	<pre>OS10(conf-if-eth1/1/4)# spanning-tree vlan 10 priority 16</pre>
Supported Releases	10.2.0E or later

spanning-tree vlan root

Designates a device as primary or secondary root bridge.

Syntax	<code>spanning-tree vlan <i>vlan-id</i> root {primary secondary}</code>
Parameters	<ul style="list-style-type: none"> <code><i>vlan-id</i></code> — Enter a VLAN ID number (1 to 4093).

- `root` — Designate the bridge as primary or secondary root.
- `primary` — Designate the bridge as primary or root bridge.
- `secondary` — Designate the bridge as secondary or secondary root bridge.

Default	Not configured
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(config)# spanning-tree vlan 1 root primary</pre>
Supported Releases	10.2.0E or later

Rapid Spanning-Tree Protocol

Rapid Spanning-Tree Protocol (RSTP) is similar to STP, but provides faster convergence and interoperability with devices configured with STP and MSTP. RSTP is disabled by default. All enabled interfaces in L2 mode are automatically added to the RSTP topology.

Configuring RSTP is a two-step process:

1. Ensure that the interfaces are in L2 mode.
2. Globally enable RSTP.

Enable globally

RSTP enables STP on all physical and port-channel interfaces which are in L2 mode to automatically include the interfaces as part of the RSTP topology. Only one path from any bridge to any other bridge is enabled. Bridges block a redundant path by disabling one of the link ports.

- Configure spanning-tree mode to RSTP in CONFIGURATION mode.

```
spanning-tree mode rstp
```

- Disable RSTP globally for all L2 interfaces in CONFIGURATION mode.

```
spanning-tree disable
```

- Remove an interface from the RSTP topology in INTERFACE mode.

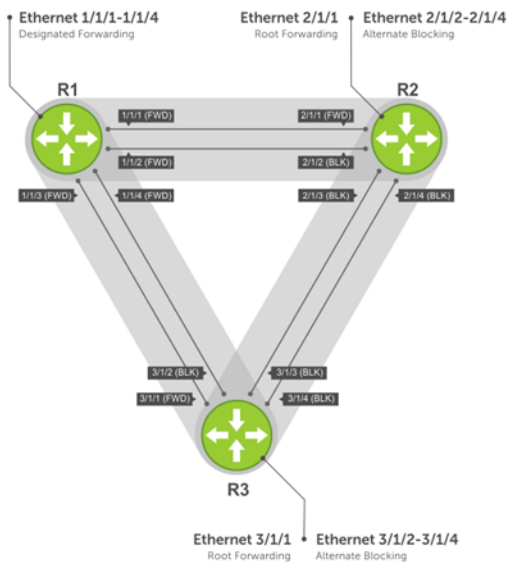
```
spanning-tree disable
```

- Re-enable an interface in INTERFACE mode.

```
no spanning-tree disable
```

- Re-enable RSTP globally for all L2 interfaces in CONFIGURATION mode.

```
no spanning-tree disable
```

View all port participating in RSTP

```
OS10# show spanning-tree
Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32768, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID      Prio  Cost      Sts      Cost Bridge ID          PortID
-----
ethernet1/1/1 128.260    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/2 128.264    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/3 128.268    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/4 128.272    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/5:1 128.276    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/5:2 128.277    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/5:3 128.278    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/5:4 128.279    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/6:1 128.280    128   2000      FWD     0      32768 3417.4455.667f    128.150
ethernet1/1/6:2 128.281    128   2000      FWD     0      32768 3417.4455.667f    128.151
ethernet1/1/6:3 128.282    128   2000      FWD     0      32768 3417.4455.667f    128.152
ethernet1/1/6:4 128.283    128   2000      BLK     0      32768 3417.4455.667f    128.153
ethernet1/1/7 128.284    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/8 128.288    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/9 128.292    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/10 128.296    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/11 128.300    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/12 128.304    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/13 128.308    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/14 128.312    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/15 128.316    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/16 128.320    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/17 128.324    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/18 128.328    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/19 128.332    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/20 128.336    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/21 128.340    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/22 128.344    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/23 128.348    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/24 128.352    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/25 128.356    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/26 128.360    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/27 128.364    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/28 128.368    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/29 128.372    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/30 128.376    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/31 128.380    128   200000000 BLK      0      0      0000.0000.0000    0.0
ethernet1/1/32 128.384    128   200000000 BLK      0      0      0000.0000.0000    0.0
```

Interface Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
ethernet1/1/1	Disb	128.260	128	200000000	BLK	0	AUTO	No
ethernet1/1/2	Disb	128.264	128	200000000	BLK	0	AUTO	No
ethernet1/1/3	Disb	128.268	128	200000000	BLK	0	AUTO	No
ethernet1/1/4	Disb	128.272	128	200000000	BLK	0	AUTO	No
ethernet1/1/5:1	Disb	128.276	128	200000000	BLK	0	AUTO	No

Global parameters

The root bridge sets the values for forward-time, hello-time, and max-age, and overwrites the values set on other bridges participating in the RSTP group. Dell EMC recommends that only experienced network administrators change the RSTP group parameters. Poorly planned modification of the RSTP parameters can negatively affect network performance.

Forward-time 15 seconds — Amount of time an interface waits in the Listening state and the Learning state before it transitions to the Forwarding state.

Hello-time 2 seconds — Time interval in which the bridge sends RSTP BPDUs.

Max-age 20 seconds — Length of time the bridge maintains configuration information before it refreshes that information by recomputing the RSTP topology.

Port cost Port cost values to set the path cost of the interface:

- 100-Mb/s Ethernet interfaces — 200000
- 1-Gigabit Ethernet interfaces — 20000
- 10-Gigabit Ethernet interfaces — 2000
- 40-Gigabit Ethernet interfaces — 500
- Port-channel with 100 Mb/s Ethernet interfaces — 200000
- Port-channel with 1-Gigabit Ethernet interfaces — 20000
- Port-channel with 10-Gigabit Ethernet interfaces — 2000
- Port-channel with 1x40Gigabit Ethernet interface — 500
- Port-channel with 2x40Gigabit Ethernet interfaces — 250

- Change the forward-time in CONFIGURATION mode (4 to 30, default 15).

```
spanning-tree rstp forward-time seconds
```

- Change the hello-time in CONFIGURATION mode (1 to 10, default 2). With large configurations (especially those configurations with more ports) Dell EMC recommends increasing the hello-time.

```
spanning-tree rstp hello-time seconds
```

- Change the max-age in CONFIGURATION mode (6 to 40, default 20).

```
spanning-tree rstp max-age seconds
```

View current interface parameters

```
OS10# show spanning-tree active
```

```
Spanning tree enabled protocol rstp with force-version rstp
```

```
Executing IEEE compatible Spanning Tree Protocol
```

```
Root ID Priority 32768, Address 90b1.1cf4.9b8a
```

```
Root Bridge hello time 2, max age 20, forward delay 15
```

```
Bridge ID Priority 32768, Address 90b1.1cf4.9b8a
```

```
We are the root
```

```
Configured hello time 2, max age 20, forward delay 15
```

```
Interface Designated
```

```
Name PortID Prio Cost Sts Cost Bridge ID PortID
```

```
-----
```

ethernet3/1/1	244.128	128	500	BLK	0	32768	90b1.1cf4.9b8a	128.244
ethernet3/1/2	248.128	128	500	BLK	0	32768	90b1.1cf4.9b8a	128.248
ethernet3/1/3	252.128	128	500	FWD	0	32768	90b1.1cf4.9b8a	128.252
ethernet3/1/4	256.128	128	500	BLK	0	32768	90b1.1cf4.9b8a	128.256

```
Interface
```

```
Name Role PortID Prio Cost Sts Cost Link-type Edge
```

```
-----
ethernet3/1/1 Altr 128.244 128 500 BLK 0 AUTO No
ethernet3/1/2 Altr 128.248 128 500 BLK 0 AUTO No
ethernet3/1/3 Root 128.252 128 500 FWD 0 AUTO No
ethernet3/1/4 Altr 128.256 128 500 BLK 0 AUTO No
-----
```

Interface parameters

Set the port cost and port priority values on interfaces in L2 mode.

Port cost Value that is based on the interface type. The previous table lists the default values. The greater the port cost, the less likely the port is selected to be a forwarding port.

Port priority Influences the likelihood that a port is selected to be a forwarding port in case that several ports have the same port cost.

- Change the port cost of an interface in INTERFACE mode (1 to 200000000).

```
spanning-tree rstp cost cost
```

- Change the port priority of an interface in INTERFACE mode (0 to 240, default 128).

```
spanning-tree rstp priority priority-value
```

View current global parameter values

```
OS10# show spanning-tree active

Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 90b1.1cf4.9b8a
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32768, Address 90b1.1cf4.9b8a
We are the root
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID  Prio Cost Sts Cost Bridge ID  PortID
-----
ethernet3/1/1 244.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.244
ethernet3/1/2 248.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.248
ethernet3/1/3 252.128 128 500 FWD 0 32768 90b1.1cf4.9b8a 128.252
ethernet3/1/4 256.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.256
Interface
Name          Role PortID  Prio Cost Sts Cost Link-type Edge
-----
ethernet3/1/1 Altr 128.244 128 500 BLK 0 AUTO No
ethernet3/1/2 Altr 128.248 128 500 BLK 0 AUTO No
ethernet3/1/3 Root 128.252 128 500 FWD 0 AUTO No
ethernet3/1/4 Altr 128.256 128 500 BLK 0 AUTO No
```

Root bridge selection

RSTP determines the root bridge. Assign one bridge a lower priority to increase the likelihood that it is selected as the root bridge.

- Assign a number as the bridge priority or designate it as the primary or secondary root in CONFIGURATION mode. Configure the priority value range (0 to 65535 in multiples of 4096, default 32768). The lower the number assigned, the more likely this bridge becomes the root bridge.

```
spanning-tree rstp priority priority-value
```

View bridge priority and root bridge assignment

```
OS10# show spanning-tree active
Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
```

```

Root ID      Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 36864, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15
Interface
Name          PortID  Prio  Cost  Sts  Cost Bridge ID      Designated
-----
ethernet1/1/6:3 128.282 128   2000  FWD  0    32768 3417.4455.667f 128.152
ethernet1/1/6:4 128.283 128   2000  BLK  0    32768 3417.4455.667f 128.153
Interface
Name          Role   PortID  Prio  Cost  Sts  Cost Link-type Edge
-----
ethernet1/1/6:3  Root 128.282 128   2000  FWD  0    AUTO    No
ethernet1/1/6:4  Altr 128.283 128   2000  BLK  0    AUTO    No

```

EdgePort forward traffic

EdgePort allows the interface to forward traffic approximately 30 seconds sooner as it skips the Blocking and Learning states. The spanning-tree bpduguard enable command causes the interface hardware to shut down when it receives a BPDU.

CAUTION: Configure EdgePort only on links connecting to an end station. EdgePort can cause loops if you enable it on an interface connected to a network.

- Enable EdgePort on an interface in INTERFACE mode.

```
spanning-tree port type edge
```

Configure EdgePort and view interface status

```
OS10(conf-if-eth1/1/5)# spanning-tree port type edge
```

View interface status

```

OS10# show spanning-tree interface ethernet 1/1/5
ethernet1/1/5 of RSTP 1 is designated Forwarding
Edge port:yes port guard :none (default)
Link type is point-to-point (auto)
Boundary: YES bpdu filter :disable bpdu guard :disable bpduguard shutdown-on-
violation :disable RootGuard: disable LoopGuard disable
Bpdus (MRecords) sent 610, received 5
Interface
Name          PortID  Prio  Cost  Sts  Cost Bridge ID      Designated
-----
ethernet1/1/5 128.272 128   500   FWD  0    32768 90b1.1cf4.a911 128.272
=====

```

Spanning-tree extensions

STP extensions ensure efficient network convergence by securely enforcing the active network topology. OS10 supports BPDU filtering, BPDU guard, loop guard, and root guard STP extensions.

- BPDU filtering** Protects the network from unexpected flooding of BPDUs from an erroneous device. Enabling BPDU Filtering instructs the hardware to drop BPDUs and prevents flooding from reaching the CPU. BPDU filtering is enabled by default on Edge ports. All BPDUs received on the Edge port are dropped. If you explicitly configure BPDU filtering on a port, that port drops all BPDUs that it receives.
- BPDU guard** Blocks the L2 bridged ports and LAG ports connected to end hosts and servers from receiving any BPDUs. When you enable BPDU guard, it places a port (bridge or LAG) in an Error_Disable or Blocking state if the port receives any BPDU frames. In a LAG, all member ports (including new members) are placed in an Blocking state. The network traffic drops but the port continues to forward BPDUs to the CPU that are later dropped. To prevent further reception of BPDUs, configure a port to shut down using the shutdown command. The port can only resume operation from the Shutdown state after manual intervention.

Root guard

Avoids bridging loops and preserves the root bridge position during network transitions. STP selects the root bridge with the lowest priority value. During network transitions, another bridge with a lower priority may attempt to become the root bridge and cause unpredictable network behavior. Configure the `spanning-tree guard root` command to avoid such an attempt and preserves the position of the root bridge. Root guard is enabled on ports that are designated ports. The root guard configuration applies to all VLANs configured on the port.

Loop guard

Prevents L2 forwarding loops caused by a hardware failure (cable failure or an interface fault). When a hardware failure occurs, a participating spanning tree link becomes unidirectional and a port stops receiving BPDUs. When a blocked port stops receiving BPDUs, it transitions to a Forwarding state causing spanning tree loops in the network. You can enable loop guard on a port that transitions to the Loop-Inconsistent state until it receives BPDUs using the `spanning-tree guard loop` command. After BPDUs are received, the port moves out of the Loop-Inconsistent (or blocking) state and transitions to an appropriate state determined by STP. Enabling loop guard on a per port basis enables it on all VLANs configured on the port. If you disable loop guard on a port, it is moved to the Listening state.

If you enable BPDU filter and BPDU guard on the same port, the BPDU filter configuration takes precedence. Root guard and loop guard are mutually exclusive. Configuring one overwrites the other from the active configuration.

- Enable spanning-tree BPDU filter in INTERFACE mode. Use the `spanning-tree bpdudfilter disable` command to disable the BPDU filter on the interface.

```
spanning-tree bpdudfilter enable
```

- Enable spanning-tree BPDU guard in INTERFACE mode.

```
spanning-tree bpduguard enable
```

- Use the `shutdown` command to shut down the port channel interface, all member ports that are disabled in the hardware.
- Use the `spanning-tree bpduguard disable` command to add a physical port to a port-channel already in the Error Disable state, the new member port is also disabled in the hardware.
- Set the guard types to avoid loops in INTERFACE mode.

```
spanning-tree guard {loop | root | none}
```

- `loop` — Set the guard type to loop.
- `none` — Set the guard type to none.
- `root` — Set the guard type to root.

BPDU filter

```
OS10(conf-if-eth1/1/4)# spanning-tree bpdudfilter enable
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is designated Blocking
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdudfilter : Enable bpdudguard : bpduguard shutdown-on-
violation :disable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 134, received 138
Interface                                     Designated
Name      PortID    Prio Cost Sts  Cost  Bridge ID          PortID
-----
ethernet1/1/4  128.272  128  500  BLK  500   32769   90b1.1cf4.a911 128.272
```

BPDU guard

```
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# spanning-tree bpduguard enable
OS10(conf-if-eth1/1/4)# exit
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is designated Blocking
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdudfilter : Enable bpdudguard : bpduguard shutdown-on-
violation :enable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 134, received 138
```

Interface Name	PortID	Prio	Cost	Sts	Cost	Bridge ID	Designated PortID
ethernet1/1/4	128.272	128	500	BLK	500	32769	90b1.1cf4.a911 128.272

Loop guard

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# spanning-tree guard loop
OS10(config-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdu filter : bpdu guard : bpduguard shutdown-on-
violation :disable RootGuard: disable LoopGuard enable
Bpdus (MRecords) sent 7, received 20
```

Interface Name	PortID	Prio	Cost	Sts	Cost	Bridge ID	Designated PortID
ethernet1/1/4	128.272	128	500	FWD	0	32769	90b1.1cf4.9d3b 128.272

Root guard

```
OS10(config-if-eth1/1/4)# spanning-tree guard root
OS10(config-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdu filter : bpdu guard : bpduguard shutdown-on-
violation :disable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 7, received 33
```

Interface Name	PortID	Prio	Cost	Sts	Cost	Bridge ID	Designated PortID
ethernet1/1/4	128.272	128	500	BLK	500	32769	90b1.1cf4.a911 128.272

RSTP commands

clear spanning-tree counters

Clears the counters for STP.

Syntax `clear spanning-tree counters [interface {ethernet node/slot/port[:subport] | port-channel number}]`

Parameters

- `interface` — Enter the interface type:
 - `ethernet node/slot/port[:subport]` — Deletes the spanning-tree counters from a physical port.
 - `port-channel number` — Deletes the spanning-tree counters for a port-channel interface (1 to 128).

Default Not configured

Command Mode EXEC

Usage Information Clear all STP counters on the device per Ethernet interface or port-channel.

Example

```
OS10# clear spanning-tree counters interface port-channel 10
```

Supported Releases 10.2.0E or later

show spanning-tree active

Displays the RSTP configuration and information for RSTP-active interfaces.

Syntax `show spanning-tree active`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show spanning-tree active

Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 90b1.1cf4.9b8a
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32768, Address 90b1.1cf4.9b8a
We are the root
Configured hello time 2, max age 20, forward delay 15
Interface                               Designated
Name      PortID  Prio Cost Sts Cost Bridge ID  PortID
-----
ethernet3/1/1 244.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.244
ethernet3/1/2 248.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.248
ethernet3/1/3 252.128 128 500 FWD 0 32768 90b1.1cf4.9b8a 128.252
ethernet3/1/4 256.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.256
Interface
Name      Role PortID  Prio Cost Sts Cost Link-type Edge
-----
ethernet3/1/1 Altr 128.244 128 500 BLK 0 AUTO No
ethernet3/1/2 Altr 128.248 128 500 BLK 0 AUTO No
ethernet3/1/3 Root 128.252 128 500 FWD 0 AUTO No
ethernet3/1/4 Altr 128.256 128 500 BLK 0 AUTO No
```

Supported Releases 10.2.0E or later

show spanning-tree interface

Displays spanning-tree interface information for Ethernet and port-channels.

Syntax `show spanning-tree interface {ethernet node/slot/port [:subport] | port-channel port-id} [detail]`

- Parameters**
- `ethernet node/slot/port[:subport]` — Displays spanning-tree information for a physical interface.
 - `port-channel port-id` — Displays spanning-tree information for a port-channel number (1 to 128).
 - `detail` — (Optional) Displays detailed information on the interface.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show spanning-tree interface ethernet 1/1/6:2 detail
Port 281 (ethernet1/1/6:2) of RSTP 1 is root Forwarding
Port path cost 2000, Port priority 128, Port Identifier 281.128
Designated root has priority 32768, address 34:17:44:55:66:7f
Designated bridge has priority 32768, address 34:17:44:55:66:7f
Designated port id is 151.128, designated path cost
```

```
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state 1
Link type is point-to-point by default, auto
PVST Simulation is enabled by default
BPDU sent 3, received 7
```

Supported Releases 10.2.0E or later

spanning-tree bpdudfilter

Enables or disables BPDU filtering on an interface.

Syntax `spanning-tree bpdudfilter {enable | disable}`

Parameters

- `enable` — Enables the BPDU filtering on an interface.
- `disable` — Disables the BPDU filtering on an interface.

Default Disabled

Command Mode INTERFACE

Usage Information Use the `enable` parameter to enable BPDU filtering.

Example

```
OS10(conf-if-eth1/1/4)# spanning-tree bpdudfilter enable
```

Supported Releases 10.2.0E or later

spanning-tree bpduguard

Enables or disables BPDU guard on an interface.

Syntax `spanning-tree bpduguard {enable | disable}`

Parameters

- `enable` — Enables the BPDU guard filter on an interface.
- `disable` — Disables the BPDU guard filter on an interface.

Default Disabled

Command Mode INTERFACE

Usage Information BPDU guard prevents a port from receiving BPDUs. If the port receives a BPDU, it is placed in the Error-Disabled state as a protective measure.

Example

```
OS10(conf-if-eth1/1/4)# spanning-tree bpduguard enable
```

Supported Releases 10.2.0E or later

spanning-tree disable

Disables the spanning-tree mode configured with the `spanning-tree mode` command globally on the switch or on specified interfaces.

Syntax `spanning-tree disable`

Parameters None

Default Not configured.

Usage Information The `no` version of this command re-enables STP and applies the currently configured spanning-tree settings.

Command Mode CONFIGURATION
INTERFACE

Example

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# spanning-tree disable
```

Supported Releases 10.3.0E or later

spanning-tree guard

Enables or disables loop guard or root guard on an interface.

Syntax `spanning-tree guard {loop | root | none}`

- Parameters**
- `loop` — Enables loop guard on an interface.
 - `root` — Enables root guard on an interface.
 - `none` — Sets the guard mode to none.

Default Not configured

Usage Information Root guard and loop guard configurations are mutually exclusive. Configuring one overwrites the other from the active configuration.

Command Mode INTERFACE

Example

```
OS10(config-if-eth1/1/4)# spanning-tree guard root
```

Supported Releases 10.2.0E or later

spanning-tree mode

Enables an STP type (RSTP, Rapid-PVST+, or MST).

Syntax `spanning-tree mode {rstp | mst | rapid-pvst}`

- Parameters**
- `rstp` — Sets the STP mode to RSTP.
 - `mst` — Sets the STP mode to MST.
 - `rapid-pvst` — Sets the STP mode to RPVST+.

Default RPVST+

Command Mode CONFIGURATION

Usage Information All STP instances are stopped in the previous STP mode, and are restarted in the new mode. You can also change to RSTP/MST mode.

Example (RSTP)

```
OS10(config)# spanning-tree mode rstp
```

Example (MST)

```
OS10(config)# spanning-tree mode mst
```

Supported Releases 10.2.0E or later

spanning-tree port

Sets the port type as the EdgePort.

Syntax	<code>spanning-tree port type edge</code>
Parameters	None
Default	Not configured
Command Mode	INTERFACE
Usage Information	When you configure an EdgePort on a device running STP, the port immediately transitions to Forwarding state. Only configured ports connected to end hosts act as EdgePorts.
Example	<pre>OS10(config)# spanning-tree port type edge</pre>
Supported Releases	10.2.0E or later

spanning-tree rstp force-version

Configures a forced version of spanning tree to transmit BPDUs.

Syntax	<code>spanning-tree rstp force-version stp</code>
Parameters	<code>stp</code> — Force the version for the BPDUs transmitted by RSTP.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	Forces a bridge that supports RSTP or MST to operate in a STP-compatible manner to avoid frame misordering and duplication in known LAN protocols that are sensitive.
Example	<pre>OS10(config)# spanning-tree rstp force-version stp</pre>
Supported Releases	10.2.0E or later

spanning-tree rstp forward-time

Configures a time interval for the interface to wait in the Blocking state or the Learning state before moving to the Forwarding state.

Syntax	<code>spanning-tree rstp forward-time seconds</code>
Parameters	<code>seconds</code> — Enter the number of seconds an interface waits in the Blocking or Learning States before moving to the Forwarding state (4 to 30).
Default	15 seconds
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(config)# spanning-tree rstp forward-time 16</pre>
Supported Releases	10.2.0E or later

spanning-tree rstp hello-time

Sets the time interval between generation and transmission of RSTP BPDUs.

Syntax	<code>spanning-tree rstp hello-time <i>seconds</i></code>
Parameters	<i>seconds</i> — Enter a hello-time interval value in seconds (1 to 10).
Default	2 seconds
Command Mode	CONFIGURATION
Usage Information	Dell EMC recommends increasing the hello-time for large configurations (especially configurations with multiple ports).
Example	<pre>OS10(config)# spanning-tree rstp hello-time 5</pre>
Supported Releases	10.2.0E or later

spanning-tree rstp mac-flush-threshold

Sets the threshold value to flush MAC addresses on RSTP instance.

Syntax	<code>spanning-tree rstp mac-flush-threshold <i>threshold-value</i></code>
Parameters	<i>threshold-value</i> —Enter the threshold value for the number of flushes, ranging from 0 to 65535. The default value is 0.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The no version of this command removes the threshold value.
Example	<pre>OS10(config)# spanning-tree rstp mac-flush-threshold 255</pre>
Supported Releases	10.4.0E(R1) or later

spanning-tree rstp max-age

Configures the time period the bridge maintains configuration information before refreshing the information by recomputing the RSTP topology.

Syntax	<code>max-age <i>seconds</i></code>
Parameters	<i>seconds</i> — Enter a maximum age value in seconds (6 to 40).
Default	20 seconds
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(config)# spanning-tree rstp max-age 10</pre>
Supported Releases	10.2.0E or later

spanning-tree rstp

Sets the priority value for RSTP.

Syntax	<code>spanning-tree rstp priority <i>priority value</i></code>
Parameters	<code>priority <i>priority value</i></code> — Enter a bridge-priority value in increments of 4096 (0 to 61440). Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	RSTP determines the root bridge but you can assign one bridge a lower priority to increase the probability it being the root bridge. A lower <i>priority value</i> increases the probability of the bridge becoming a root bridge.
Example	<pre>OS10(config)# spanning-tree rstp priority 200</pre>
Supported Releases	10.2.0E or later

Virtual LANs

VLANs segment a single flat L2 broadcast domain into multiple logical L2 networks. Each VLAN is uniquely identified by a VLAN ID or tag consisting of 12 bits in the Ethernet frame. VLAN IDs range from 1 to 4093 and can provide a total of 4093 logical networks.

You can assign ports on a single physical device to one or more VLANs creating multiple logical instances on a single physical device. The virtual logical switches spanning across different physical devices emulate multiple logically segmented L2 networks on a single physical network.

Each VLAN has its own broadcast domain and the unicast, multicast, and broadcast network traffic from ports that belong to a VLAN is forwarded or flooded to ports in the same VLAN only. Traffic between VLANs must be routed from one VLAN to another. You can also assign each VLAN an IP address to group all the ports within a single IP subnet.

Segment a L2 network using VLANs to:

- Minimize broadcast and multicast traffic in the L2 network
- Increase security by isolating ports into different VLANs
- Ease network management

Default VLAN

All interface ports are administratively up (in L2 mode) and are automatically placed in the default VLAN as untagged interfaces.

When you assign a port to a non-default VLAN in Trunk mode, the interface remains an untagged member of the default VLAN and a tagged member of the new VLAN. When you assign a port to a non-default VLAN in Access mode, it removes from the default VLAN and is assigned to the new VLAN as an untagged member of the new VLAN.

- VLAN 1 is the default VLAN.
- You cannot delete the default VLAN. However, you can change the default VLAN ID number using the `default vlan-id` command.

Use the `show vlan` command to verify that the interface is part of the default VLAN (VLAN 1).

Default VLAN configuration

```
OS10# show vlan

Codes: * - Default VLAN, G-GVRP VLANs, R-Remote Port Mirroring VLANs, P-Primary, C-Community, I-Isolated
Q: A-Access (Untagged), T-Tagged
  x-Dot1x untagged, X-Dot1x tagged
  G-GVRP tagged, M-Vlan-stack, H-VSN tagged
```

```

i-Internal untagged, I-Internal tagged, v-VLT untagged, V-VLT tagged
NUM      Status      Description      Q Ports
* 1      up              A Eth1/1/1-1/1/54

```

Create or remove VLANs

You can create VLANs and add physical interfaces or port-channel (LAG) interfaces to the VLAN as tagged or untagged members. You can add an Ethernet interface as a trunk port or as an access port, but it cannot be added as both at the same time.

Multiple non-default vlans with physical and port channel ports in access and trunk modes

```

OS10# show vlan

Codes: * - Default VLAN, G-GVRP VLANs, R-Remote Port Mirroring VLANs, P-Primary, C-
Community, I-Isolated
Q: A-Access (Untagged), T-Tagged
   x-Dot1x untagged, X-Dot1x tagged
   G-GVRP tagged, M-Vlan-stack, H-VSN tagged
   i-Internal untagged, I-Internal tagged, v-VLT untagged, V-VLT tagged
NUM      Status      Description      Q Ports
* 1      up              A Eth1/1/2 1/1/3:2 1/1/3:3 1/1/3:4
1/1/4
1/1/5 1/1/6 1/1/7 1/1/8 1/1/9 1/1/10 1/1/11 1/1/12 1/1/13 1/1/14 1/1/15 1/1/16 1/1/17
1/1/18
1/1/19 1/1/20 1/1/21 1/1/22 1/1/23 1/1/24 1/1/25:1 1/1/25:2 1/1/25:3 1/1/25:4 1/1/26
1/1/27
1/1/28 1/1/30 1/1/32
                                A Po40
                                T Eth1/1/3:2
                                T Po40
                                A Eth1/1/31
                                T Eth1/1/25:4 1/1/32
                                T Po40
                                A Eth1/1/3:1
49 1/1/50 1/1/51 1/1/52 1/1/53 1/1/54

```

The shutdown command stops L3 (routed) traffic only. L2 traffic continues to pass through the VLAN. If the VLAN is not a routed VLAN configured with an IP address, the shutdown command has no effect on VLAN traffic.

When you delete a VLAN (no interface vlan *vlan-id* command), any interfaces assigned to that VLAN are assigned to the default VLAN as untagged interfaces.

Configure a port-based VLAN, enter INTERFACE-VLAN mode for VLAN related configuration tasks and create a VLAN. Assign interfaces in L2 mode to the VLAN to enable it.

1. Create a VLAN and enter the VLAN number in INTERFACE mode (1 to 4093).

```
interface vlan vlan-id
```

2. Delete a VLAN in CONFIGURATION mode.

```
no interface vlan vlan-id
```

Create VLAN

```
OS10(config)# interface vlan 108
```

Delete VLAN

```
OS10(config)# no interface vlan 108
```

View configured VLANs

```
OS10(config)# do show interface vlan
```

```
Vlan 1 is up, line protocol is up
Address is , Current address is
```

```
Interface index is 69208865
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:
```

```
Vlan 200 is up, line protocol is up
Address is , Current address is
Interface index is 69209064
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:
```

```
Vlan 320 is up, line protocol is up
Address is , Current address is
Interface index is 69209184
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:
```

Access mode

An access port is an untagged member of only one VLAN. Configure a port in Access mode and configure which VLAN carries the traffic for that interface. If you do not configure the VLAN for a port in Access mode (or an access port), the interface carries traffic for VLAN 1 (default VLAN).

Change the access port membership in a VLAN by specifying the new VLAN. You must create the VLAN before you can assign the port in Access mode to that VLAN. Use the `no switchport access vlan` command to reset to default VLAN.

1. Configure a port in INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
```

2. Set the interface to Switchport mode as access in INTERFACE mode.

```
switchport mode access
```

3. Enter the VLAN number for the untagged port in INTERFACE mode.

```
switchport access vlan vlan-id
```

Configure port in access mode

```
OS10(config)# interface ethernet 1/1/9
OS10(config-if-eth1/1/9)# switchport mode access
OS10(config-if-eth1/1/9)# switchport access vlan 604
```

Show running configuration

```
OS10# show running-configuration
...
!
interface ethernet1/1/5
...
switchport access vlan 604
no shutdown
```

```
!  
interface vlan1  
  no shutdown  
  ...
```

Trunk mode

A trunk port can be a member of multiple VLANs set up on an interface. A trunk port can transmit traffic for all VLANs. To transmit traffic on a trunk port with multiple VLANs, OS10 uses tagging or the 802.1q encapsulation method.

1. Configure a port in INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
```

2. Change the Switchport mode to Trunk mode in INTERFACE mode.

```
switchport mode trunk
```

3. Enter the allowed VLANs on the trunk port in INTERFACE mode.

```
switchport trunk allowed vlan vlan-id
```

Configure port in trunk mode

```
OS10(config)# interface ethernet 1/1/6  
OS10(conf-if-eth1/1/6)# switchport mode trunk  
OS10(conf-if-eth1/1/6)# switchport trunk allowed vlan 108
```

View running configuration

```
OS10# show running-configuration  
...  
!  
interface ethernet1/1/8  
  switchport mode trunk  
  switchport trunk allowed vlan 108  
  no shutdown  
!  
interface vlan1  
  no shutdown  
!  
...
```

Assign IP address

You can assign an IP address to each VLAN to make it a L3 VLAN — the ports in that VLAN belong to that particular IP subnet.

The traffic between the ports in different VLANs route using the IP address. Configure the L3 VLAN interface to remain administratively UP or DOWN using the `shutdown` and `no shutdown` commands. This provisioning only affects the L3 traffic across the members of a VLAN and does not affect the L2 traffic.

You cannot assign an IP address to the default VLAN (VLAN 1). You can place VLANs and other logical interfaces in L3 mode to receive and send routed traffic.

1. Create a VLAN in CONFIGURATION mode (1 to 4093).

```
interface vlan vlan-id
```

2. Assign an IP address and mask to the VLAN in INTERFACE-VLAN mode.

```
ip address ip-address/prefix-length [secondary]
```

- *ip-address/prefix-length* — Enter the IP address in dotted-decimal format (A.B.C.D/x).
- *secondary* — Enter the interface backup IP address.

Assign IP address to VLAN

```
OS10(config)# interface vlan 200
OS10(conf-if-vl-200)# ip address 10.1.15.1/8
```

View VLAN configuration

```
OS10(conf-if-vl-200)# do show interface vlan

Vlan 1 is up, line protocol is up
Address is , Current address is
Interface index is 69208865
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

Vlan 200 is up, line protocol is up
Address is , Current address is
Interface index is 69209064
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

Vlan 320 is up, line protocol is up
Address is , Current address is
Interface index is 69209184
Internet address is 20.2.11.1/24
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:
```

View VLAN configuration

You can view configuration information related to VLANs using `show` commands.

- View the VLAN status and configuration information in EXEC mode.

```
show vlan
```

- View the VLAN interface configuration in EXEC mode.

```
show interfaces vlan
```

- View the VLAN interface configuration for a specific VLAN ID in EXEC mode.

```
show interfaces vlan vlan-id
```

View VLAN configuration

```
OS10# show vlan

Codes: * - Default VLAN, G-GVRP VLANs, R-Remote Port Mirroring VLANs, P-Primary, C-
Community, I-Isolated
Q: A-Access (Untagged), T-Tagged
x-Dot1x untagged, X-Dot1x tagged
G-GVRP tagged, M-Vlan-stack, H-VSN tagged
```


i-Internal untagged, I-Internal tagged, v-VLT untagged, V-VLT tagged				
NUM	Status	Description	Q Ports	
* 1	up		A Eth1/1/1-1/1/32	
			A Po40	
200	up		T Eth1/1/3:2	
			T Po40	
			A Eth1/1/31	
320	up		T Eth1/1/25:4 1/1/32	
			T Po40	
			A Eth1/1/3:1	

View interface VLAN configuration

```
OS10# show interface vlan
Vlan 1 is up, line protocol is up
Address is , Current address is
Interface index is 69208865
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queuing strategy: fifo Time since last
interface status change:

Vlan 200 is up, line protocol is up
Address is , Current address is
Interface index is 69209064
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queuing strategy: fifo Time since last
interface status change:

Vlan 320 is up, line protocol is up
Address is , Current address is
Interface index is 69209184
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queuing strategy: fifo Time since last
interface status change:
```

View interface configuration for specific VLAN

```
OS10# show interface vlan 320
Vlan 320 is up, line protocol is up
Address is , Current address is
Interface index is 69209184
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queuing strategy: fifo Time since last
interface status change:
```

VLAN commands

description (VLAN)

Adds a description to the selected VLAN.

Syntax `description description`

Parameters	<i>description</i> — Enter a text string to identify the VLAN (up to 80 characters).
Default	Not configured
Command Mode	INTERFACE-VLAN
Usage Information	None
Example	<pre>OS10(conf-if-vlan)# description vlan3</pre>
Supported Releases	10.2.0E or later

interface vlan

Creates a VLAN interface.

Syntax	<code>interface vlan <i>vlan-id</i></code>
Parameters	<i>vlan-id</i> — Enter the VLAN ID number (1 to 4093).
Default	VLAN 1
Command Mode	CONFIGURATION
Usage Information	FTP, TFTP, MAC ACLs, and SNMP operations are not supported — IP ACLs are supported on VLANs only. The <code>no</code> version of this command deletes the interface.
Example	<pre>OS10(config)# interface vlan 10 OS10(conf-if-vl-10)#</pre>
Supported Releases	10.2.0E or later

show vlan

Displays VLAN configurations.

Syntax	<code>show vlan <i>vlan-id</i></code>
Parameters	<i>vlan-id</i> — (Optional) Enter a VLAN ID number (1 to 4093).
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to view VLAN configuration information for a specific VLAN ID.
Example	<pre>OS10(config)# do show vlan Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs Q: A - Access (Untagged), T - Tagged NUM Status Description Q Ports * 1 Active * A Eth1/1/15 A Po100 2101 Active * T Eth1/1/1,1/1/3 T Po100 2102 Active * T Eth1/1/1,1/1/3</pre>
Supported Releases	10.2.0E or later

Port monitoring

Port monitoring enables monitoring of ingress or egress traffic of one port to another for analysis. A monitoring port (MG) or destination port, is the port where the monitored traffic is sent for analysis. A monitored port (MD) is the source interface which is monitored for traffic analysis, also called source port.

Depending on the location of the destination interface, port monitoring is performed as follows:

- **Local port monitoring** — The port monitoring is performed in the same switch. The switch forwards a copy of incoming and outgoing traffic from one port to another port for further analysis.
- **Remote port monitoring (RPM)** — The port monitoring is performed on traffic running across a remote device in the same network. The monitored traffic is carried over the L2 network.
- **Encapsulated remote port monitoring (ERPM)** — The port monitoring is performed on an L3 network. The traffic from the source port is encapsulated and forwarded to the destination port in another switch.

Local port monitoring

The local port monitoring monitors traffic from one or more ports from the switch to one or more ports on the same switch. For local port monitoring, the monitored source and monitoring destination ports are on the same device.

Configure local monitoring session

1. Verify that the intended monitoring port has no configuration other than `no shutdown` and `no switchport`.

```
show running-configuration
```

2. Create a monitoring session in CONFIGURATION mode.

```
monitor session session-id [local]
```

3. Enter the source and direction of monitored traffic in MONITOR-SESSION mode.

```
source interface interface-type {both | rx | tx}
```

4. Enter the destination of traffic in MONITOR-SESSION mode.

```
destination interface interface-type
```

Create monitoring session

```
OS10(config)# monitor session 1  
OS10(conf-mon-local-1)#
```

Configure source and destination port, and traffic direction

```
OS10(conf-mon-local-1)# source interface ethernet 1/1/7-1/1/8 rx  
OS10(conf-mon-local-1)# destination interface ethernet1/1/1  
OS10(conf-mon-local-1)# no shut
```

View configured monitoring sessions

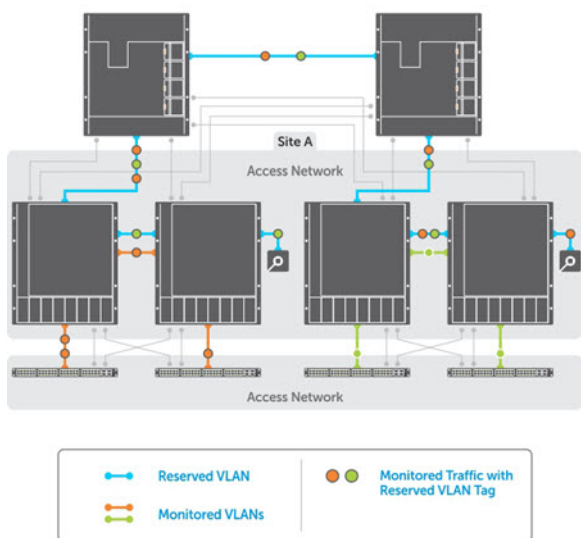
In the State field, `true` indicates that the port is enabled. In the Reason field, `Is UP` indicates that hardware resources are allocated.

```
OS10# show monitor session all  
S.Id Source Destination Dir SrcIP DstIP DSCP TTL State Reason  
-----  
1 ethernet1/1/7 ethernet1/1/1 rx N/A N/A N/A N/A true Is UP
```

Remote port monitoring

Remote port monitoring allows you to monitor ingress and/or egress traffic on multiple source ports of multiple devices and forward the monitored traffic to multiple destination ports on different remote devices. Remote port monitoring helps network administrators monitor and analyze traffic to troubleshoot network problems in a time-saving and efficient way.

In a remote port monitoring session, monitored traffic is tagged with a VLAN ID and switched on a user-defined, non-routable L2 VLAN. The VLAN is reserved in the network to carry only monitored traffic, which is forwarded on all egress ports of the VLAN. You must configure each intermediate switch that participates in the transport of monitored traffic with the reserved L2 VLAN. Remote port monitoring supports monitoring sessions in which multiple source and destination ports distribute across multiple network devices.



Session and VLAN requirements

Remote port monitoring requires a source session (monitored ports on different source devices), a reserved tagged VLAN for transporting monitored traffic (configured on source, intermediate, and destination devices), and a destination session (destination ports connected to analyzers on destination devices).

- Configure any network device with source ports and destination ports and enable it to function in an intermediate transport session for a reserved VLAN at the same time for multiple remote port monitoring sessions. Enable and disable individual monitoring sessions.
- A remote port monitoring session mirrors monitored traffic by prefixing the reserved VLAN tag to monitored packets to transmit using the reserved VLAN.
- The source address, destination address, and original VLAN ID of the mirrored packet are prefixed with the tagged VLAN header. Untagged source packets are tagged with the reserved VLAN ID.
- The member port of the reserved VLAN must have the MTU and IPMTU value as MAX+4 (to hold the VLAN tag parameter).
- To associate with source session, the reserved VLAN can have a maximum of four member ports.
- To associate with destination session, the reserved VLAN can have multiple member ports.
- The reserved VLAN cannot have untagged ports.

Reserved L2 VLAN

- MAC address learning in the reserved VLAN is automatically disabled.
- There is no restriction on the VLAN IDs used for the reserved remote monitoring VLAN. Valid VLAN IDs are from 2 to 4093. The default VLAN ID is not supported.
- In monitored traffic, packets that have the same destination MAC address as an intermediate or destination device in the path used by the reserved VLAN to transport the mirrored traffic are dropped by the device that receives the traffic if the device has a L3 VLAN configured.

Source session

- Configure physical ports and port-channels as sources in remote port monitoring and use them in the same source session. You can use both L2 (configured with the `switchport` command) and L3 ports as source ports. Optionally configure one or more source VLANs to configure the VLAN traffic to be monitored on source ports.
- Use the default VLAN and native VLANs as a source VLAN.
- You cannot configure the dedicated VLAN used to transport mirrored traffic as a source VLAN.

Restrictions

- When you use a source VLAN, enable flow-based monitoring (`flow-based enable`).
- In a source VLAN, only received (`rx`) traffic is monitored.
- In S5148F-ON, only received (`rx`) traffic is monitored.
- You cannot configure a source port-channel or source VLAN in a source session if the port-channel or VLAN has a member port configured as a destination port in a remote port monitoring session.
- You cannot use a destination port for remote port monitoring as a source port, including the session the port functions as the destination port.
- The reserved VLAN used to transport mirrored traffic must be a L2 VLAN — L3 VLANs are not supported.

Configure remote port monitoring

Remote port monitoring requires a source interface (monitored ports on different source network devices) and a reserved tagged VLAN for transporting mirrored traffic (configured on the source, intermediate, and destination devices).

1. Create a remote monitoring session in CONFIGURATION mode.

```
monitor session session-id type rpm-source
```

2. Enter the source to monitor traffic in MONITOR-SESSION mode.

```
source interface interface-range direction
```

3. Enter the destination to send the traffic to in MONITOR-SESSION mode.

```
destination remote-vlan vlan-id
```

4. Enable the monitoring interface in MONITOR-SESSION mode.

```
no shut
```

Create remote monitoring session

```
OS10(config)# monitor session 10 type rpm-source
OS10(conf-mon-rpm-source-10)#
```

Configure source and destination port, and traffic direction

```
OS10(conf-mon-rpm-source-10)# source interface vlan 10 rx
OS10(conf-mon-rpm-source-10)# destination remote-vlan 100
OS10(conf-mon-rpm-source-10)# no shut
```

View monitoring session

```
OS10(conf-mon-rpm-source-10)# do show monitor session all
S.Id  Source  Destination  Dir  SrcIP  DstIP  DSCP  TTL  State  Reason
-----
1     vlan10  vlan 100    rx   N/A    N/A    N/A   N/A  true   Is UP
```

Encapsulated remote port monitoring

The monitored traffic can also be transmitted over an L3 network to a remote analyzer. The encapsulated remote port monitoring (ERPM) session mirrors traffic from the source ports/lags or source VLANs and forwards the traffic using routable GRE-encapsulated packets to the destination IP address specified in the session.

Consider the following points while configuring an ERPM session:

- OS10 supports only the ERPM source session. The encapsulated packets terminate at the destination IP address, the remote analyzer.
- The source IP address must be a valid local IP address for the session to be up.
- The destination IP address must be on a remote L3 node that supports standard GRE decapsulation.
- If the destination IP address is not reachable, the session goes down.
- OS10 does not support ERPM destination session and decapsulation of ERPM packets at the destination switch.
- You can configure a maximum of 4 ERPM sessions with a maximum of 128 source ports in each session. You can configure these 4 ERPM sessions in one of the following methods:
 - Single directional with either 4 ingress or 4 egress sessions.
 - Bidirectional with 2 ingress and 2 egress sessions.
- You can monitor a source VLAN only through flow-based monitoring. Only ingress is supported in a flow-based source VLAN monitoring.
- You cannot configure an interface with ERPM traffic as a source for an ERPM session.
- You cannot monitor an RPM VLAN as a source.
- You cannot configure the same destination IP address for two sessions.
- You cannot configure an interface that serves as egress for GRE tunnel as a source interface.
- ERPM supports only GRE over IPv4 tunneling.
- ERPM does not support ECMP.
- You can use third party devices as only tunnel-transit devices.
- OS10 does not support monitoring VLAN sub-interfaces and CPU generated packets.

Configure encapsulated remote port monitoring

Encapsulated remote port monitoring requires valid source and destination IP addresses. Ensure that the source IP address is local and destination IP address is remote. You can also configure the TTL and DSCP values.

Create monitoring session

```
OS10(config)# monitor session 10 type erpm-source
S10(conf-mon-erpm-source-10)#
```

Configure source port, source and destination IP addresses, and protocol type

```
OS10(conf-mon-erpm-source-10)# source interface ethernet 1/1/2
OS10(conf-mon-erpm-source-10)# source-ip 1.1.1.1 destination-ip 3.3.3.3 gre-protocol
35006
OS10(conf-mon-erpm-source-10)# ip ttl 16
OS10(conf-mon-erpm-source-10)# ip dscp 63
OS10(conf-mon-erpm-source-10)# no shut
```

View configured ERPM session

```
OS10(conf-mon-erpm-source-6)# do show monitor session all
```

S.Id	Source	Destination	Dir	Mode	Source IP	Dest IP	DSCP
TTL	Gre-Protocol	State	Reason				
6	ethernet1/1/2	remote-ip	both	port	1.1.1.1	3.3.3.3	63
16	35006	true	Is UP				

View running configuration of monitor session

```
OS10# show running-configuration monitor
!
monitor session 10 type erpm-source
```

```
source-ip 1.1.1.1 destination-ip 3.3.3.3
source interface ethernet1/1/2
no shut
```

Flow-based monitoring

Flow-based monitoring conserves bandwidth by inspecting only specified traffic instead of all interface traffic. Using flow-based monitoring, you can monitor only traffic received by the source port that matches criteria in ingress access-lists.

1. Enable flow-based monitoring for a monitoring session in MONITOR-SESSION mode.

```
flow-based enable
```

2. Return to CONFIGURATION mode.

```
exit
```

3. Create an access list in CONFIGURATION mode.

```
ip access-list access-list-name
```

4. Define access-list rules using `seq`, `permit`, and `deny` statements in CONFIG-ACL mode. The ACL rules describe the traffic you want to monitor. Flow monitoring is supported for IPv4 ACLs, IPv6 ACLs, and MAC ACLs.

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count
[byte]] [fragments] [threshold-in-msgs count] [capture session session-id]
```

5. Return to CONFIGURATION mode.

```
exit
```

6. Apply the flow-based monitoring ACL to the monitored source port in CONFIGURATION mode (up to 140 characters).

```
ip access-group access-list-name {in | out}
```

Enable flow-based monitoring

```
OS10(config)# monitor session 1
OS10(conf-mon-local-1)# flow-based enable
OS10(conf-mon-local-1)# exit
OS10(config)# ip access-list ipacl1
OS10(conf-ipv4-acl)# deny ip host 1.1.1.23 any capture session 1 count
OS10(conf-ipv4-acl)# exit
OS10(config)# mac access-list mac1
OS10(conf-mac-acl)# deny any any capture session 1
OS10(conf-mac-acl)# exit
OS10(config)# interface ethernet 1/1/9
OS10(conf-if-eth1/1/9)# mac access-group mac1 in
OS10(conf-if-eth1/1/9)# end
OS10# show mac access-lists in
Ingress MAC access-list mac1
Active on interfaces :
  ethernet1/1/9
seq 10 deny any any capture session 1 count (0 packets)
```

Remote port monitoring on VLT

In a network, devices configured with peer VLT nodes are considered as a single device. You can apply remote port monitoring (RPM) on the VLT devices in a network.

In a failover case, the monitored traffic reaches the packet analyzer connected to the TOR through the VLT interconnect link.

NOTE:

- In VLT devices configured with RPM, when the VLT link is down, the monitored packets might drop for some time. The time is equivalent to the VLT failover recovery time (delay restore).

- ERPM does not work on VLT devices.

RPM on VLT scenarios

Consider a simple VLT setup where two VLT devices are connected using VLTi and a top-of-rack (TOR) switch is connected to both the VLT peers using VLT LAGs in a ring topology. In this setup, the following table describes the possible scenarios when RPM is used to mirror traffic.

NOTE: The ports that are connected to the VLT domain, but not part of the VLT-LAG, are called orphan ports.

Table 2. RPM on VLT scenarios

Scenario	Recommendation
<p>Mirror an orphan port or VLT LAG or VLTi member port to VLT LAG. The packet analyzer is connected to the TOR switch.</p>	<p>The following is an example of recommended configuration on the peer VLT device:</p> <ol style="list-style-type: none"> 1. Create RPM VLAN <pre data-bbox="842 667 1493 808">! interface vlan 100 no shutdown remote-span !</pre> 2. Create an L2 ACL for the RPM VLAN - RPM session and attach it to VLTi LAG interface. <pre data-bbox="842 898 1493 1189">! mac access-list rpm seq 10 permit any any capture session 10 vlan 100 ! interface ethernet 1/1/1 no shutdown switchport access vlan 1 mac access-group rpm in !</pre> 3. Create a flow based RPM session on the peer VLT device to monitor the VLTi LAG interface as source. <pre data-bbox="842 1279 1493 1473">! monitor session 10 type rpm-source destination remote-vlan 100 flow-based enable source interface ethernet1/1/1 (ICL lag member) !</pre>
<p>Mirror a VLAN with VLTi LAG as member to any orphan port on the same VLT device. The packet analyzer is connected to the local VLT device through the orphan port.</p>	<p>The following is an example of recommended configuration on the VLT device:</p> <ol style="list-style-type: none"> 1. Create an L2 ACL for the local session and attach it to the VLTi LAG interface. <pre data-bbox="842 1659 1493 1951">! mac access-list local seq 10 permit any any capture session 10 ! interface ethernet 1/1/1 no shutdown switchport access vlan 1 mac access-group local in !</pre>

Table 2. RPM on VLT scenarios (continued)

Scenario	Recommendation
	<p>2. Create a flow based local session on the VLT device to monitor VLTi LAG interface member (ethernet 1/1/1) as source.</p> <pre> ! monitor session 10 type destination interface ethernet 1/1/10 flow-based enable source interface ethernet1/1/1 no shut ! </pre>
Mirror a VLAN with VLTi LAG as member to VLT LAG on the same VLT device. The packet analyzer is connected to the TOR switch.	—
Mirror VLT LAG of TOR, or any port in the TOR to any orphan port in the VLT device. Configure VLT nodes as intermediate device. The packet analyzer is connected to the TOR switch.	—
Mirror VLT LAG to any orphan port on the same VLT device. The packet analyzer is connected to the local VLT device through the orphan port.	If the packet analyzer is directly connected to the VLT peer in which the source session is configured, use local port monitoring instead of RPM.
Mirror an orphan port in primary VLT device to any orphan port on secondary VLT device through VLTi. The packet analyzer is connected to the secondary VLT device through the orphan port. In this case, the mirroring packets are duplicated.	—
Mirror VLT LAG of the primary VLT device to any orphan port on secondary VLT device through VLTi. The packet analyzer is connected to the secondary VLT device through the orphan port.	—
Mirror a member port of VLTi LAG or VLT LAG to any orphan port in the same device. The packet analyzer is connected to the local VLT device through the orphan port.	If the packet analyzer is directly connected to the VLT peer in which the source session is configured, use local port monitoring instead of RPM.
Mirror a member port of VLTi LAG to VLT LAG on the same VLT device. The packet analyzer is connected to the TOR switch.	—
Mirror VLT LAG or VLT member port as part of source VLAN and destination VLAN. The packet analyzer is connected to the TOR switch.	—

Port monitoring commands

description (Port Monitoring)

Configures a description for the port monitoring session. The monitoring session can be one of the following: local, RPM, or ERPM.

- Syntax** `description string`
- Parameters** `string` — Enter a description of the monitoring session (up to 255 characters).
- Default** Not configured
- Command Mode** MONITOR-SESSION

Usage Information The no version of this command removes the description text.

Example

```
OS10(conf-mon-local-1)# description remote
```

```
OS10(conf-mon-rpm-source-5)# description "RPM Sesssion"
```

```
OS10(conf-mon-erpm-source-10)# description "ERPM Session"
```

Supported Releases 10.2.0E or later

destination (Port Monitoring)

Sets the destination where monitored traffic is sent to. The monitoring session can be local or RPM.

Syntax destination {interface *interface-type* | remote-vlan *vlan-id*}

Parameters

interface-type — Enter the interface type for a local monitoring session.

- ethernet *node/slot/port[:subport]* — Enter the Ethernet interface information as the destination.
- port-channel *id-number* — Enter a port-channel number as the destination (1 to 128).
- vlan *vlan-id* — Enter a VLAN ID as the destination (1 to 4093).

remote-vlan vlan-id—Enter a remote VLAN ID as the destination for RPM monitoring session (1 to 4093).

Default Not configured

Command Mode MONITOR-SESSION

Usage Information The no version of this command resets the value to the default.

Example

```
OS10(conf-mon-local-10)# destination interface port-channel 10
```

```
OS10(conf-mon-rpm-source-3)# destination remote-vlan 20
```

Supported Releases 10.2.0E or later

flow-based

Enables flow-based monitoring. The monitoring session can be one of the following: local, RPM, or ERPM.

Syntax flow-based enable

Parameters None

Default Disabled

Command Mode MONITOR-SESSION

Usage Information The no version of this command disables the flow-based monitoring.

Example

```
OS10(conf-mon-local-1)# flow-based enable
```

```
OS10(conf-mon-rpm-source-2)# flow-based enable
```

```
OS10(conf-mon-erpm-source-3)# flow-based enable
```

Supported Releases 10.2.0E or later

ip

Configures the IP time to live (TTL) value and the differentiated services code point (DSCP) value for the ERPM traffic.

Syntax `ip {ttl t11-number | dscp dscp-number}`

Parameters

- *t11-number* — Enter the TTL value (1 to 255)
- *dscp-number* — Enter the DSCP value (0 to 63).

Default

- TTL: 255
- DSCP: 0

Command Mode MONITOR-SESSION (ERPM)

Usage Information The no version of this command removes the TTL and the DSCP values configured.

Example

```
OS10(conf-mon-erpm-source-10)# ip ttl 16
OS10(conf-mon-erpm-source-10)# ip DSCP 63
```

Supported Releases 10.4.0E(R1) or later

monitor session

Creates a session for monitoring traffic with port monitoring.

Syntax `monitor session session-id type [local | rpm-source | erpm-source]`

Parameters

- *session-id* — Enter a monitor session ID (1 to 18).
- *local* — (Optional) Enter a local monitoring session.
- *rpm-source* — (Optional) Enter a remote monitoring session.
- *erpm-source* — (Optional) Enter an encapsulated remote monitoring session.

Default local

Command Mode CONFIGURATION

Usage Information The no version of this command removes the monitor session.

Example

```
OS10(config)# monitor session 1
OS10(conf-mon-local-1)#
```

Example (RPM)

```
OS10(config)# monitor session 5 type rpm-source
OS10(conf-mon-rpm-source-5)#
```

Example (ERPM)

```
OS10(config)# monitor session 10 type erpm-source
OS10(conf-mon-erpm-source-10)#
```

Supported Releases 10.2.0E or later

show monitor session

Displays information about a monitoring session.

Syntax `show monitor session {session-id | all}`

- Parameters**
- `session-id` — Enter the session ID number (1 to 18).
 - `all` — View all monitoring sessions.

Default All

Command Mode EXEC

Usage Information In the State field, `true` indicates that the port is enabled. In the Reason field, `Is UP` indicates that hardware resour

Example (specific session)

```
OS10# show monitor session 1
S.Id  Source          Destination      Dir  Mode  Source IP      Dest IP
-----
1     ethernet1/1/1    remote-ip       both port 11.11.11.1    11.11.11.11
```

Example (all sessions)

```
OS10# show monitor session all
S.Id  Source          Destination      Dir  Mode  Source IP      Dest IP
-----
1     ethernet1/1/1    remote-ip       both port 11.11.11.1    11.11.11.11
9     ethernet1/1/9
7     ethernet1/1/9    vlan40         both port N/A           N/A
4     ethernet1/1/1
Destination is not resolved
6     ethernet1/1/2    remote-ip       both port 11.11.11.1    2.2.2.1
session does not exist
```

Supported Releases 10.2.0E or later

shut

Disables the monitoring session. The monitoring session can be one of the following: local, RPM, or ERPM.

Syntax `shut`

Parameters None

Default Disabled

Command Mode MONITOR-SESSION

Usage Information The `no` version of this command enables the monitoring session.

Example

```
OS10(config)# monitor session 1
OS10(conf-mon-local-1)# no shut
```

```
OS10(config)# monitor session 5 type rpm-source
OS10(conf-mon-rpm-source-5)# no shut
```

```
OS10(config)# monitor session 10 type erpm-source
OS10(conf-mon-erpm-source-10)# no shut
```

Supported Releases 10.2.0E or later

source (Port Monitoring)

Configures a source for port monitoring. The monitoring session can be one of the following: local, RPM, or ERPM.

Syntax	<code>source interface <i>interface-type</i> {both rx tx}</code>
Parameters	<ul style="list-style-type: none">• <i>interface-type</i> — Enter the interface type:<ul style="list-style-type: none">◦ <code>ethernet <i>node/slot/port[:subport]</i></code> — Enter the Ethernet interface information as the monitored source.◦ <code>port-channel <i>id-number</i></code> — Enter the port-channel interface number as the monitored source (1 to 128). This option is not supported in S5148F-ON .◦ <code>vlan <i>vlan-id</i></code> — Enter the VLAN identifier as the monitored source (1 to 4093).• <code>both</code> — Monitor both receiving and transmitting packets. This option is not supported in S5148F-ON and not supported on VLAN interfaces for other platforms.• <code>rx</code> — Monitor only received packets.• <code>tx</code> — Monitor only transmitted packets. This option is not supported in S5148F-ON and not supported on VLAN interfaces for other platforms.
Default	Not configured
Command Mode	MONITOR-SESSION
Usage Information	None
Example	<pre>OS10(config)# monitor session 1 OS10(conf-mon-local-1)# source interface ethernet 1/1/7 rx OS10(config)# monitor session 5 type rpm-source OS10(conf-mon-rpm-source-5)# source interface ethernet 1/1/10 rx OS10(config)# monitor session 10 type erpm-source OS10(conf-mon-erpm-source-10)# source interface ethernet 1/1/5 rx</pre>
Supported Releases	10.2.0E or later

source-ip

Configures the source, destination, and protocol type of the monitored port for an ERPM monitoring session.

Syntax	<code>source-ip <i>source ip-address</i> <i>destination-ip destination ip-address</i> [<i>gre-protocol protocol-value</i>]</code>
Parameters	<ul style="list-style-type: none">• <i>source ip-address</i> — Enter the source IP address.• <i>destination ip-address</i> — Enter the destination IP address.• <i>protocol-value</i> — Enter the GRE protocol value (1 to 65535, default: 35006).
Default	Not configured
Command Mode	MONITOR-SESSION
Usage Information	None
Example	<pre>OS10(config)# monitor session 10 OS10(conf-mon-erpm-source-10)# source-ip 10.16.132.181 destination-ip 172.16.10.11 gre-protocol 35006</pre>
Supported Releases	10.4.0E(R1) or later

Layer 3

Bidirectional forwarding detection (BFD)	Provides rapid failure detection in links with adjacent routers (see BFD commands).
Border Gateway Protocol (BGP)	Provides an external gateway protocol that transmits inter-domain routing information within and between autonomous systems (see BGP Commands).
Equal Cost Multi-Path (ECMP)	Provides next-hop packet forwarding to a single destination over multiple best paths (see ECMP Commands).
IPv4 Routing	Provides forwarding of packets to a destination IP address, based on a routing table. This routing table defines how packets are routed — dynamically, broadcasted directly to, using proxy ARP, as well as what type of information is included with the packets (see IPv4 Routing Commands).
IPv6 Routing	Provides routing for the IPv6 address space, stateless auto-configuration, header format simplifications, and improved support for options and extensions (see IPv6 Routing Commands).
Open Shortest Path First (OSPF)	Provides a link-state routing protocol that communicates with all other devices in the same autonomous system area using link-state advertisements (LSAs). OS10 supports up to 10,000 OSPF routes for OSPFv2 to designate up to 8,000 routes as external, and up to 2,000 as inter/intra area routes (see OSPF Commands).
Virtual Router Redundancy Protocol (VRRP)	Provides a mechanism to eliminate a single point of failure in a statically routed network (see VRRP Commands).
Virtual Routing and Forwarding (VRF)	Provides a mechanism to partition a physical router into multiple virtual routers (see VRF Commands).

Virtual routing and forwarding

Virtual routing and forwarding (VRF) allows to partition a physical router into multiple virtual routers. The control and data plane are isolated in each virtual router (VR) so that traffic does not flow across VRs. VRF allows multiple instances of routing tables to co-exist within the same router at the same time.

OS 10 supports a management VRF instance, a default VRF instance, and up to 16 non-default VRF instances. Use the default and non-default VRF instances to configure routing.

You can move the management interface from the default to management VRF instance.

By default, OS10 initially assigns all physical interfaces and all logical interfaces to the default VRF instance.

Configure management VRF

You can assign only management interfaces to the management VRF instance.

Before you assign the management interface to the management VRF instance, remove all the configured settings, including the IP address, on the management interface.

1. Enter the `ip vrf management` command in the CONFIGURATION mode. Use non-transaction-based configuration mode only. Do not use transaction-based mode.
2. Add the management interface by using the `interface management` command in the VRF CONFIGURATION mode.

Configure management VRF

```
OS10(config)# ip vrf management
OS10(conf-vrf)# interface management
```

You can enable various services in the either of the management or default VRF instances. Refer to the following table for the services supported in the management VRF instance and the default VRF instance.

Table 3. Services supported

Application	Management VRF	Default VRF	Non default VRF
COPP ACL	Yes	Yes	No
DHCP client	Yes	Yes	Yes
DHCP relay	No	Yes	Yes
DHCP server	No	Yes	No
DNS client	Yes	Yes	Yes
FTP client	Yes	Yes	No
HTTP client	Yes	Yes	No
ICMP / Ping	Yes	Yes	No
NTP client	Yes	Yes	No
NTP server	Yes	Yes	No
BGP	No	Yes	Yes
OSPFV2 /OSPFV3	No	Yes	No
RADIUS server	Yes	Yes	No
SCP client	Yes	Yes	No
sFlow	No	Yes	No
SFTP	Yes	Yes	No
SNMP traps	Yes	Yes	No
SSH server`	Yes	Yes	No
Syslog	Yes	Yes	No
Telnet server	Yes	Yes	No
TFTP client	Yes	Yes	No
Traceroute	Yes	Yes	Yes
VLT backup link	Yes	Yes	No
VRRP	Yes	Yes	No

Configuring a static route for a management VRF instance

- Configure a static route that directs traffic to the management interface.

CONFIGURATION

```
management route ip-address mask management ethernet or management route ipv6-address
prefix-length management ethernet
```

You can also configure the management route to direct traffic to a physical interface in case of the management VRF instance. For example: `management route 10.1.1.5/24 ethernet 1/1/4` or `management route 2::/64 ethernet 1/1/1`.

- Configure a static entry in the IPv6 neighbor discovery.

CONFIGURATION

```
ipv6 neighbor vrf management 1::1 ethernet 1/1/1 xx:xx:xx:xx:xx:xx
```

Configure non-default VRF instances

In addition to a management VRF instance and default VRF, OS 10 also supports non-default VRF instances. You can create up to a maximum of 16 non-default VRF instances.

While you can assign management interfaces only to the management VRF instance, you can assign any physical or logical interface – VLAN, port channel or loopback, to a non-default VRF instance.

When you create a new non-default VRF instance, OS10 does not assign any interface to it. You can assign to the new VRF instance any of existing physical or logical interfaces, provided they are not already assigned to another non-default VRF.

NOTE: When you create a new logical interface, OS10 assigns it automatically to the default VRF instance. In addition, OS10 initially assigns all physical interfaces to the default VRF instance.

You can reassign any interface assigned to a non-default VRF instance back to the default VRF instance.

- Create a non-default VRF instance by specifying a name and enter VRF configuration mode.

CONFIGURATION

```
ip vrf vrf-name
```

Assigning an interface to a non-default VRF instance

After creating a non-default VRF instance you can associate a n interface to the VRF instance that you created.

To assign an interface to a non-default VRF, perform the following steps:

1. Enter the interface that you want to assign to a non-default VRF instance.

CONFIGURATION

```
interface ethernet 1/1/1
```

2. Remove the interface from L2 switching.

INTERFACE

```
no switchport
```

3. Assign the interface to a non-default VRF.

INTERFACE CONFIGURATION

```
ip vrf forwarding vrf-test
```

Before assigning a n interface to a VRF instance, ensure that no IP address is configured on the interface.

NOTE: In the default configuration, the interface is in L3 mode and it does not have an IP address. You can associate an interface in L3 mode and with default configuration to a VRF. You can associate an interface only with one VRF instance. Overwriting associations between interfaces and VRFs is not allowed, until all the interface configurations including the previous VRF associations are deleted.

4. Assign an IPv4 address to the interface.

INTERFACE CONFIGURATION

```
ip address 10.1.1.1/24
```

5. Assign an IPv6 address to the interface.

INTERFACE CONFIGURATION

```
ipv6 address 1::1/64
```


You can also auto configure an IPv6 address using the `ipv6 address autoconfig` command.

NOTE: Before configuring any routing protocol in a VRF instance, you need to first assign an IP address to at least one of the interfaces assigned to the VRF instance on which you want to configure routing protocols.

Assigning a loopback interface to a non-default VRF instance

After creating a non-default VRF instance you can associate a loopback interface to the VRF instance that you created.

To assign a loopback interface to a non-default VRF, perform the following steps:

1. Enter the loopback interface that you want to assign to a non-default VRF instance.

```
CONFIGURATION
interface loopback 5
```

2. Remove the interface from L2 switching.

```
INTERFACE
no switchport
```

3. Assign the interface to a non-default VRF.

```
INTERFACE CONFIGURATION
ip vrf forwarding vrf-test
```

Before assigning an interface to a VRF instance, ensure that no IP address is configured on the interface.

4. Assign an IPv4 address to the interface.

```
INTERFACE CONFIGURATION
ip address 10.1.1.1/24
```

5. Assign an IPv6 address to the interface.

```
INTERFACE CONFIGURATION
ipv6 address 1::1/64
```

You can also auto configure an IPv6 address using the `ipv6 address autoconfig` command.

Assigning an interface back to the default VRF instance

To assign an interface back to the default VRF, perform the following steps:

1. Enter the interface that you want to assign back to the default VRF instance.

```
CONFIGURATION
interface ethernet 1/1/1
```

2. Remove the interface from L2 switching.

```
INTERFACE
no switchport
```

3. Assign the interface back to the default VRF instance.

```
INTERFACE CONFIGURATION
no ip vrf forwarding
```

Assigning the management interface back to the default VRF instance

To assign the management interface back to the default VRF, perform the following steps:

1. Enter the management VRF instance.

```
CONFIGURATION
ip vrf management
```

2. Assign the management interface back to the default VRF instance.

```
CONFIGURATION VRF
```

no interface management

Deleting a non-default VRF instance

Before deleting a non-default VRF instance, ensure all the dependencies and associations corresponding to that VRF instance are first removed or disabled. Following table shows the dependencies that you have to remove before deleting a non-default VRF instance:

Table 4. Configurations to be removed


CONFIGURATION	MODE	COMMAND
IP address — In interface configuration mode, undo the IP address configuration.	INTERFACE CONFIGURATION	OS10(conf-if-eth1/1/10:1)#no ip address <i>ipv4-address</i> or no ipv6 address <i>ipv6-address</i>
Port — In interface configuration mode, remove the interface association corresponding to the VRF instance that you want to delete.	INTERFACE CONFIGURATION	OS10(conf-if-eth1/1/10:1)#no ip vrf forwarding

After removing all dependences, you can delete the non-default VRF instances that you create.

- Delete a non-default VRF instance using the following command:

CONFIGURATION

```
no ip vrf vrf-name
```

 **NOTE:** You cannot delete the default VRF instance.

Configuring a static route for a non-default VRF instance

- Configure a static route in a non-default VRF instance. Static routes contain IP addresses of the next-hop neighbors that are reachable through the non-default VRF. These IP addresses could also belong to the interfaces that are part of the non-default VRF instance.

CONFIGURATION

```
ip route vrf vrf-name ip-address mask next-hop-ip-address or ipv6 route vrf vrf-name ipv6-address prefix-length next-hp[=ipv6-address]
```

For example: `ip route vrf red 10.1.1.5/24 10.1.1.6` or `ipv6 route vrf red 2::/64 3::1`

- Configure the route to direct traffic to a front-panel port in case of a non-default VRF instance.

CONFIGURATION

```
ip route ip-address-mask ethernet interface-type or ipv6 route ipv6-address-mask ethernet interface-type
```

For example: `ip route 10.1.1.5/24 ethernet 1/1/1` or `ipv6 route 2::/64 ethernet 1/1/1`. Where ethernet 1/1/1 is part of the non-default VRF.

Configuring static entry in IPv6 neighbor

- Configure a static entry in the IPv6 neighbor discovery.

CONFIGURATION

```
ipv6 neighbor vrf vrf-test 1::1 ethernet 1/1 xx:xx:xx:xx:xx:xx
```

Sample VRF configuration

The following configuration illustrates a typical VRF set-up.

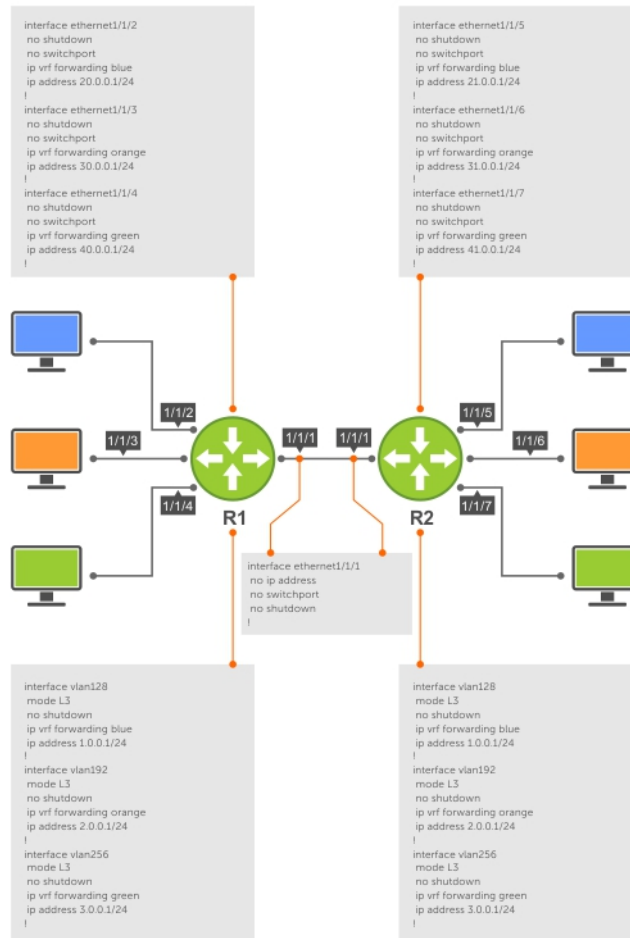


Figure 3. Setup VRF Interfaces

The following example relates to the configuration shown in the above illustrations.

Router 1

```

ip vrf blue
!
ip vrf orange
!
ip vrf green
!
interface ethernet 1/1/1
    no ip address
    no switchport
    no shutdown
!
interface ethernet1/1/2
    no shutdown
    no switchport
    ip vrf forwarding blue
    ip address 20.0.0.1/24
!
interface ethernet1/1/3
    no shutdown
    no switchport
    ip vrf forwarding orange
    ip address 30.0.0.1/24
!
interface ethernet1/1/4
    no shutdown
    no switchport

```

```

ip vrf forwarding green
ip address 40.0.0.1/24
!
interface vlan128
mode L3
no shutdown
ip vrf forwarding blue
ip address 1.0.0.1/24
!
interface vlan192
mode L3
no shutdown
ip vrf forwarding orange
ip address 2.0.0.1/24
!
!
interface vlan256
mode L3
no shutdown
ip vrf forwarding green
ip address 3.0.0.1/24
!
ip route vrf green 30.0.0.0/24 3.0.0.1

```

Router 2

```

ip vrf blue
!
ip vrf orange
!
ip vrf green
!
interface ethernet 1/1/1
no ip address
no switchport
no shutdown
!
interface ethernet1/1/5
no shutdown
no switchport
ip vrf forwarding blue
ip address 21.0.0.1/24
!
interface ethernet1/1/6
no shutdown
no switchport
ip vrf forwarding orange
ip address 31.0.0.1/24
!
interface ethernet1/1/7
no shutdown
no switchport
ip vrf forwarding green
ip address 41.0.0.1/24
!
interface vlan128
mode L3
no shutdown
ip vrf forwarding blue
ip address 1.0.0.1/24
!
interface vlan192
mode L3
no shutdown
ip vrf forwarding orange
ip address 2.0.0.1/24
!
interface vlan256
mode L3
no shutdown
ip vrf forwarding green
ip address 3.0.0.1/24

```

```
!  
ip route vrf green 31.0.0.0/24 3.0.0.1
```

The following shows the output of the show commands on Router 1.

Router 1

```
OS10# show ip vrf  
VRF-Name          Interfaces  
blue              Eth1/1/2  
                  Vlan128  
  
default           Mgmt1/1/1  
                  Vlan1,24-25,200  
  
green             Eth1/1/4  
                  Vlan256  
  
orange           Eth1/1/3  
                  Vlan192
```

```
OS10# show ip route vrf blue  
Codes: C - connected  
        S - static  
        B - BGP, IN - internal BGP, EX - external BGP  
        O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,  
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,  
        E2 - OSPF external type 2, * - candidate default,  
        + - summary route, > - non-active route  
Gateway of last resort is not set  
  Destination          Gateway                Dist/Metric  
Last Change  
-----  
-----  
C      20.0.0.0/24      via 20.0.0.1          ethernet1/1/2          0/0  
01:46:41
```

```
OS10# show ip route vrf orange  
Codes: C - connected  
        S - static  
        B - BGP, IN - internal BGP, EX - external BGP  
        O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,  
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,  
        E2 - OSPF external type 2, * - candidate default,  
        + - summary route, > - non-active route  
Gateway of last resort is not set  
  Destination          Gateway                Dist/Metric  
Last Change  
-----  
-----  
C      30.0.0.0/24      via 30.0.0.1          ethernet1/1/3          0/0  
01:55:00
```

```
OS10# show ip route vrf green  
Codes: C - connected  
        S - static  
        B - BGP, IN - internal BGP, EX - external BGP  
        O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,  
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,  
        E2 - OSPF external type 2, * - candidate default,  
        + - summary route, > - non-active route  
Gateway of last resort is not set  
  Destination          Gateway                Dist/Metric  
Last Change  
-----  
-----  
C      40.0.0.0/24      via 40.0.0.1          ethernet1/1/4          0/0  
02:01:15  
=====
```

The following shows the output of the show commands on Router 2.

Router 2

```
OS10# show ip vrf
VRF-Name          Interfaces
blue              Eth1/1/5
                  Vlan128

default           Mgmt1/1/1
                  Vlan1,24-25,200

green             Eth1/1/7
                  Vlan256

orange            Eth1/1/6
                  Vlan192
```

```
OS10# show ip route vrf blue
```

```
Codes: C - connected
        S - static
        B - BGP, IN - internal BGP, EX - external BGP
        O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
        E2 - OSPF external type 2, * - candidate default,
        + - summary route, > - non-active route
Gateway of last resort is not set
  Destination                                Gateway                                Dist/Metric
Last Change
-----
C      21.0.0.0/24                            via 21.0.0.1                            ethernet1/1/5                            0/0
02:05:00
```

```
OS10# show ip route vrf orange
```

```
Codes: C - connected
        S - static
        B - BGP, IN - internal BGP, EX - external BGP
        O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
        E2 - OSPF external type 2, * - candidate default,
        + - summary route, > - non-active route
Gateway of last resort is not set
  Destination                                Gateway                                Dist/Metric
Last Change
-----
C      31.0.0.0/24                            via 31.0.0.1                            ethernet1/1/6                            0/0
02:09:19
```

```
OS10# show ip route vrf green
```

```
Codes: C - connected
        S - static
        B - BGP, IN - internal BGP, EX - external BGP
        O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
        N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
        E2 - OSPF external type 2, * - candidate default,
        + - summary route, > - non-active route
Gateway of last resort is not set
  Destination                                Gateway                                Dist/Metric
Last Change
-----
C      41.0.0.0/24                            via 41.0.0.1                            ethernet1/1/7                            0/0
02:45:16
=====
```

View VRF instance information

To display information about VRF configuration, enter the `show ip vrf` command. To display information on all VRF instances (including the default VRF 0), do not enter a value for `vrf-name`.

- Display the interfaces assigned to a VRF instance.

EXEC

```
show ip vrf [vrf-name]
```

VRF commands

interface management

Adds management interface to the management VRF instance.

Syntax `interface management`

Parameters None

Default Not configured

Command Mode VRF CONFIGURATION

Usage Information The `no` version of this command removes the management interface from the management VRF instance.

Example

```
OS10(config)# ip vrf management
OS10(conf-vrf)# interface management
```

Supported Releases 10.4.0E(R1) or later

ip domain-list vrf

Configures a domain list for the management VRF instance or any non-default VRF instance that you create.

Syntax `ip domain-list vrf {management | vrf-name} domain-names`

- Parameters**
- `management`—Enter the keyword `management` to configure a domain list for the management VRF instance.
 - `vrf-name`—Enter the name of the non-default VRF instance to configure a domain list for that non-default VRF instance.
 - `domain-names`—Enter the list of domain names.

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the domain list configuration from the management or the non-default VRF instance.

Example

```
OS10(config)# ip domain-list vrf management dns1 dell.com
or
OS10(config)# ip domain-list vrf blue dns1 dell.com
```

Supported Releases 10.4.0E(R1) or later

ip domain-name vrf

Configures a domain name for the management VRF instance or any non-default VRF instance that you create.

Syntax `ip domain-name vrf {management | vrf-name} domain-name`

- Parameters**
- `management`—Enter the keyword `management` to configure a domain name for the management VRF instance.

- *vrf-name*—Enter the name of the non-default VRF instance to configure a domain name for that VRF instance.
- *domain-name*—Enter the domain name.

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the host name from the management or non-default VRF instance.

Example

```
OS10(config)# ip domain-name vrf management dell.com
or
OS10(config)# ip domain-name vrf blue dell.com
```

Supported Releases 10.4.0E(R1) or later

ip vrf

Create a non-default VRF instance.

Syntax `ip vrf vrf-name`

Parameters

- *vrf-name*—Enter the name of the non-default VRF that you want to create. Enter a VRF name that is not greater than 32 characters in length.

Default Not configured

Command Mode CONFIGURATION

Usage Information Enter the `ip vrf vrf-name` command only in non-transaction-based configuration mode. Do not use transaction-based mode. You can create up to a maximum of 16 non-default VRF instances. The `no ip vrf vrf-name` command removes the non-default VRF instance that you specify.

Example

```
OS10(config)# ip vrf vrf-test
OS10(conf-vrf-test)#
```

Supported Releases 10.4.1.0 or later

ip ftp vrf

Configures an FTP client for the management VRF instance.

Syntax `ip ftp vrf management`

Parameters None

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the management VRF instance configuration from the FTP client.

Example

```
OS10(config)# ip ftp vrf management
```

Supported Releases 10.4.0E(R1) or later

ip host vrf

Configures a host name for the management VRF instance or a non-default VRF instance and maps the host name to an IP/IPv6 address.

Syntax	<code>ip host vrf {management vrf-name} hostname {IP-address Ipv6-address}</code>
Parameters	<ul style="list-style-type: none">• <code>management</code>—Enter the keyword <code>management</code> to configure a host name for the management VRF instance.• <code>vrf-name</code>—Enter the name of the non-default VRF instance to configure a host name for that VRF instance.• <code>hostname</code>—Enter the host name.• <code>IP-address Ipv6-address</code>—Enter the host IP/IPv6 address.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the host name from the management or non-default VRF instance.
Example	<pre>OS10(config)# ip host vrf management dell 10.1.1.1 or OS10(config)# ip host vrf blue dell 10.1.1.1</pre>
Supported Releases	10.4.0E(R1) or later

ip http vrf

Configures an HTTP client for the management VRF instance.

Syntax	<code>ip http vrf management</code>
Parameters	None
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the management VRF instance configuration from the HTTP client.
Example	<pre>OS10(config)# ip http vrf management</pre>
Supported Releases	10.4.0E(R1) or later

ip name-server vrf

Configures a DNS name server for the management VRF instance or a non-default VRF instance.

Syntax	<code>ip name-server vrf {management vrf-name}</code>
Parameters	<ul style="list-style-type: none">• <code>management</code>—Enter the keyword <code>management</code> to configure a DNS name server for the management VRF instance.• <code>vrf-name</code>—Enter the name of the non-default VRF instance to configure a DNS name server for that VRF instance.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the management or non-default VRF instance configuration from the name sever.

Example

```
OS10(config)# ip name-server vrf management
or
OS10(config)# ip name-server vrf blue
```

Supported Releases

10.4.0E(R1) or later

ip scp vrf

Configures a SCP connection for the management VRF instance.

Syntax `ip scp vrf management`

Parameters None

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes management VRF instance configuration from the SCP client.

Example

```
OS10(config)# ip scp vrf management
```

Supported Releases

10.4.0E(R1) or later

ip sftp vrf

Configures an SFTP client for the management VRF instance.

Syntax `ip sftp vrf management`

Parameters None

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the management VRF instance configuration from the SFTP client.

Example

```
OS10(config)# ip sftp vrf management
```

Supported Releases

10.4.0E(R1) or later

ip tftp vrf

Configures a TFTP client for the management VRF instance.

Syntax `ip tftp vrf management`

Parameters None

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the management VRF instance configuration from the TFTP client.

Example

```
OS10(config)# ip tftp vrf management
```

Supported Releases 10.4.0E(R1) or later

ip vrf management

Configures the management VRF instance.

Syntax ip vrf management

Parameters None

Default Not configured

Command Mode CONFIGURATION

Usage Information Enter the `ip vrf management` command only in non-transaction-based configuration mode. Do not use transaction-based mode. The `no` version of this command removes the management VRF instance configuration.

Example

```
OS10(config)# ip vrf management
OS10(conf-vrf)#
```

Supported Releases 10.4.0E(R1) or later

show hosts vrf

Displays the host table in the management or non-default VRF instance.

Syntax show hosts vrf {management | vrf-name}

Parameters

- `management`—Enter the keyword `management` to display the host table in the management VRF instance.
- `vrf-name`—Enter the name of the non-default VRF instance to display the host table in that VRF instance.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show hosts vrf management
Default Domain Name : dell.com
Domain List : abc.com xyz.net
Name Servers : 10.16.126.1
=====
                        Static Host to IP mapping Table
=====
Host                                                              IP-Address
-----
google.com
172.217.160.142
yahoo.com
98.139.180.180
```

Supported Releases 10.4.0E(R1) or later

show ip vrf

Displays the VRF instance information.

Syntax show ip vrf [management | vrf-name]

- Parameters**
- `management`—Enter the keyword `management` to display information corresponding to the management VRF instance.
 - `vrf-name`—Enter the name of the non-default VRF instance to display information corresponding to that VRF instance.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show ip vrf
VRF-Name      Interfaces
default       Mgmt1/1/1
               Eth1/1/1-1/1/2
               Vlan1

management
```

```
OS10# show ip vrf management
VRF-Name      Interfaces
management
```

Supported Releases 10.4.0E(R1) or later

Bidirectional Forwarding Detection

The Bidirectional Forwarding Detection (BFD) protocol rapidly detects communication failures between two adjacent routers. BFD is a simple and lightweight replacement for link-state detection mechanisms in existing routing protocols. It also provides a failure detection solution for links with no routing protocol.

BFD provides forwarding-path failure detection that is performed in milliseconds, instead of seconds, as with routing protocol hello packets. Because BFD is independent of routing protocols, it provides consistent failure detection in a network. BFD eliminates multiple protocol-dependent timers and methods. Networks converge faster because BFD triggers link-state changes in the routing protocol sooner and more consistently.

BFD operates as a simple hello mechanism. Two neighboring routers running BFD establish a session using a three-way handshake. After the session is established, the routers exchange periodic control packets at sub-second intervals. If a router does not receive a hello packet within a specified time, routing protocols are notified that the forwarding path is down.

In addition, BFD sends a control packet when there is a state change or change in a session parameter. These control packets are sent without regard to transmit and receive intervals in a routing protocol.

BFD is an independent and generic protocol, which all media, topologies, and routing protocols can support using any encapsulation. OS10 implements BFD at Layer 3 (L3) and with User Datagram Protocol (UDP) encapsulation. BFD is supported for static and dynamic routing protocols, such as VRRP, OSPF, OSPFv3, IS-IS, and BGP.

 **NOTE:** In this release, BFD is only supported for BGP.

BFD session states

To establish a BFD session between two routers, enable BFD on both sides of the link. BFD routers can operate in both active and passive roles.

- The active router starts the BFD session. Both routers can be active in the same session.
- The passive router does not start a session. It only responds to a request for session initialization from the active router.

A BFD session can occur in Asynchronous and Demand modes. OS10 BFD supports only Asynchronous mode.

- In Asynchronous mode, both systems send periodic control messages at a specified interval to indicate that their session status is Up.

- In Demand mode, if one router requests Demand mode, the other router stops sending periodic control packets; it only sends a response to status inquiries from the Demand mode initiator. Either peer router, but not both, can request Demand mode at any time.

A BFD session can have four states: `Administratively Down`, `Down`, `Init`, and `Up`. The default BFD session state is `Down`.

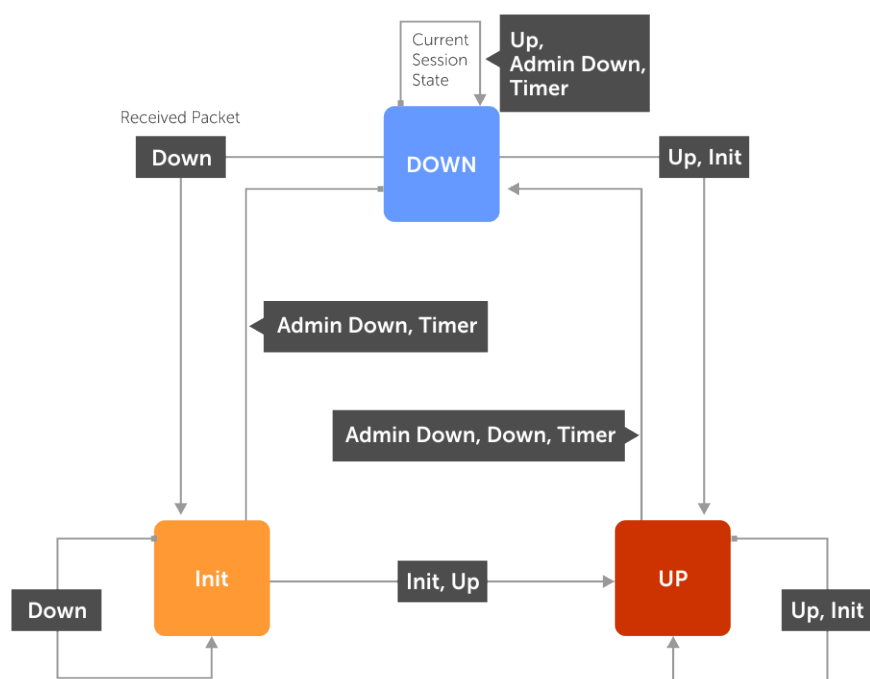
- `Administratively Down` — The local BFD router does not participate in the session.
- `Down` — The remote BFD router is not sending control packets or does not send them within the detection time for the session.
- `Init` — The local BFD router is communicating to the remote router in the session.
- `Up` — Both BFD routers are sending control packets.

A BFD session's state changes to `Down` if:

- A control packet is not received within the detection time.
- Demand mode is active and a control packet is not received in response to a poll packet.

Example: BFD session state changes

The session state on a router changes according to the status notification it receives from the peer router. For example, if the current session state is `Down` and the router receives a `Down` status notification from the remote router, the session state on the local router changes to `Init`.

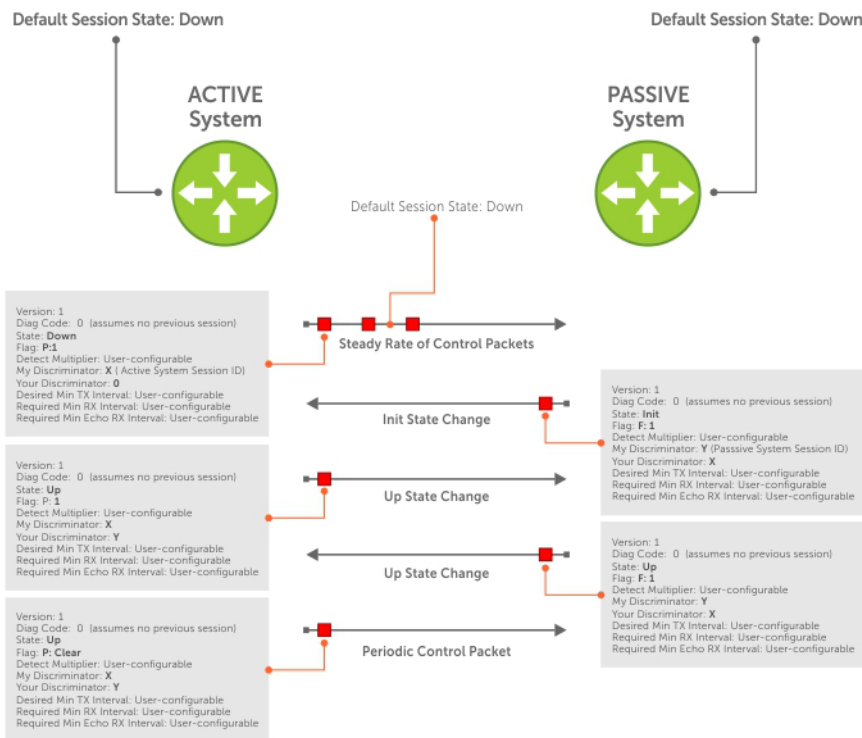


BFD three-way handshake

A BFD session requires a three-way handshake between neighboring routers. In the following example, the handshake assumes:

- One router is active, and the other router is passive.
 - This is the first session established on this link.
 - The default session state on both ports is `Down`.
1. The active system sends a steady stream of control packets to indicate that its session state is `Down`, until the passive system responds. These packets are sent at the desired transmit interval of the Active system. The `Your Discriminator` field is set to zero.
 2. When the passive system receives a control packet, it changes its session state to `Init` and sends a response to indicate its state change. The response includes its session ID in the `My Discriminator` field and the session ID of the remote system in the `Your Discriminator` field.
 3. The active system receives the response from the passive system and changes its session state to `Up`. It then sends a control packet to indicate this state change. Discriminator values are exchanged, and transmit intervals are negotiated.

- The passive system receives the control packet and changes its state to Up. Both systems agree that a session is established. However, because both members must send a control packet, which requires a response, whenever there is a state change or change in a session parameter, the passive system sends a final response indicating the state change. After this, periodic control packets are exchanged.



BFD configuration

Before you configure BFD for a routing protocol, first enable BFD globally on both routers in the link. BFD is disabled by default.

- OS10 supports:
 - 64 BFD sessions at 100 minimum transmit and receive intervals with a multiplier of 4
 - 100 BFD sessions at 200 minimum transmit and receive intervals with a multiplier of 3
- OS10 does not support Demand mode, authentication, and the Echo function.
- OS10 does not support BFD on multi-hop and virtual links.
- OS10 supports protocol liveness only for routing protocols.
- OS10 BFD supports only the BGP routing protocol. For IPv4 and IPv6 BGP, OS10 supports only the default VRF.

Configure BFD globally

Before you configure BFD for static routing or a routing protocol, configure BFD globally on each router, including the global BFD session settings. BFD is disabled by default.

- Configure the global BFD session parameters in CONFIGURATION mode.

```
bfd interval milliseconds min_rx milliseconds multiplier number role {active | passive}
```

- `interval milliseconds` — Enter the time interval for sending control packets to BFD peers, from 100 to 1000; default 200. Dell EMC recommends using more than 100 milliseconds.
- `min_rx milliseconds` — Enter the maximum waiting time for receiving control packets from BFD peers, from 100 to 1000; default 200. Dell EMC recommends using more than 100 milliseconds.

- `multiplier number` — Enter the number of consecutive packets that must not be received from a BFD peer before the session state changes to Down, from 3 to 50; default 3.
- `role {active | passive}` — Enter `active` if the router initiates BFD sessions. Both BFD peers can be active at the same time. Enter `passive` if the router does not initiate BFD sessions, and only responds to a request from an active BFD to initialize a session. The default is `active`.

2. Enable BFD globally in CONFIGURATION mode.

```
bfd enable
```

To verify that BFD is globally enabled, enter the `show running-config bfd` command.

BFD global configuration

```
OS10(config)# bfd interval 250 min_rx 300 multiplier 4 role passive
OS10(config)# bfd enable
OS10(config)# do show running-config bfd
!
bfd enable
bfd interval 250 min_rx 300 multiplier 4 role passive
```

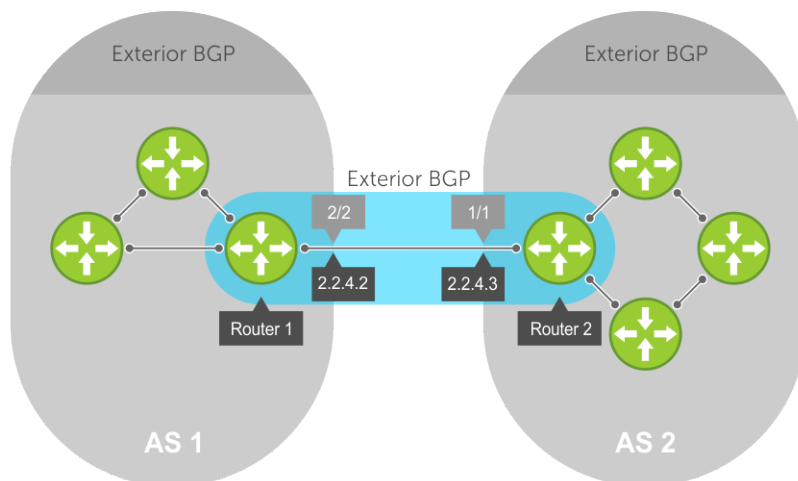
BFD for BGP

In a BGP core network, BFD enables faster network reconvergence. BFD rapidly detects communication failures in BGP fast-forwarding paths between internal BGP (iBGP) and external BGP (eBGP) peers. BFD for BGP is supported on physical, port-channel, and VLAN interfaces. BFD for BGP does not support the BGP multihop feature.

Before configuring BFD for BGP, first configure BGP on the interconnected routers. For more information, see [Border Gateway Protocol](#).

BFD for BGP example

In this BFD for BGP configuration example, Router 1 and Router 2 use eBGP in a transit network to interconnect AS1 and AS2. The eBGP routers exchange information with each other and with iBGP routers to maintain connectivity and accessibility within each autonomous system.



When you configure a BFD session with a BGP neighbor, you can:

- Establish a BFD session with a specified BGP neighbor using the `neighbor ip-address bfd` commands.
- Establish BFD sessions with all neighbors discovered by BGP using the `bfd all-neighbors` command.

For example:

Router 1

```
OS10(conf)# bfd enable
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# neighbor 2.2.4.3
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown
OR
OS10(conf)# bfd enable
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# bfd all-neighbors interval 200 min_rx 200 multiplier 6 role
active
```

Router 2

```
OS10(conf)# bfd enable
OS10(conf)# router bgp 2
OS10(config-router-bgp-2)# neighbor 2.2.4.2
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown
OR
OS10(conf)# bfd enable
OS10(conf)# router bgp 2
OS10(config-router-bgp-2)# bfd all-neighbors interval 200 min_rx 200 multiplier 6 role
active
```

BFD packets originating from a router are assigned to the highest priority egress queue to minimize transmission delays. Incoming BFD control packets received from the BGP neighbor are assigned to the highest priority queue within the control plane policing (CoPP) framework to avoid BFD packets drops due to queue congestion.

BFD notifies BGP of any failure conditions that it detects on the link. BGP initiates recovery actions.

BFD for BGP is supported only on directly connected BGP neighbors and in both BGP IPv4 and IPV6 networks. A maximum of 100 simultaneous BFD sessions are supported.

If each BFD for BGP neighbor receives a BFD control packet within the configured BFD interval for failure detection, the BFD session remains up and BGP maintains its adjacencies. If a BFD for BGP neighbor does not receive a control packet within the detection interval, the router informs any clients of the BFD session, and other routing protocols, about the failure. It then depends on the routing protocol that uses the BGP link to determine the appropriate response to the failure condition. The normal response is to terminate the peering session for the routing protocol and reconverge by bypassing the failed neighboring router. A log message is generated whenever BFD detects a failure condition.

Configure BFD for BGP

OS10 supports the establishment of BFD sessions with IPv4 or IPv6 BGP neighbors using the default VRF. When you configure BFD for BGP, you can enable BFD sessions with all BGP neighbors discovered by BGP or with a specified neighbor.

1. Configure BFD session parameters and enable BFD globally on all interfaces in CONFIGURATION mode as described in [Configure BFD globally](#).

```
bfd interval milliseconds min_rx milliseconds multiplier number role {active |
passive}
bfd enable
```

2. Enter the AS number of a remote BFD peer in CONFIGURATION mode, from 1 to 65535 for a 2-byte AS number and from 1 to 4294967295 for a 4-byte AS number. Only one AS number is supported per system. If you enter a 4-byte AS number, 4-byte AS support is enabled automatically.

```
router bgp as-number
```

3. Enter the IP address of a BFD peer in ROUTER-BGP mode. Enable a BFD session and the BGP link in ROUTER-NEIGHBOR mode. The global BFD session parameters configured in Step 1 are used.

```
neighbor ip-address
  bfd
  no shutdown
```

OR

Configure BFD sessions with all neighbors discovered by the BGP in ROUTER-BGP mode. The BFD session parameters you configure override the global session parameters configured in Step 1.

```
bfd all-neighbors [interval milliseconds min_rx milliseconds multiplier number role
{active | passive}]
```

- *interval milliseconds* — Enter the time interval for sending control packets to BFD peers, from 100 to 1000; default 200. Dell EMC recommends using more than 100 milliseconds.
- *min_rx milliseconds* — Enter the maximum waiting time for receiving control packets from BFD peers, from 100 to 1000; default 200. Dell EMC recommends using more than 100 milliseconds.
- *multiplier number* — Enter the maximum number of consecutive packets that are not received from a BFD peer before the session state changes to Down, from 3 to 50; default 3.
- *role {active | passive}* — Enter *active* if the router initiates BFD sessions. Both BFD peers can be active at the same time. Enter *passive* if the router does not initiate BFD sessions, and only responds to a request from an active BFD to initialize a session. The default is *active*.

To ignore the configured `bfd all-neighbors` settings for a specified neighbor, enter the `bfd disable` command in ROUTER-NEIGHBOR mode.

OR

Enter a BGP template with neighborhood name in ROUTER-BGP mode. Configure BFD sessions with all neighbors which inherit the template in ROUTER-TEMPLATE mode. For more information on how to use BGP templates, see [Peer templates](#). The global BFD session parameters configured in Step 1 are used.

```
template template-name
  bfd
  no shutdown
```

4. Verify the BFD for BGP configuration in EXEC mode.

```
show bfd neighbors [detail]
```

BFD for BGP all-neighbors configuration

```
OS10(conf)# bfd interval 200 min_rx 200 multiplier 6 role active
OS10(conf)# bfd enable
OS10(conf)# router bgp 4
OS10(config-router-bgp-4)# bfd all-neighbors interval 200 min_rx 200 multiplier 6 role
active
```

BFD for BGP single-neighbor configuration

```
OS10(conf)# bfd interval 200 min_rx 200 multiplier 6 role active
OS10(conf)# bfd enable
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# neighbor 150.150.1.1
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown
```

BFD for BGP template configuration

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300)# template ebgppg
OS10(config-router-template)# bfd
OS10(config-router-template)# exit
OS10(config-router-bgp-300)# neighbor 3.1.1.1
OS10(config-router-neighbor)# inherit template ebgppg
OS10(config-router-neighbor)# no shutdown
```

Display BFD operation

```
OS10# show bfd neighbors
* - Active session role
-----
LocalAddr      RemoteAddr    Interface    State Rx-int Tx-int Mult VRF   Clients
```

```
-----  
* 150.150.1.2 150.150.1.1 vlan10 up 1000 1000 5 default bgp
```

```
OS10# show bfd neighbors detail  
Session Discriminator: 1  
Neighbor Discriminator: 2  
Local Addr: 150.150.1.2  
Local MAC Addr: 90:b1:1c:f4:ab:fd  
Remote Addr: 150.150.1.1  
Remote MAC Addr: 90:b1:1c:f4:a4:d4  
Interface: vlan10  
State: up  
Configured parameters:  
TX: 1000ms, RX: 1000ms, Multiplier: 5  
Actual parameters:  
TX: 1000ms, RX: 1000ms, Multiplier: 5  
Neighbor parameters:  
TX: 200ms, RX: 200ms, Multiplier: 49  
Role: active  
VRF: default  
Client Registered: bgp  
Uptime: 01:58:09  
Statistics:  
  Number of packets received from neighbor: 7138  
  Number of packets sent to neighbor: 7138
```

Verify BFD for BGP

```
OS10(config-router-bgp-101)# show ip bgp summary  
BGP router identifier 30.1.1.2 local AS number 101  
Global BFD is enabled  
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx  
20.1.1.1 101 781 777 11:16:13 0  
30.1.1.1 101 787 779 11:15:35 0
```

```
OS10(config-router-bgp-101)# show ip bgp neighbors  
BGP neighbor is 20.1.1.1, remote AS 101, local AS 101 internal link
```

```
BGP version 4, remote router ID 30.1.1.1  
BGP state ESTABLISHED, in this state for 11:19:01  
Last read 00:24:31 seconds  
Hold time is 180, keepalive interval is 60 seconds  
Configured hold time is 180, keepalive interval is 60 seconds  
Fall-over disabled
```

Neighbor is using Global level BFD Configuration

```
Received 784 messages  
  1 opens, 0 notifications, 0 updates  
  783 keepalives, 0 route refresh requests  
Sent 780 messages  
  2 opens, 0 notifications, 0 updates  
  778 keepalives, 0 route refresh requests  
Minimum time between advertisement runs is 30 seconds  
Minimum time before advertisements start is 0 seconds  
Capabilities received from neighbor for IPv4 Unicast:  
  MULTIPROTO_EXT(1)  
  ROUTE_REFRESH(2)  
  CISCO_ROUTE_REFRESH(128)  
  4_OCTET_AS(65)  
Capabilities advertised to neighbor for IPv4 Unicast:  
  MULTIPROTO_EXT(1)  
  ROUTE_REFRESH(2)  
  CISCO_ROUTE_REFRESH(128)  
  4_OCTET_AS(65)  
Prefixes accepted 0, Prefixes advertised 0  
Connections established 1; dropped 0  
Last reset never  
For address family: IPv4 Unicast  
  Allow local AS number 0 times in AS-PATH attribute  
Prefixes ignored due to:
```

```
Martian address 0, Our own AS in AS-PATH 0
Invalid Nexthop 0, Invalid AS-PATH length 0
Wellknown community 0, Locally originated 0
```

```
Local host: 20.1.1.2, Local port: 179
Foreign host: 20.1.1.1, Foreign port: 58248
```

BFD commands

bfd

Enables BFD sessions with specified neighbors.

Syntax bfd

Parameters None

Default Not configured

Command Mode ROUTER-NEIGHBOR
 ROUTER-TEMPLATE

Usage Information

- Use the `bfd` command to configure BFD sessions with a specified neighbor or neighbors which inherit a BGP template. Use the `neighbor {ip-address | ipv6-address}` command in ROUTER-BGP mode to specify the neighbor. Use the `template template-name` command in ROUTER-BGP mode to specify a BGP template. Use the `no bfd` command in ROUTER-NEIGHBOR mode to disable BFD sessions with a neighbor.
- Use the `bfd all-neighbors` command to configure L3 protocol-specific BFD parameters for all BFD sessions between discovered neighbors. The BFD parameters you configure override the global session parameters configured with the `bfd interval` command.

Example

```
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# neighbor 10.1.1.1
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown
```

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300)# template ebpppg
OS10(config-router-template)# bfd
OS10(config-router-template)# exit
OS10(config-router-bgp-300)# neighbor 3.1.1.1
OS10(config-router-neighbor)# inherit template ebpppg
OS10(config-router-neighbor)# no shutdown
```

Supported releases 10.4.1.0 or later

bfd all-neighbors

Configures the parameters used in all BFD sessions between neighbors discovered by an L3 protocol.

Syntax bfd all-neighbors [*milliseconds min_rx milliseconds multiplier number role*
 {active | passive}]

Parameters

- *interval milliseconds* — Enter the time interval for sending control packets to BFD peers, from 100 to 1000. Dell EMC recommends using more than 100 milliseconds.
- *min_rx milliseconds* — Enter the maximum waiting time for receiving control packets from BFD peers, from 100 to 1000. Dell EMC recommends using more than 100 milliseconds.
- *multiplier number* — Enter the maximum number of consecutive packets that must not be received from a BFD peer before the session state changes to Down, from 3 to 50.

- `role {active | passive}` — Enter `active` if the router initiates BFD sessions. Both BFD peers can be active at the same time. Enter `passive` if the router does not initiate BFD sessions, and only responds to a request from an active BFD to initialize a session.

Default The time interval for sending control packets to BFD peers is 200 milliseconds.
 The maximum waiting time for receiving control packets from BFD peers is 200 milliseconds.
 The number of consecutive packets that must be received from a BFD peer is 3.
 The BFD role is `active`

Command Mode ROUTER-BGP

Usage Information

- Use the `bfd all-neighbors` command to configure BFD sessions between discovered neighbors. The BFD session parameters you configure override the global session parameters configured with the `bfd interval` command. To disable BFD and ignore the configured `bfd all-neighbors` settings for a specified neighbor, enter the `bfd disable` command in ROUTER-NEIGHBOR mode.
- To remove the configured all-neighbors settings for all BGP neighbors, enter the `no` version of the command. To return to the default values, enter the `bfd all-neighbors` command.

Example

```
OS10(conf-router-bgp)# bfd all-neighbors interval 250 min_rx 300
multiplier 4 role passive
```

Supported releases 10.4.1.0 or later

bfd disable

Ignores the configured `bfd all-neighbors` settings and disables BFD for a specified neighbor.

Syntax `bfd disable`

Parameters None

Default Not configured

Command Mode ROUTER-NEIGHBOR

Usage Information Use the `neighbor ip-address` command in ROUTER-BGP mode to specify a neighbor. Use the `bfd disable` command to disable BFD sessions with the neighbor.

Example

```
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# neighbor 10.1.1.1
OS10(config-router-neighbor)# bfd disable
```

Supported releases 10.4.1.0 or later

bfd enable

Enables BFD on all interfaces on the switch.

Syntax `bfd enable`

Parameters None

Default BFD is disabled.

Command Mode CONFIGURATION

Usage Information Before you configure BFD for static routing or a routing protocol, enable BFD globally on each router in a BFD session. To globally disable BFD on all interfaces, enter the `no bfd enable` command.

Example

```
OS10(config)# bfd enable
```

Supported releases 10.4.1.0 or later

bfd interval

Configures parameters for all BFD sessions on the switch.

Syntax `bfd interval milliseconds min_rx milliseconds multiplier number role {active | passive}`

- Parameters**
- `interval milliseconds` — Enter the time interval for sending control packets to BFD peers, from 100 to 1000. Dell EMC recommends using more than 100 milliseconds.
 - `min_rx milliseconds` — Enter the maximum waiting time for receiving control packets from BFD peers, from 100 to 1000. Dell EMC recommends using more than 100 milliseconds.
 - `multiplier number` — Enter the number of consecutive packets that must not be received from a BFD peer before the session state changes to Down, from 3 to 50.
 - `role {active | passive}` — Enter `active` if the router initiates BFD sessions. Both BFD peers can be active at the same time. Enter `passive` if the router does not initiate BFD sessions, and only responds to a request from an active BFD to initialize a session.

Default

The time interval for sending control packets to BFD peers is 200 milliseconds.
The maximum waiting time for receiving control packets from BFD peers is 200 milliseconds.
The number of consecutive packets that must be received from a BFD peer is 3.
The BFD role is `active`.

Command Mode CONFIGURATION

Usage Information Use the `bfd interval` command to configure global BFD session settings. To configure the BFD parameters used in sessions established with neighbors discovered by an L3 protocol, use the `bfd all-neighbors` command. To remove the configured global settings and return to the default values, enter the `no` version of the command.

Example

```
OS10(config)# bfd interval 250 min_rx 300 multiplier 4 role passive
```

Supported releases 10.4.1.0 or later

show bfd neighbors

Displays information about BFD neighbors from all interfaces using the default VRF.

Syntax `show bfd neighbors [detail]`

Parameters `detail` — (Optional) View detailed information about BFD neighbors.

Default Not configured

Command Mode EXEC

Usage Information Use the `show bfd neighbors` command to verify that a BFD session between neighbors is up using the default VRF instance. Enter the `details` parameter to view the BFD session parameters.

Example

```
OS10# show bfd neighbors
* - Active session role
-----
LocalAddr      RemoteAddr    Interface    State Rx-int Tx-int Mult VRF  Clients
-----
* 150.150.1.2  150.150.1.1  vlan10      up    1000  1000  5   default  bgp
```

```
OS10# show bfd neighbors detail
Session Discriminator: 1
```

```
Neighbor Discriminator: 2
Local Addr: 150.150.1.2
Local MAC Addr: 90:b1:1c:f4:ab:fd
Remote Addr: 150.150.1.1
Remote MAC Addr: 90:b1:1c:f4:a4:d4
Interface: vlan10
State: up
Configured parameters:
TX: 1000ms, RX: 1000ms, Multiplier: 5
Actual parameters:
TX: 1000ms, RX: 1000ms, Multiplier: 5
Neighbor parameters:
TX: 200ms, RX: 200ms, Multiplier: 49
Role: active
VRF: default
Client Registered: bgp
Uptime: 01:58:09
Statistics:
  Number of packets received from neighbor: 7138
  Number of packets sent to neighbor: 7138
```

Supported releases 10.4.1.0 or later

Border Gateway Protocol

Border Gateway Protocol (BGP) is an interautonomous system routing protocol that transmits interdomain routing information within and between autonomous systems (AS). The primary function of BGP is to exchange network reachability information with other BGP systems. BGP adds reliability to network connections by using multiple paths from one router to another. Unlike most routing protocols, BGP uses TCP as its transport protocol.

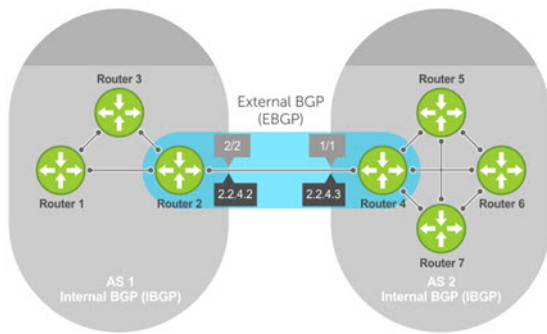
Autonomous systems

BGP autonomous systems are a collection of nodes under a single administration with shared network routing policies. Each AS has a number, which an Internet authority assigns—you do not assign the BGP number.

The Internet Assigned Numbers Authority (IANA) identifies each network with a unique AS number (ASN). The AS numbers 64512 through 65534 are reserved for private purposes. The AS numbers 0 and 65535 cannot be used in a live environment. IANA assigns valid AS numbers in the range of 1 to 64511.

- Multihomed AS** Maintains connections to more than one other AS. This group allows the AS to remain connected to the Internet if a complete failure occurs to one of their connections. This type of AS does not allow traffic from one AS to pass through on its way to another AS.
- Stub AS** Connected to only one AS.
- Transit AS** Provides connections through itself to separate networks. For example, Router 1 uses Router 2—the transit AS, to connect to Router 4. Internet service providers (ISPs) are always a transit AS because they provide connections from one network to another. An ISP uses a transit AS to sell transit service to a customer network.

When BGP operates inside an AS - AS1 or AS2, it functions as an Internal Border Gateway Protocol (IBGP). When BGP operates between AS endpoints - AS1 and AS2, it functions as an External Border Gateway Protocol (EBGP). IBGP provides routers inside the AS with the path to reach a router external to the AS. EBGP routers exchange information with other EBGP routers and IBGP routers to maintain connectivity and accessibility.



Classless interdomain routing

BGPv4 supports classless interdomain routing (CIDR) with aggregate routes and AS paths. CIDR defines a network using a prefix consisting of an IP address and mask, resulting in efficient use of the IPv4 address space. Using aggregate routes reduces the size of routing tables.

Path-vector routing

BGP uses a path-vector protocol which maintains dynamically updated path information. Path information updates which return to the originating node are detected and discarded. BGP does not use a traditional Internal Gateway Protocol (IGP) matrix but makes routing decisions based on path, network policies, and/or rule sets.

Full-mesh topology

In an AS, a BGP network must be in “full mesh” for routes received from an internal BGP peer to send to another IBGP peer. Each BGP router talks to all other BGP routers in a session. For example, in an AS with four BGP routers, each router has three peers; in an AS with six routers, each router has five peers.

Sessions and peers

A BGP session starts with two routers communicating using the BGP. The two end-points of the session are called *peers*. A peer is also called a *neighbor*. Events and timers determine the information exchange between peers. BGP focuses on traffic routing policies.

Sessions

In operations with other BGP peers, a BGP process uses a simple finite state machine consisting of six states—Idle, Connect, Active, OpenSent, OpenConfirm, and Established. For each peer-to-peer session, a BGP implementation tracks the state of the session. The BGP defines the messages that each peer exchanges to change the session from one state to another.

- Idle** BGP initializes all resources, refuses all inbound BGP connection attempts, and starts a TCP connection to the peer.
- Connect** Router waits for the TCP connection to complete and transitions to the `OpenSent` state if successful. If that transition is not successful, BGP resets the `ConnectRetry` timer and transitions to the `Active` state when the timer expires.
- Active** Router resets the `ConnectRetry` timer to zero and returns to the `Connect` state.
- OpenSent** Router sends an `Open` message and waits for one in return after a successful `OpenSent` transition.
- OpenConfirm** Neighbor relation establishes and is in the `OpenConfirm` state after the `Open` message parameters are agreed on between peers. The router then receives and checks for agreement on the parameters of the open messages to establish a session.
- Established** Keepalive messages exchange, and after a successful receipt, the router is in the `Established` state. Keepalive messages continue to send at regular periods. The keepalive timer establishes the state to verify connections.

After the connection is established, the router sends and receives keepalive, update, and notification messages to and from its peer.

Peer templates

Peer templates allow BGP neighbors to inherit the same outbound policies. Instead of manually configuring each neighbor with the same policy, you can create a peer group with a shared policy that applies to individual peers. A peer template provides efficient update calculation with simplified configuration.

Peer templates also aid in convergence speed. When a BGP process sends the same information to many peers, a long output queue may be set up to distribute the information. For peers that are members of a peer template, the information is sent to one place then passed on to the peers within the template.

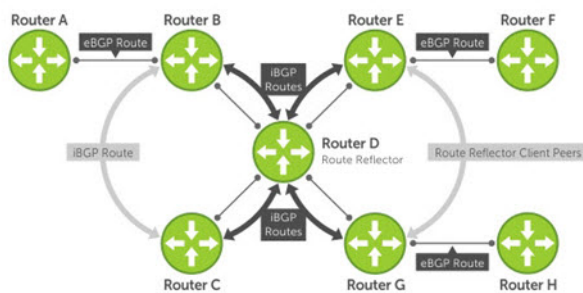
Route reflectors

Route reflectors (RRs) reorganize the IBGP core into a hierarchy and allow route advertisement rules. Route reflection divides IBGP peers into two groups — client peers and nonclient peers.

- If a route is received from a nonclient peer, it reflects the route to all client peers
- If a route is received from a client peer, it reflects the route to all nonclient and client peers

An RR and its client peers form a *route reflection cluster*. BGP speakers announce only the best route for a given prefix. RR rules apply after the router makes its best path decision.

NOTE: Do not use RRs in forwarding paths — hierarchal RRs that maintain forwarding plane RRs could create route loops.



Routers B, C, D, E, and G are members of the same AS—AS100. These routers are also in the same route reflection cluster, where Router D is the route reflector. Routers E and G are client peers of Router D, and Routers B and C are nonclient peers of Router D.

1. Router B receives an advertisement from Router A through EBGP. Because the route is learned through EBGP, Router B advertises it to all its IBGP peers — Routers C and D.
2. Router C receives the advertisement but does not advertise it to any peer because its only other peer is Router D (an IBGP peer) and Router D has already learned it through IBGP from Router B.
3. Router D does not advertise the route to Router C because Router C is a nonclient peer. The route advertisement came from Router B which is also a nonclient peer.
4. Router D does reflect the advertisement to Routers E and G because they are client peers of Router D.
5. Routers E and G advertise this IBGP learned route to their EBGP peers — Routers F and H.

Multiprotocol BGP

Multiprotocol BGP (MBGP) is an extension to BGP that supports multiple address families—IPv4 and IPv6. MBGP carries multiple sets of unicast and multicast routes depending on the address family.

You can enable the MBGP feature on a per router, per template, and/or a per peer basis. The default is the IPv4 unicast routes.

BGP session supports multiple address family interface (AFI) and sub address family interface (SAFI) combinations, BGP uses OPEN message to convey this information to the peers. As a result, the IPv6 routing information is exchanged over the IPv4 peers and vice versa.

BGP routers that support IPv6 can set up BGP sessions using IPv6 peers. If the existing BGP-v4 session is capable of exchanging ipv6 prefixes, the same is used to carry ipv4 as well as ipv6 prefixes. If the BGP-v4 neighbor goes down, it also impacts the IPv6 route exchange. If BGP-v6 session exists, it continues to operate independently from BGP-v4.

Multiprotocol BGPv6 supports many of the same features and functionality as BGPv4. IPv6 enhancements to MBGP include support for an IPv6 address family and Network Layer Reachability Information (NLRI) and next hop attributes that use the IPv6 addresses.

Attributes

Routes learned using BGP have associated properties that are used to determine the best route to a destination when multiple paths exist to a particular destination. These properties are called *BGP attributes* which influence route selection for designing robust networks. There are no hard-coded limits on the number of supported BGP attributes.

BGP attributes for route selection:

- Weight
- Local preference
- Multiexit discriminators
- Origin
- AS path
- Next-hop

Communities

BGP communities are sets of routes with one or more common attributes. Communities assign common attributes to multiple routes at the same time. Duplicate communities are not rejected.

Selection criteria

Best path selection criteria for BGP attributes:

1. Prefer the path with the largest WEIGHT attribute, and prefer the path with the largest LOCAL_PREF attribute.
2. Prefer the path that is locally originated using the `network` command, `redistribute` command, or `aggregate-address` command. Routes originated using a `network` or `redistribute` command are preferred over routes that originate with the `aggregate-address` command.
3. (Optional) If you configure the `bgp bestpath as-path ignore` command, skip this step because the AS_PATH is not considered. Prefer the path with the shortest AS_PATH:
 - An AS_SET has a path length of 1 no matter how many are in the set
 - A path with no AS_PATH configured has a path length of 0
 - AS_CONFED_SET is not included in the AS_PATH length
 - AS_CONFED_SEQUENCE has a path length of 1 no matter how many ASs are in the AS_CONFED_SEQUENCE
4. Prefer the path with the lowest ORIGIN type—IGP is lower than EGP and EGP is lower than INCOMPLETE.
5. Prefer the path with the lowest multiexit discriminator (MED) attribute:
 - This comparison is only done if the first neighboring AS is the same in the two paths. The MEDs compare only if the first AS in the AS_SEQUENCE is the same for both paths.
 - Configure the `bgp always-compare-med` command to compare MEDs for all paths.
 - Paths with no MED are treated as “worst” and assigned a MED of 4294967295.
6. Prefer external (EBGP) to internal (IBGP) paths or confederation EBGp paths, and prefer the path with the lowest IGP metric to the BGP next-hop.
7. The system deems the paths as equal and only performs the following steps if the criteria are not met:
 - Configure the IBGP multipath or EBGp multipath using the `maximum-path` command.
 - The paths being compared were received from the same AS with the same number of AS in the AS Path but with different next-hops.
 - The paths were received from IBGP or EBGp neighbor, respectively.
8. If you enable the `bgp bestpath router-id ignore` command and:
 - If the Router-ID is the same for multiple paths because the routes were received from the same route—skip this step.
 - If the Router-ID is **not** the same for multiple paths, prefer the path that was first received as the Best Path. The path selection algorithm returns without performing any of the checks detailed.
9. Prefer the external path originated from the BGP router with the lowest router ID. If both paths are external, prefer the oldest path—first received path. For paths containing an RR attribute, the originator ID is substituted for the router ID. If two paths have the same router ID, prefer the path with the lowest cluster ID length. Paths without a cluster ID length are set to a 0 cluster ID length.
10. Prefer the path originated from the neighbor with the lowest address. The neighbor address is used in the BGP neighbor configuration and corresponds to the remote peer used in the TCP connection with the local router.

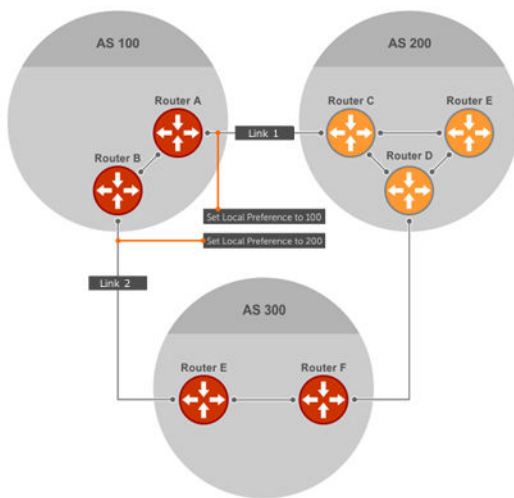
In Non-Deterministic mode, the `bgp non-deterministic-med` command applies. Paths compare in the order they arrive. This method leads to system selection of different best paths from a set of paths. Depending on the order they were received from the neighbors, MED may or may not get compared between the adjacent paths. In Deterministic mode, the system compares MED. MED is compared between the adjacent paths within an AS group because all paths in the AS group are from the same AS.

Weight and local preference

The weight attribute is local to the router and does not advertise to neighboring routers. If the router learns about more than one route to the same destination, the route with the highest weight is preferred. The route with the highest weight is installed in the IP routing table.

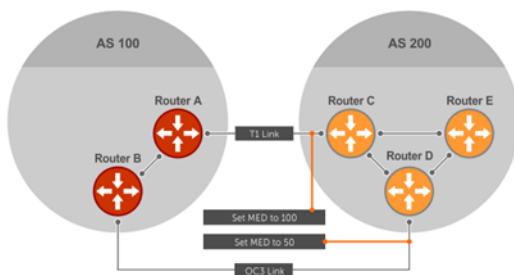
The local preference — LOCAL_PREF represents the degree of preference within the entire AS. The higher the number, the greater the preference for the route.

LOCAL_PREF is one of the criteria that determines the best path — other criteria may impact selection, see [Best path selection](#). Assume that LOCAL_PREF is the only attribute applied and AS 100 has two possible paths to AS 200. Although the path through Router A is shorter, the LOCAL_PREF settings have the preferred path going through Router B and AS 300. This advertises to all routers within AS 100, causing all BGP speakers to prefer the path through Router B.



Multixit discriminators

If two autonomous systems connect in more than one place, use a multixit discriminator (MED) to assign a preference to a preferred path. MED is one of the criteria used to determine best path—other criteria may also impact selection.



One AS assigns the MED a value. Other AS uses that value to decide the preferred path. Assume that the MED is the only attribute applied and there are two connections between AS 100 and AS 200. Each connection is a BGP session. AS 200 sets the MED for its Link 1 exit point to 100 and the MED for its Link 2 exit point to 50. This sets up a path preference through Link 2. The MEDs advertise to AS 100 routers so they know which is the preferred path.

MEDs are nontransitive attributes. If AS 100 sends the MED to AS 200, AS 200 does not pass it on to AS 300 or AS 400. The MED is a locally relevant attribute to the two participating AS — AS 100 and AS 200. The MEDs advertise across both links—if a link goes down, AS 100 has connectivity to AS 300 and AS 400.

Origin

The origin indicates how the prefix came into BGP. There are three origin codes—IGP, EGP, and INCOMPLETE.

- IGP** Prefix originated from information learned through an IGP.
- EGP** Prefix originated from information learned from an EGP, which Next Generation Protocol (NGP) replaced.
- INCOMPLETE** Prefix originated from an unknown source.

An IGP indicator means that the route was derived inside the originating AS. EGP means that a route was learned from an external gateway protocol. An INCOMPLETE origin code results from aggregation, redistribution, or other indirect ways of installing routes into BGP.

The question mark (?) indicates an origin code of INCOMPLETE, and the lower case letter (i) indicates an origin code of IGP.

Origin configuration

```
OS10# show ip bgp
BGP local RIB : Routes to be Added , Replaced , Withdrawn
BGP local router ID is 30.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop    Metric  LocPrf  Weight  Path
*>I          1.1.1.0/24  17.1.1.2  0        0        0        i
*>I          2.2.2.0/24  17.1.1.2  0        0        0        ?
*>I          3.3.3.0/24  17.1.1.2  0        0        0        e
```

AS path and next-hop

The AS path is the AS list that all the prefixes listed in the update have passed through. The BGP speaker adds the local AS number when advertising to an EBGP neighbor. Any update that contains the AS path number 0 is valid.

The next-hop is the IP address used to reach the advertising router:

- For EBGP neighbors, the next-hop address is the IP address of the connection between neighbors.
- For IBGP neighbors, the EBGP next-hop address is carried into the local AS. A next hop attribute sets when a BGP speaker advertises itself to another BGP speaker outside the local AS and when advertising routes within an AS.

For EBGP neighbors, the next-hop address corresponding to a BGP route does not resolve if the next-hop address is not the same as the neighbor IP address. The next-hop attribute also serves as a way to direct traffic to another BGP speaker, instead of waiting for a speaker to advertise. When a next-hop BGP neighbor is unreachable, the connection to that BGP neighbor goes down after the hold-down timer expiry.

When you enable `fast-external-fallover` and if the router has learned the routes from the BGP neighbor, the BGP session terminates immediately if the next-hop becomes unreachable—without waiting for the hold-down time.

Best path selection

Best path selection selects the best route out of all paths available for each destination, and records each selected route in the IP routing table for traffic forwarding. Only valid routes are considered for best path selection. BGP compares all paths, in the order in which they arrive, and selects the best paths. Paths for active routes are grouped in ascending order according to their neighboring external AS number.

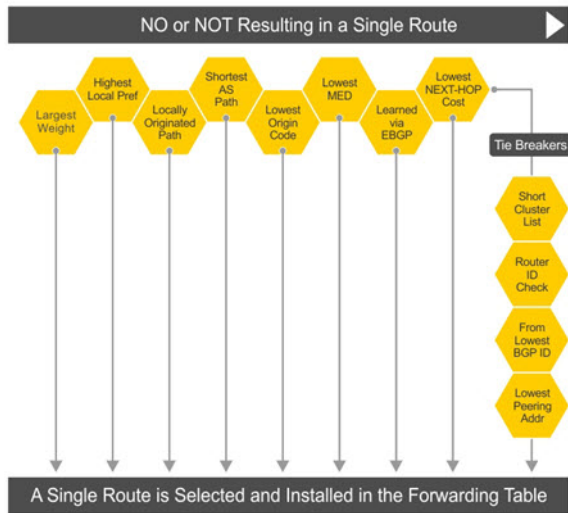
OS10 follows *deterministic* MED to select different best paths from a set of paths. This may depend on the order the different best paths are received from the neighbors — MED may or may not get compared between adjacent paths. BGP best path selection is deterministic by default.

The best path in each group is selected based on specific criteria—only one best path is selected at a time. If BGP receives more than one best path, it moves on to the next list of valid paths in the list, and continues until it reaches the end of the list.

When you configure the `non-deterministic-med` command, paths are compared in the order they arrive. OS10 follows this method to select different best paths from a set of paths, depending on the order they were received from the neighbors—MED may or may not get compared between the adjacent paths.

By default, the `bestpath as-path multipath-relax` command is disabled. This prevents BGP from load-balancing a learned route across two or more EBGP peers. To enable load-balancing across different EBGP peers, enter the `bestpath as-path multipath-relax` command.

If you configure the `bgp bestpath as-path ignore` command and the `bestpath as-path multipath-relax` command at the same time, an error message displays—only enable one command at a time.



More path support

More path (Add-Path) reduces convergence times by advertising multiple paths to its peers for the same address prefix without replacing existing paths with new ones. By default, a BGP speaker advertises only the best path to its peers for a given address prefix.

If the best path becomes unavailable, the BGP speaker withdraws its path from its local router information base (RIB) and recalculates a new best path. This situation requires both IGP and BGP convergence and is a lengthy process. BGP add-path also helps switch over to the next new best path when the current best path is unavailable.

The Add-Path capability to advertise more paths is supported only on IBGP peers—it is not supported on EBGP peers and BGP peer groups.

Ignore router ID calculations

Avoid unnecessary BGP best path transitions between external paths under certain conditions. The `bestpath router-id ignore` command reduces network disruption caused by routing and forwarding plane changes and allows for faster convergence.

Advertise cost

As the default process for redistributed routes, OS10 supports IGP cost as MED. Both auto-summarization and synchronization are disabled by default.

BGPv4 and BGPv6 support

- Deterministic MED, default
- A path with a missing MED is treated as worst path and assigned an `0xffffffff` MED value
- Delayed configuration at system boot — OS10 reads the entire configuration file BEFORE sending messages to start BGP peer sessions

4-Byte AS numbers

OS10 supports 4-byte AS number configurations by default. The 4-byte support is advertised as a new BGP capability - 4-BYTE-AS, in the OPEN message. A BGP speaker that advertises 4-Byte-AS capability to a peer, and receives the same from that peer must encode AS numbers as 4-octet entities in all messages.

If the AS number of the peer is different, the 4-byte speaker brings up the neighbor session using a reserved 2-byte ASN, 23456 called AS_TRANS. The AS_TRANS is used to interop between a 2-byte and 4-byte AS number.

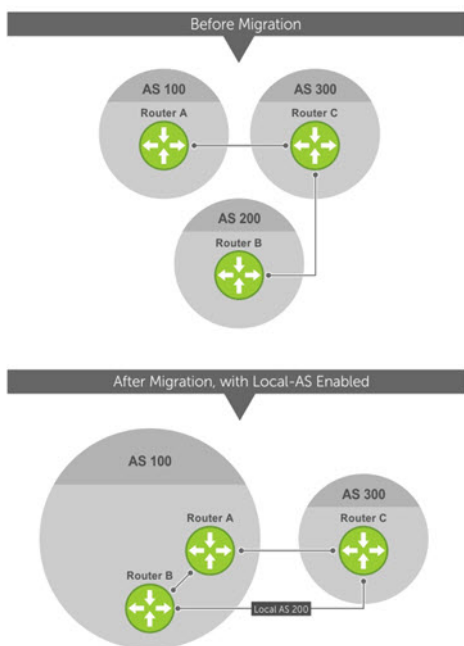
Where the 2-byte format is 1 to 65535, the 4-byte format is 1 to 4294967295. You can enter AS numbers using the traditional format.

AS number migration

You can transparently change the AS number of an entire BGP network. Changing the AS number ensures that the routes propagate throughout the network while migration is in progress. When migrating one AS to another and combining multiple AS, an EBGP network may lose its routing to an IBGP if the AS number changes.

Migration is difficult as all IBGP and EBGP peers of the migrating network must be updated to maintain network reachability. Local-AS allows the BGP speaker to operate as if it belongs to a virtual AS network besides its physical AS network.

Disable the local-as command after migration. Failure to disable the local-as command after migration causes the local-as command to replace the original AS number of the system. You must reconfigure the system with a new AS number.



Router A, Router B, and Router C belong to AS 100, 200, and 300, respectively. Router A acquired Router B — Router B has Router C as its client. When Router B is migrating to Router A, it must maintain the connection with Router C without immediately updating Router C's configuration. Local-AS allows Router B to appear as if it still belongs to Router B's old network, AS 200, to communicate with Router C.

The Local-AS does not prepend the updates with the AS number received from the EBGP peer if you use the `no prepend` command. If you do not select `no prepend`, the default, the Local-AS adds to the first AS segment in the AS-PATH. If you use an inbound route-map to prepend the AS-PATH to the update from the peer, the Local-AS adds first.

If Router B has an inbound route-map applied on Router C to prepend `65001 65002` to the AS-PATH, these events take place on Router B:

- Receive and validate the update.
- Prepend local-as 200 to AS-PATH.
- Prepend `65001 65002` to AS-PATH.

Local-AS prepends before the route map to give the appearance that the update passed through a router in AS 200 before it reaches Router B.

Configure Border Gateway Protocol

BGP is disabled by default. To enable the BGP process and start to exchange information, assign an AS number and use commands in ROUTER-BGP mode to configure a BGP neighbor.

BGP neighbor adjacency changes	All BGP neighbor changes are logged
Fast external fallover	Enabled
Graceful restart	Disabled
Local preference	100
4-byte AS	Enabled
MED	0
Route flap dampening parameters	<ul style="list-style-type: none"> • half-life = 15 minutes • max-suppress-time = 60 minutes • reuse = 750 • suppress = 2000
Timers	<ul style="list-style-type: none"> • keepalive = 60 seconds • holdtime = 180 seconds
Add-path	Disabled

Enable BGP

Before enabling BGP, assign a BGP router ID to the switch using the following command:

- In the ROUTER BGP mode, enter the `router-id ip-address` command. Where in, `ip-address` is the IP address corresponding to a configured L3 interface (physical, loopback, or LAG).

BGP is disabled by default. The system supports one AS number — you must assign an AS number to your device. To establish BGP sessions and route traffic, configure at least one BGP neighbor or peer. In BGP, routers with an established TCP connection are called *neighbors* or *peers*. After a connection establishes, the neighbors exchange full BGP routing tables with incremental updates afterward. Neighbors also exchange the KEEPALIVE messages to maintain the connection.

You can classify BGP neighbor routers or peers as internal or external. Connect EBGP peers directly, unless you enable EBGP multihop — IBGP peers do not need direct connection. The IP address of an EBGP neighbor is usually the IP address of the interface directly connected to the router. The BGP process first determines if all internal BGP peers are reachable, then it determines which peers outside the AS are reachable.

1. Assign an AS number, and enter ROUTER-BGP mode from CONFIGURATION mode (1 to 65535 for 2-byte, 1 to 4294967295 for 4-byte). Only one AS number is supported per system. If you enter a 4-byte AS number, 4-byte AS support is enabled automatically.

```
router bgp as-number
```

2. Enter a neighbor in ROUTER-BGP mode.

```
neighbor ip-address
```

3. Add a remote AS in ROUTER-NEIGHBOR mode, from 1 to 65535 for 2-byte or 1 to 4294967295 for 4-byte.

```
remote-as as-number
```

4. Enable the BGP neighbor in ROUTER-NEIGHBOR mode.

```
no shutdown
```

5. (Optional) Add a description text for the neighbor in ROUTER-NEIGHBOR mode.

```
description text
```

To reset the configuration when you change the configuration of a BGP neighbor, use the `clear ip bgp *` command. To view the BGP status, use the `show ip bgp summary` command.

Configure BGP

```
OS10# configure terminal
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 5.1.1.1
OS10(config-router-neighbor)# remote-as 1
OS10(config-router-neighbor)# description n1_abcd
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# template t1
OS10(config-router-template)# description peer_template_1_abcd
```

View BGP summary with 2-byte AS number

```
OS10# show ip bgp summary

BGP router identifier 202.236.164.86 local AS number 64901
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
120.10.1.1 64701 664 662 04:47:52 established 12000
```

View BGP summary with 4-byte AS number

```
OS10# show ip bgp summary
BGP router identifier 11.1.1.1, local AS number 4294967295
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
1 neighbor(s) using 8192 bytes of memory

Neighbor AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/Pfx
5.1.1.2 4294967295 0 0 0 0 0 00:00:00 Active
```

For the router ID, the system selects the first configured IP address or a random number. To view the status of BGP neighbors, use the `show ip bgp neighbors` command. For BGP neighbor configuration information, use the `show running-config bgp` command.

The example shows two neighbors — one is an external BGP neighbor, and the other is an internal BGP neighbor. The first line of the output for each neighbor displays the AS number and states if the link is external or internal.

The third line of the `show ip bgp neighbors` output contains the BGP state. If anything other than *established* displays, the neighbor is not exchanging information and routes - see IPv6 commands for more information.

View BGP neighbors

```
OS10# show ip bgp neighbors
BGP neighbor is 5.1.1.1, remote AS 1, internal link
BGP version 4, remote router ID 6.1.1.1
BGP state established, in this state for 00:03:11
Last read 01:08:40 seconds, hold time is 180, keepalive interval is 60 seconds
Received 11 messages
3 opens, 1 notifications, 3 updates
4 keepalives, 0 route refresh requests
Sent 14 messages
3 opens, 1 notifications, 0 updates
10 keepalives, 0 route refresh requests

Minimum time between advertisement runs is 0 seconds
Description: n1_abcd
Capabilities received from neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)ROUTE_REFRESH(2)CISCO_ROUTE_REFRESH(128)
Capabilities advertised to neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)ROUTE_REFRESH(2)CISCO_ROUTE_REFRESH(128)

Prefixes accepted 3, Prefixes advertised 0

Connections established 3; dropped 2
Closed by neighbor sent 00:03:26 ago

Local host: 5.1.1.2, Local port: 43115
Foreign host: 5.1.1.1, Foreign port: 179
```

View BGP running configuration

```
OS10# show running-configuration bgp
!
router bgp 100
!
 neighbor 5.1.1.1
 description n1_abcd
```

Configuring BGP in a non-default VRF instance

To configure BGP in a non-default VRF instance.

1. Assign an AS number, and enter ROUTER-BGP mode from CONFIGURATION mode (1 to 65535 for 2-byte, 1 to 4294967295 for 4-byte). Only one AS number is supported per system. If you enter a 4-byte AS number, 4-byte AS support is enabled automatically.

```
router bgp as-number
```

2. Enter ROUTER-BGP-VRF mode to configure BGP in a non-default VRF instance.

```
vrf vrf-name
```

3. Enter a neighbor in CONFIG-ROUTER-VRF mode.

```
neighbor ip-address
```

4. Add a remote AS in ROUTER-NEIGHBOR mode, from 1 to 65535 for 2-byte or 1 to 4294967295 for 4-byte.

```
remote-as as-number
```

5. Enable the BGP neighbor in ROUTER-NEIGHBOR mode.

```
no shutdown
```

6. (Optional) Add a description text for the neighbor in ROUTER-NEIGHBOR mode.

```
description text
```

To reset the configuration when you change the configuration of a BGP neighbor, use the `clear ip bgp *` command. To view the BGP status, use the `show ip bgp summary` command.

Configure BGP

```
OS10# configure terminal
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# vrf blue
OS10(config-router-vrf)# neighbor 5.1.1.1
OS10(config-router-neighbor)# remote-as 1
OS10(config-router-neighbor)# description n1_abcd
OS10(config-router-neighbor)# exit
OS10(config-router-vrf)# template t1
OS10(config-router-template)# description peer_template_1_abcd
```

Configure Dual Stack

OS10 supports dual stack for BGPv4 and BGPv6. Dual stack BGP allows simultaneous exchange of same IPv4 or IPv6 prefixes through different IPv4 and IPv6 peers. You can enable dual stack using the `activate` command in the corresponding address-family mode. By default, `activate` command is enabled for the IPv4 address family for all the neighbors.

If a BGP-v4 neighbor wants to carry ipv6 prefix information, it activates the IPv6 address-family. For a BGP-v6 neighbor to carry ipv4 prefix, it activates the IPv4 address-family.

1. Enable support for the IPv6 unicast family in CONFIG-ROUTER-BGP mode.

```
address family ipv6 unicast
```


2. Enable IPv6 unicast support on a BGP neighbor/template in CONFIG-ROUTER-BGP-AF mode.

```
activate
```

Peer templates

To configure multiple BGP neighbors at one time, you can create and populate a BGP peer template. An advantage of configuring peer templates is that members of a peer template inherit the configuration properties of the template and share update policy. Always create a peer template and assign a name to it before adding members to the peer template. Create a peer template before configuring any route policies for the template.

NOTE: An outbound filter policy, distribute list or route map, is not supported on a peer group member.

1. Enable BGP, and assign the AS number to the local BGP speaker in CONFIGURATION mode, from 1 to 65535 for 2 byte, 1 to 4294967295 | 0.1 to 65535.65535 for 4 byte, or 0.1 to 65535.65535 in dotted format.

```
router bgp as-number
```

2. Create a peer template by assigning a neighborhood name to it in ROUTER-BGP mode.

```
template template-name
```

3. Add a neighbor as a remote AS in ROUTER-TEMPLATE mode, from 1 to 65535 for 2 byte, 1 to 4294967295 | 0.1 to 65535.65535 for 4 byte, or 0.1 to 65535.65535 in dotted format.

```
neighbor ip-address
```

4. Add a remote neighbor, and enter the AS number in ROUTER-TEMPLATE mode.

```
remote-as as-number
```

- To add an EBGP neighbor, configure the `as-number` parameter with a number different from the BGP `as-number` configured in the `router bgp as-number` command.
- To add an IBGP neighbor, configure the `as-number` parameter with the same BGP `as-number` configured in the `router bgp as-number` command.

5. (Optional) Add a text description for the template in ROUTER-TEMPLATE mode.

```
description text
```

6. Assign a peer-template with a peer-group name from which to inherit to the neighbor in ROUTER-NEIGHBOR mode.

```
inherit template template-name
```

7. Enable the neighbor in ROUTER-BGP mode.

```
neighbor ip-address
```

8. Enable the peer-group in ROUTER-NEIGHBOR mode.

```
no shutdown
```

When you add a peer to a peer group, it inherits all the peer group configured parameters. When you disable a peer group, all the peers within the peer template that are in the Established state move to the Idle state. A neighbor cannot become a part of a peer group if it has any of these commands configured:

- `advertisement-interval`
- `next-hop-self`
- `route-map out`
- `route-reflector-client`
- `send-community`

A neighbor may keep its configuration after it is added to a peer group if the neighbor configuration is more specific than the peer group and if the neighbor configuration does not affect outgoing updates.

To display the peer-group configuration assigned to a BGP neighbor, enter the `show ip bgp peer-group peer-group-name` command. The `show ip bgp neighbor` command output does not display peer-group configurations.

Configure peer templates

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300)# template ebgppg
OS10(config-router-template)# remote-as 100
OS10(config-router-template)# description peer_template_1_abcd
OS10(config-router-template)# exit
OS10(config-router-bgp-300)# neighbor 3.1.1.1
OS10(config-router-neighbor)# inherit template ebgppg
OS10(config-router-neighbor)# no shutdown
```

View peer group status

```
OS10(config-router-neighbor)# do show ip bgp peer-group ebgppg
Peer-group ebgppg, remote AS 100
  BGP version 4
  Minimum time between advertisement runs is 30 seconds
  Description: peer_template_1_abcd
  For address family: Unicast
  BGP neighbor is ebgppg, peer-group external
  Update packing has 4_OCTET_AS support enabled

Number of peers in this group 1
Peer-group members:
```

View running configuration

```
OS10(config-router-neighbor)# do show running-configuration bgp
!
router bgp 300
!
neighbor 3.1.1.1
inherit template ebgppg
no shutdown
!
template ebgppg
remote-as 100
description peer_template_1_abcd
```

Peer templates for a non-default VRF instance

You can create peer templates to add multiple neighbors at a time to the non-default VRF instance that you create.

1. Enable BGP, and assign the AS number to the local BGP speaker in CONFIGURATION mode, from 1 to 65535 for 2 byte, 1 to 4294967295 | 0.1 to 65535.65535 for 4 byte, or 0.1 to 65535.65535 in dotted format.

```
router bgp as-number
```

2. Enter the CONFIG-ROUTER-VRF mode to create a peer template for the non-default VRF instance that you create.

```
vrf vrf-name
```

3. Create a peer template by assigning a neighborhood name to it in CONFIG-ROUTER-VRF mode.

```
template template-name
```

4. Add a neighbor as a remote AS in ROUTER-TEMPLATE mode, from 1 to 65535 for 2 byte, 1 to 4294967295 | 0.1 to 65535.65535 for 4 byte, or 0.1 to 65535.65535 in dotted format.

```
neighbor ip-address
```

5. Add a remote neighbor, and enter the AS number in ROUTER-TEMPLATE mode.

```
remote-as as-number
```

- To add an EBGp neighbor, configure the *as-number* parameter with a number different from the BGP *as-number* configured in the `router bgp as-number` command.

- To add an IBGP neighbor, configure the `as-number` parameter with the same BGP as-number configured in the `router bgp as-number` command.

6. (Optional) Add a text description for the template in ROUTER-TEMPLATE mode.

```
description text
```

7. Assign a peer-template with a peer-group name from which to inherit to the neighbor in ROUTER-NEIGHBOR mode.

```
inherit template template-name
```

8. Enable the neighbor in ROUTER-BGP mode.

```
neighbor ip-address
```

9. Enable the peer-group in ROUTER-NEIGHBOR mode.

```
no shutdown
```

When you add a peer to a peer group, it inherits all the peer group configured parameters. When you disable a peer group, all the peers within the peer template that are in the Established state move to the Idle state. A neighbor cannot become a part of a peer group if it has any of these commands configured:

- `advertisement-interval`
- `next-hop-self`
- `route-map out`
- `route-reflector-client`
- `send-community`

A neighbor may keep its configuration after it is added to a peer group if the neighbor configuration is more specific than the peer group and if the neighbor configuration does not affect outgoing updates.

To display the peer-group configuration assigned to a BGP neighbor, enter the `show ip bgp peer-group peer-group-name` command. The `show ip bgp neighbor` command output does not display peer-group configurations.

Configure peer templates

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300) vrf blue
OS10(config-router-vrf)# template ebgppg
OS10(config-router-template)# remote-as 100
OS10(config-router-template)# description peer_template_1_abcd
OS10(config-router-template)# exit
OS10(config-router-vrf)# neighbor 3.1.1.1
OS10(config-router-neighbor)# inherit template ebgppg
OS10(config-router-neighbor)# no shutdown
```

Neighbor fall-over

The BGP neighbor fall-over feature reduces the convergence time while maintaining stability. When you enable fall-over, BGP tracks IP reachability to the peer remote address and the peer local address.

When remote or peer local addresses become unreachable, BGP brings the session down with the peer. For example, if no active route exists in the routing table for peer IPv6 destinations/local address, BGP brings the session down.

By default, the hold time governs a BGP session. Configure BGP fast fall-over on a per-neighbor or peer-group basis. BGP routers typically carry large routing tables as frequent session resets are not desirable. If fall-over is enabled, the connection to an internal BGP peer is immediately reset if the host route added to reach the internal peer fails.

1. Enter the neighbor IP address in ROUTER-BGP mode.

```
neighbor ip-address
```

2. Disable fast fall-over in ROUTER-NEIGHBOR mode.

```
no fall-over
```

3. Enter the neighbor IP address in ROUTER-BGP mode.

```
neighbor ip-address
```

4. Enable BGP fast fall-Over in ROUTER-NEIGHBOR mode.

```
fall-over
```

Configure neighbor fall-over

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 3.1.1.1
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# fall-over
OS10(config-router-neighbor)# no shutdown
```

Verify neighbor fall-over on neighbor

```
OS10(config-router-neighbor)# do show ip bgp neighbors 3.1.1.1
BGP neighbor is 3.1.1.1, remote AS 100, local AS 100 internal link

BGP version 4, remote router ID 3.3.3.33
BGP state ESTABLISHED, in this state for 00:17:17
Last read 00:27:54 seconds
Hold time is 180, keepalive interval is 60 seconds
Configured hold time is 180, keepalive interval is 60 seconds
Fall-over enabled

Received 23 messages
  1 opens, 0 notifications, 1 updates
 21 keepalives, 0 route refresh requests
Sent 21 messages
  1 opens, 0 notifications, 0 updates
 20 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds
Capabilities received from neighbor for IPv4 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)
  4_OCTET_AS(65)
Capabilities advertised to neighbor for IPv4 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)
  4_OCTET_AS(65)
Prefixes accepted 3, Prefixes advertised 0
Connections established 1; dropped 0
Last reset never
For address family: IPv4 Unicast
  Allow local AS number 0 times in AS-PATH attribute
Prefixes ignored due to:
  Martian address 0, Our own AS in AS-PATH 0
  Invalid Nexthop 0, Invalid AS-PATH length 0
  Wellknown community 0, Locally originated 0

For address family: IPv6 Unicast
  Allow local AS number 0 times in AS-PATH attribute
Local host: 3.1.1.3, Local port: 58633
Foreign host: 3.1.1.1, Foreign port: 179
```

Verify neighbor fall-over on peer-group

```
OS10# show running-configuration

!
router bgp 102
!
address-family ipv4 unicast
  aggregate-address 6.1.0.0/16
!
```

```

neighbor 40.1.1.2
  inherit template bgppg
  no shutdown
!
neighbor 60.1.1.2
  inherit template bgppg
  no shutdown
!
neighbor 32.1.1.2
  remote-as 100
  no shutdown
!
template bgppg
  fall-over
  remote-as 102
!

```

Configure password

You can enable message digest 5 (MD5) authentication with a password on the TCP connection between two BGP neighbors.

Configure the same password on both BGP peers. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection. Configuring a password for a neighbor establishes a new connection.

Configure password

- Configure the password in both the BGP peers using the `password {9 encrypted password-string|password-string}` in ROUTER-NEIGHBOR CONFIGURATION or ROUTER-TEMPLATE CONFIGURATION mode. . The password provided in ROUTER-NEIGHBOR mode gets more preference than the password in ROUTER-TEMPLATE mode. You can enter the password either as plain text or in encrypted format.
- View the password configuration using the `show configuration` command.

Example configuration in Peer 1

ROUTER-NEIGHBOR mode

```

OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# ip address 11.1.1.1/24
OS10(config-if-eth1/1/5)# router bgp 10
OS10(config-router-bgp-10)# neighbor 11.1.1.2
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# remote-as 10
OS10(config-router-neighbor)# password abcdell

```

ROUTER-TEMPLATE mode

```

OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# ip address 11.1.1.1/24
OS10(config-if-eth1/1/5)# router bgp 10
OS10(config-router-bgp-10)# template pass
OS10(config-router-template)# password 9
f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
OS10(config-router-template)# exit
OS10(config-router-bgp-10)# neighbor 11.1.1.2
OS10(config-router-neighbor)# inherit template pass

```

View password configuration in peer 1

```

OS10(config-router-neighbor)# show configuration
!
neighbor 11.1.1.2
  password 9 0fbelad397712f74f4df903b4ff4b7b6e22cc377180432d7523a70d403d41565

```

```
remote-as 10
no shutdown
```

```
OS10(config-router-neighbor)# do show running-configuration bgp
!
router bgp 10
!
  template pass
  password 9 f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
!
  neighbor 11.1.1.2
  inherit template pass
  password 9 01320afb39f49134882b0a9814fe6e8e228f616f60a35958844775314c00f0e5
  remote-as 10
  no shutdown
```

Example configuration in Peer 2

ROUTER-NEIGHBOR mode

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(config-if-eth1/1/5)# no switchport
ip OS10(config-if-eth1/1/5)# ip address 11.1.1.2/24
OS10(config-if-eth1/1/5)# router bgp 20
OS10(config-router-bgp-20)# neighbor 11.1.1.1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# remote-as 20
OS10(config-router-neighbor)# password abcdell
```

ROUTER-TEMPLATE mode

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# ip address 11.1.1.2/24
OS10(config-if-eth1/1/5)# router bgp 20
OS10(config-router-bgp-20)# template pass
OS10(config-router-template)# password 9
f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
OS10(config-router-template)# exit
OS10(config-router-bgp-20)# neighbor 11.1.1.1
OS10(config-router-neighbor)# inherit template pass
```

View password configuration in peer 2

```
OS10(config-router-neighbor)# show configuration
!
neighbor 11.1.1.1
  password 9 0fbelad397712f74f4df903b4ff4b7b6e22cc377180432d7523a70d403d41565
  remote-as 20
  no shutdown
```

```
OS10(config-router-neighbor)# do show running-configuration bgp
!
router bgp 20
  neighbor 11.1.1.2
  password 9 f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
  remote-as 20
  no shutdown
```

Fast external fallover

Fast external fallover terminates EBGP sessions of any directly adjacent peer if the link used to reach the peer goes down. BGP does not wait for the hold-down timer to expire.

Fast external fallover is enabled by default. To disable or re-enable it, use the [no] `fast-external-fallover` command. For the `fast-external-fallover` command to take effect on an established BGP session, you must reset the session using the `clear ip bgp {* | peer-ipv4-address | peer-ipv6-address}` command.

View fast external fallover configuration

```
OS10(config)# do show running-configuration bgp
!
router bgp 300
!
neighbor 3.1.1.1
  remote-as 100
  no shutdown
!
neighbor 3::1
  remote-as 100
  no shutdown
!
address-family ipv6 unicast
  activate
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
  ip address 3.1.1.3/24
  no switchport
  no shutdown
  ipv6 address 3::3/64
OS10(conf-if-eth1/1/1)# shutdown
OS10(conf-if-eth1/1/1)# do show ip bgp summary
BGP router identifier 11.11.11.11 local AS number 300
Neighbor          AS              MsgRcvd    MsgSent
Up/Down           State/Pfx
3.1.1.1           100             6           6
00:00:15         Active
3::1              100             8           11
00:00:15         Active
OS10(conf-if-eth1/1/1)#
```

View fast external fallover unconfiguration

```
OS10(config-router-bgp-300)# do show running-configuration bgp
!
router bgp 300
  no fast-external-fallover
!
neighbor 3.1.1.1
  remote-as 100
  no shutdown
!
neighbor 3::1
  remote-as 100
  no shutdown
!
address-family ipv6 unicast
  activate
OS10(config-router-bgp-300)#
OS10(conf-if-eth1/1/1)# do clear ip bgp *
OS10# show ip bgp summary
BGP router identifier 11.11.11.11 local AS number 300
Neighbor  AS              MsgRcvd    MsgSent    Up/Down    State/Pfx
-----
3.1.1.1   100             7           4          00:00:08   3
3::1     100             9           5          00:00:08   4
OS10#
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# shutdown
OS10(conf-if-eth1/1/1)# do show ip bgp summary
BGP router identifier 11.11.11.11 local AS number 300
Neighbor  AS              MsgRcvd    MsgSent    Up/Down    State/Pfx
-----
3.1.1.1   100             7           4          00:00:29   3
```

```

3::1      100      9          5          00:00:29    4
OS10(conf-if-eth1/1/1)#
OS10(config-router-bgp-neighbor-af)# Apr 27 01:39:03 OS10 dn_sm[2065]: Node.1-
Unit.1:PRI:alert [os10:event],
%Dell EMC (OS10) %BGP_NBR_BKWD_STATE_CHG: Backward state change occurred Hold Time
expired for Nbr:3.1.1.3 VRF:default
Apr 27 01:39:03 OS10 dn_sm[2065]: Node.1-Unit.1:PRI:alert [os10:event], %Dell EMC
(OS10) %BGP_NBR_BKWD_STATE_CHG: Backward
state change occurred Hold Time expired for Nbr:3::3 VRF:default

```

Passive peering

When you enable a peer-template, the system sends an OPEN message to initiate a TCP connection. If you enable passive peering for the peer template, the system does not send an OPEN message but responds to an OPEN message.

When a BGP neighbor connection with authentication rejects a passive peer-template, the system prevents another passive peer-template on the same subnet from connecting with the BGP neighbor. To work around this constraint, change the BGP configuration or change the order of the peer template configuration.

You can restrict the number of passive sessions the neighbor accepts using the `limit` command.

1. Enable BGP, and assign the AS number to the local BGP speaker in CONFIGURATION mode (1 to 65535 for 2-byte, 1 to 4294967295 for 4-byte).

```
router bgp as-number
```

2. Configure a template that does not initiate TCP connections with other peers in ROUTER-BGP mode (up to 16 characters).

```
template template-name
```

3. Create and enter the AS number for the remote neighbor in ROUTER-BGP-TEMPLATE mode (1 to 4294967295).

```
remote-as as-number
```

4. Enable peer listening and enter the maximum dynamic peers count in ROUTER-BGP-TEMPLATE mode (1 to 4294967295).

```
listen neighbor ip-address limit
```

Only after the peer template responds to an OPEN message sent on the subnet does the state of its BGP change to ESTABLISHED. After the peer template is ESTABLISHED, the peer template is the same as any other peer template, see [Peer templates](#).

If you do not configure a BGP device in Peer-Listening mode, a session with a dynamic peer comes up. Passwords are not supported on BGPv4/v6 dynamic peers.

Configure passive peering

```

OS10(config)# router bgp 10
OS10(conf-router-bgp-10)# template bgppg
OS10(conf-router-template)# remote-as 100
OS10(conf-router-template)# listen 32.1.0.0/8 limit 10

```

Local AS

During BGP network migration, you can maintain existing AS numbers. Reconfigure your routers with the new information to disable after the migration. Network migration is not supported on passive peer templates. You must configure [Peer templates](#) before assigning it to an AS.

1. Enter a neighbor IP address, A.B.C.D, in ROUTER-BGP mode.

```
neighbor ip-address
```

2. Enter a local-as number for the peer, and the AS values not prepended to announcements from the neighbors in ROUTER-NEIGHBOR mode (1 to 4294967295).

```
local-as as number [no prepend]
```


- Return to ROUTER-BGP mode.

```
exit
```

- Enter a template name to assign to the peer-groups in ROUTER-BGP mode (up to 16 characters).

```
template template-name
```

- Enter a local-as number for the peer in ROUTER-TEMPLATE mode.

```
local-as as number [no prepend]
```

- Add a remote AS in ROUTER-TEMPLATE mode (1 to 65535 for 2 bytes, 1 to 4294967295 for 4 bytes).

```
remote-as as-number
```

Allow external routes from neighbor

```
OS10(config)# router bgp 10
OS10(conf-router-bgp-10)# neighbor 32.1.1.2
OS10(conf-router-neighbor)# local-as 50
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-10)# template bgppg1
OS10(conf-router-template)# fall-over
OS10(conf-router-template)# local-as 400
OS10(conf-router-template)# remote-as 102
```

Local AS number disabled

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# neighbor 32.1.1.2
OS10(conf-router-neighbor)# no local-as 100
```

AS number limit

Sets the number of times an AS number occurs in an AS path. The `allow-as` parameter permits a BGP speaker to allow the AS number for a configured number of times in the updates received from the peer.

The AS-PATH loop is detected if the local AS number is present more than the number of times in the command.

- Enter the neighbor IP address to use the AS path in ROUTER-BGP mode.

```
neighbor ip address
```

- Enter Address Family mode in ROUTER-NEIGHBOR mode.

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

- Allow the neighbor IP address to use the AS path the specified number of times in ROUTER-BGP-NEIGHBOR-AF mode (1 to 10).

```
allowas-in number
```

Configure AS number appearance

```
OS10(config)# router bgp 10
OS10(conf-router-bgp-10)# neighbor 1.1.1.2
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# allowas-in 5
```

View AS numbers in AS paths

```
OS10# show running-configuration bgp
!
router bgp 101
  no fast-external-fallover
!
address-family ipv4 unicast
```

```

dampening
!
neighbor 17.1.1.2
  remote-as 102
  no shutdown
!
address-family ipv4 unicast
  allowas-in 4

```

Show IP BGP

```

OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172:16:1::2
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv6 unicast
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# end
OS10# show running-configuration bgp
!
router bgp 100
!
neighbor 172:16:1::2
  remote-as 100
  no shutdown
!
address-family ipv6 unicast
  activate
  allowas-in 1
OS10# show ip bgp
BGP local RIB : Routes to be Added , Replaced , Withdrawn
BGP local router ID is 100.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed/network, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

```

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>I	55::/64	172:16:1::2	0	0	0	100 200 300 400
i						
*>I	55:0:0:1::/64	172:16:1::2	0	0	0	100 200 300 400
i						
*>I	55:0:0:2::/64	172:16:1::2	0	0	0	100 200 300 400
i						

Redistribute routes

Add routes from other routing instances or protocols to the BGP process. You can include OSPF, static, or directly connected routes in the BGP process with the `redistribute` command.

- Include directly connected or user-configured (static) routes in ROUTER-BGP-AF mode.

```
redistribute {connected | static}
```

- Include specific OSPF routes in IS-IS in ROUTER-BGP-AF mode (1 to 65535).

```
redistribute ospf process-id
```

Disable redistributed routes

```
OS10(conf-router-bgp-af)# no redistribute ospf route-map ospf-to-bgp
```

Enable redistributed routes

```
OS10(conf-router-bgp-af)# redistribute ospf
```

Additional paths

The `add-path` command is disabled by default.

1. Assign an AS number in CONFIGURATION mode.

```
router bgp as-number
```

2. Enter a neighbor and IP address (A.B.C.D) in ROUTER-BGP mode.

```
neighbor ip-address
```

3. Enter Address Family mode in ROUTER-NEIGHBOR mode.

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

4. Allow the specified neighbor to send or receive multiple path advertisements in ROUTER-BGP mode. The `count` parameter controls the number of paths that are advertised — not the number of paths received.

```
add-path [both | received | send] count
```

Enable additional paths

```
OS10(config)# router bgp 102
OS10(config-router-bgp-102)# neighbor 32.1.1.2
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# add-path both 3
```

MED attributes

OS10 uses the MULTI_EXIT_DISC or MED attribute when comparing EBGP paths from the same AS. MED comparison is not performed in paths from neighbors with different AS numbers.

1. Enable MED comparison in the paths from neighbors with different AS in ROUTER-BGP mode.

```
always-compare-med
```

2. Change the best path MED selection in ROUTER-BGP mode.

```
bestpath med {confed | missing-as-best}
```

- `confed`—Selects the best path MED comparison of paths learned from BGP confederations.
- `missing-as-best`—Treats a path missing an MED as the most preferred one.
- `missing-as-worst`—Treats a path missing an MED as the least preferred one.

Modify MED attributes

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# always-compare-med
OS10(config-router-bgp-100)# bestpath med confed
```

Local preference attribute

You can change the value of the LOCAL_PREFERENCE attributes for all routes the router receives. To change the LOCAL_PREF value in ROUTER-BGP mode from 0 to 4294967295 with default 100, use the `default local preference value` command.

To view the BGP configuration, use the `show running-configuration` command. A more flexible method for manipulating the LOCAL_PREF attribute value is to use a route-map.

1. Assign a name to a route map in CONFIGURATION mode.

```
route-map map-name {permit | deny | sequence-number}
```

2. Change the LOCAL_PREF value for routes meeting the criteria of this route map in ROUTE-MAP mode, then return to CONFIGURATION mode.

```
set local-preference value
exit
```

3. Enter ROUTER-BGP mode.

```
router bgp as-number
```

4. Enter the neighbor to apply the route map configuration in ROUTER-BGP mode.

```
neighbor {ip-address}
```

5. Apply the route map to the neighbor's incoming or outgoing routes in ROUTER-BGP-NEIGHBOR-AF mode.

```
route-map map-name {in | out}
```

6. Enter the peer group to apply the route map configuration in ROUTER-BGP mode.

```
template template-name
```

7. Apply the route map to the peer group's incoming or outgoing routes in CONFIG-ROUTER-TEMPLATE-AF mode.

```
route-map map-name {in | out}
```

Configure and view local preference attribute

```
OS10(config)# route-map bgproutemap 1
OS10(conf-route-map)# set local-preference 500
OS10(conf-route-map)# exit
OS10(config)# router bgp 10
OS10(conf-router-bgp-10)# neighbor 10.1.1.4
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# route-map bgproutemap in
```

```
OS10 configure terminal
OS10(config)# route-map bgproutemap 1
OS10(conf-route-map)# set local-preference 500
OS10(conf-route-map)# exit
OS10(config)# router bgp 64601
OS10(conf-router-bgp-64601)# template bgppg
OS10(conf-router-template)# address-family ipv4 unicast
OS10(conf-router-bgp-template-af)# route-map bgproutemap in
```

View route-map

```
OS10(conf-route-map)# do show route-map
route-map bgproutemap, permit, sequence 1
Match clauses:
Set clauses:
  local-preference 500
  metric 400
  origin incomplete
```

Weight attribute

Influence the BGP routing based on the weight value. Routes with a higher weight value have preference when multiple routes to the same destination exist.

1. Assign a weight to the neighbor connection in ROUTER-BGP mode.

```
neighbor {ip-address}
```

2. Set a weight value for the route in ROUTER-NEIGHBOR mode (1 to 4294967295, default 0).

```
weight weight
```

- Return to ROUTER-BGP mode.

```
exit
```

- Assign a weight value to the peer-group in ROUTER-BGP mode.

```
template template name
```

- Set a weight value for the route in ROUTER-TEMPLATE mode.

```
weight weight
```

Modify weight attribute

```
OS10(config)# router bgp 10
OS10(config-router-bgp-10)# neighbor 10.1.1.4
OS10(config-router-neighbor)# weight 400
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-10)# template zanzibar
OS10(config-router-template)# weight 200
```

Enable multipath

You can have one path to a destination by default, and enable multipath to allow up to 64 parallel paths to a destination. The `show ip bgp network` command includes multipath information for that network.

- Enable multiple parallel paths in ROUTER-BGP mode.

```
maximum-paths {ebgp | ibgp} number
```

Enable multipath

```
OS10(config)# router bgp 10
OS10(config-router-bgp-10)# maximum-paths ebgp 10
```

Route-map filters

Filtering routes allows you to implement BGP policies. Use route-maps to control which routes the BGP neighbor or peer group accepts and advertises.

- Enter the neighbor IP address to filter routes in ROUTER-BGP mode.

```
neighbor ipv4-address
```

- Enter Address Family mode in ROUTER-NEIGHBOR mode.

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

- Create a route-map and assign a filtering criteria in ROUTER-BGP-NEIGHBOR-AF mode, then return to CONFIG-ROUTER-BGP mode.

```
route-map map-name {in | out}
exit
```

- `in`—Enter a filter for incoming routing updates.
 - `out`—Enter a filter for outgoing routing updates.
- Enter a peer template name in ROUTER-BGP mode.

```
template template-name
```

- Enter Address Family mode.

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

6. Create a route-map, and assign a filtering criteria in ROUTER-BGP-TEMPLATE-AF mode.

```
route-map map-name {in | out}
```

Filter BGP route

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# neighbor 40.1.1.2
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# route-map metro in
OS10(conf-router-bgp-neighbor-af)# exit
OS10(conf-router-bgp-102)# template ebgp
OS10(conf-router-template)# address-family ipv4 unicast
OS10(conf-router-bgp-template-af)# route-map metro in
```

Route reflector clusters

BGP route reflectors are intended for ASs with a large mesh. They reduce the amount of BGP control traffic. With route reflection configured properly, IBGP routers are not fully meshed within a cluster but all receive routing information.

Configure clusters of routers where one router is a concentration router and the others are clients who receive their updates from the concentration router.

1. Assign an ID to a router reflector cluster in ROUTER-BGP mode. You can have multiple clusters in an AS.

```
cluster-id cluster-id
```

2. Assign a neighbor to the router reflector cluster in ROUTER-BGP mode.

```
neighbor {ip-address}
```

3. Configure the neighbor as a route-reflector client in ROUTER-NEIGHBOR mode, then return to ROUTER-BGP mode.

```
route-reflector-client
exit
```

4. Assign a peer group template as part of the route-reflector cluster in ROUTER-BGP mode.

```
template template-name
```

5. Configure the template as the route-reflector client in ROUTER-TEMPLATE mode.

```
route-reflector-client
```

When you enable a route reflector, the system automatically enables route reflection to all clients. To disable route reflection between all clients in this reflector, use the `no bgp client-to-client reflection` command in ROUTER-BGP mode. You must fully mesh all the clients before you disable route reflection.

Configure BGP route reflector

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# cluster-id 4294967295
OS10(conf-router-bgp-102)# neighbor 32.1.1.2
OS10(conf-router-neighbor)# route-reflector-client
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-102)# template zanzibar
OS10(conf-router-template)# route-reflector-client
```

Aggregate routes

OS10 provides multiple ways to aggregate routes in the BGP routing table. At least one route of the aggregate must be in the routing table for the configured aggregate route to become active. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

1. Assign an AS number in CONFIGURATION mode.

```
router bgp as-number
```

2. Enter Address Family mode in ROUTER-BGP mode.

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

3. to aggregate in ROUTER-BGPv4-AF mode.

```
aggregate-address ip-address mask
```

Configure aggregate routes

```
OS10(config)# router bgp 105
OS10(conf-router-bgp-105)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# aggregate-address 3.3.0.0/16
```

View running configuration

```
OS10(conf-router-bgpv4-af)# do show running-configuration bgp
! Version
! Last configuration change at Jul 27 06:51:17 2016
!
!
router bgp 105
!
 address-family ipv4 unicast
  aggregate-address 3.3.0.0/16
!

neighbor 32.1.1.2
 remote-as 104
 no shutdown
!
 address-family ipv4 unicast
```

Confederations

Another way to organize routers within an AS and reduce the mesh for IBGP peers is to configure BGP confederations. As with route reflectors, Dell EMC recommends BGP confederations only for IBGP peering involving many IBGP peering sessions per router.

When you configure BGP confederations, you break the AS into smaller sub-ASs. To devices outside your network, the confederations appear as one AS. Within the confederation sub-AS, the IBGP neighbors are fully meshed and the MED, NEXT_HOP, and LOCAL_PREF attributes maintain between confederations.

1. Enter the confederation ID AS number in ROUTER-BGP mode (1 to 65535 for 2-byte, 1 to 4294967295 for 4-byte).

```
confederation identifier as-number
```

2. Enter which confederation sub-AS are peers in ROUTER-BGP mode, from 1 to 65535 for 2-byte, 1 to 4294967295 for 4-byte. All Confederation routers must be either 4 bytes or 2 bytes. You cannot have a mix of router ASN support.

```
confederation peers as-number [... as-number]
```

Configure BGP confederations

```
OS10(config)# router bgp 65501
OS10(conf-router-bgp-65501)# confederation identifier 100
OS10(conf-router-bgp-65501)# confederation peers 65502 65503 65504
OS10(conf-router-bgp-65501)# neighbor 1.1.1.2
OS10(conf-router-neighbor)# remote-as 65502
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-65501)# neighbor 2.1.1.2
OS10(conf-router-neighbor)# remote-as 65503
OS10(conf-router-neighbor)# no shutdown
```

```

OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-65501)# neighbor 3.1.1.2
OS10(conf-router-neighbor)# remote-as 65504
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-65501)# end
OS10# show running-configuration bgp
!
router bgp 65501
 confederation identifier 100
 confederation peers 65502 65503 65504
!
 neighbor 1.1.1.2
  remote-as 65502
  no shutdown
!
 neighbor 2.1.1.2
  remote-as 65503
  no shutdown
!
 neighbor 3.1.1.2
  remote-as 65504
  no shutdown

```

Route dampening

When EBGP routes become unavailable, they “flap” and the router issues both WITHDRAWN and UPDATE notices. A flap occurs when a route is withdrawn, readvertised after being withdrawn, or has an attribute change.

The constant router reaction to the WITHDRAWN and UPDATE notices causes instability in the BGP process. To minimize this instability, configure penalties (a numeric value) for routes that flap. When that penalty value reaches a configured limit, the route is not advertised, even if the route is up, the penalty value is 1024.

As time passes and the route does not flap, the penalty value decrements or decays. If the route flaps again, it is assigned another penalty. The penalty value is cumulative and adds underwithdraw, readvertise, or attribute change.

When dampening applies to a route, its path is described by:

History entry Entry that stores information on a downed route.

Dampened path Path that is no longer advertised.

Penalized path Path that is assigned a penalty.

1. Enable route dampening in ROUTER-BGP mode.

```
dampening [half-life | reuse | max-suppress-time]
```

- *half-life* — Number of minutes after which the penalty decreases (1 to 45, default 15). After the router assigns a penalty of 1024 to a route, the penalty decreases by half after the half-life period expires.
- *reuse* — Number compares to the flapping route’s penalty value. If the penalty value is less than the reuse value, the flapping route again advertises or is no longer suppressed (1 to 20000, default 750). Withdrawn routes are removed from the history state.
- *suppress* — Number compares to the flapping route’s penalty value. If the penalty value is greater than the suppress value, the flapping route no longer advertises and is suppressed (1 to 20000, default 2000).
- *max-suppress-time* — Maximum number of minutes a route is suppressed (1 to 255, default is four times the half-life value or 60 minutes).

2. View all flap statistics or for specific routes meeting the criteria in EXEC mode.

```
show ip bgp flap-statistics [ip-address [mask]]
```

- *ip-address* [*mask*] — Enter the IP address and mask.
- *filter-list as-path-name* — Enter the name of an AS-PATH ACL.
- *regexp regular-expression* — Enter a regular express to match on.

When you change the best path selection method, path selections for the existing paths remain unchanged until you reset it by using the `clear ip bgp` command in EXEC mode.

Configure values to reuse or restart route

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# dampening 2 2000 3000 10
```

View dampened (nonactive) routes

```
OS10# show ip bgp flap-statistics

BGP local router ID is 13.176.123.28
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network                               From
      Reuse                                 Path
Total number of prefixes: 0
```

View dampened paths

```
OS10# show ip bgp dampened-paths

BGP local router ID is 80.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network                               From       Reuse      Path
d*   3.1.2.0/24                             80.1.1.2   00:00:12   800 9 8 i
d*   3.1.3.0/24                             80.1.1.2   00:00:12   800 9 8 i
d*   3.1.4.0/24                             80.1.1.2   00:00:12   800 9 8 i
d*   3.1.5.0/24                             80.1.1.2   00:00:12   800 9 8 i
d*   3.1.6.0/24                             80.1.1.2   00:00:12   800 9 8 i
Total number of prefixes: 5
```

Timers

To adjust the routing timers for all neighbors, configure the timer values using the `timers` command. If both the peers negotiate with different keepalive and hold time values, the final hold time value is the lowest values received. The new keepalive value is one-third of the accepted hold time value.

- Configure timer values for all neighbors in ROUTER-NEIGHBOR mode.

```
timers keepalive holdtime
```

- `keepalive` — Time interval in seconds, between keepalive messages sent to the neighbor routers (1 to 65535, default 60).
- `holdtime` — Time interval in seconds, between the last keepalive message and declaring the router dead (3 to 65535, default 180).

View nondefault values

```
OS10# show running-configuration
...
neighbor 32.1.1.2
remote-as 103
timers 61 181
no shutdown
```

Neighbor soft-reconfiguration

BGP soft-reconfiguration allows for fast and easy route changes. Changing routing policies requires a reset of BGP sessions or the TCP connection, for the policies to take effect.

Resets cause undue interruption to traffic due to the hard reset of the BGP cache, and the time it takes to re-establish the session. BGP soft-reconfiguration allows for policies to apply to a session without clearing the BGP session. You can perform a soft-reconfiguration on a per-neighbor basis, either inbound or outbound. BGP soft-reconfiguration clears the policies without

resetting the TCP connection. After configuring soft-reconfiguration, use `clear ip bgp` to make the neighbor use soft reconfiguration.

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router replays and updates are re-evaluated. With this command, the replay and update process triggers only if a route-refresh request is not negotiated with the peer. If the request is negotiated after using the `clear ip bgp soft in` command, BGP sends a route-refresh request to the neighbor and receives all the peer's updates.

To use soft reconfiguration, or soft reset without preconfiguration, both BGP peers must support the soft route refresh capability. The soft route refresh advertises in the OPEN message sent when the peers establish a TCP session. To determine whether a BGP router supports this capability, use the `show ip bgp neighbors` command. If a router supports the route refresh capability, the `Received route refresh capability from peer` message displays.

1. Enable soft-reconfiguration for the BGP neighbor and BGP template in ROUTER-BGP mode. BGP stores all the updates that the neighbor receives but does not reset the peer-session. Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration.

```
neighbor {ip-address} soft-reconfiguration inbound
```

2. Enter Address Family mode in ROUTER-NEIGHBOR mode.

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

3. Configure soft-configuration for the neighbors belonging to the template.

```
soft-reconfiguration inbound
```

4. Clear all information or only specific details in EXEC mode.

```
clear ip bgp {neighbor-address | * } [soft in]
```

- * — Clears all peers.
- neighbor-address — Clears the neighbor with this IP address.

Soft-reconfiguration of IPv4 neighbor

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
```

Soft-reconfiguration of IPv6 neighbor

```
OS10(conf-router-neighbor)# address-family ipv6 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
```

BGP commands

activate

Enables the neighbor or peer group to be the current address-family identifier (AFI).

Syntax activate

Parameters None

Default Not configured

Command Mode ROUTER-BGP-NEIGHBOR-AF

Usage Information This command is used for exchanging IPv4 or IPv6 address family information with IPv4 or IPv6 neighbor. IPv4 unicast Address family is enabled by default. To activate IPv6 address family for IPv6 neighbor, use the `activate` command. To de-activate IPv4 address family for IPv6 neighbor, use the `no activate` command.

Example

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# activate
```

Supported Releases 10.2.0E or later

add-path

Allows the system to advertise multiple paths for the same destination without replacing previous paths with new ones.

Syntax `add-path {both path count | receive | send path count}`

- Parameters**
- `both path count` — Enter the number of paths to advertise to the peer, from 2 to 64.
 - `receive` — Receive multiple paths from the peer.
 - `send path count` — Enter the number of multiple paths to send multiple to the peer, from 2 to 64.

Default Not configured

Command Mode ROUTER-BGP-NEIGHBOR-AF

Usage Information Advertising multiple paths to peers for the same address prefix without replacing the existing path with a new one reduces convergence times. The `no` version of this command disables the multiple path advertisements for the same destination.

Example (IPv4)

```
OS10(config-router-bgp-af)# add-path both 64
```

Example (IPv6)

```
OS10(config-router-bgpv6-af)# add-path both 64
```

Example (Receive)

```
OS10(config-router-bgpv6-af)# add-path receive
```

Supported Releases 10.2.0E or later

address-family

Enters global address family configuration mode for the IP address family.

Syntax `address-family {[ipv4 | ipv6] unicast}`

- Parameters**
- `ipv4 unicast` — Enter an IPv4 unicast address family.
 - `ipv6 unicast` — Enter an IPv6 unicast address family.

Default None

Command Mode ROUTER-BGP

Usage Information This command applies to all IPv4 or IPv6 peers belonging to the template or neighbors only. The `no` version of this command removes the subsequent address-family configuration.

Example (IPv4 Unicast)

```
OS10(config)# router bgp 3
OS10(config-router-bgp-3)# address-family ipv4 unicast
OS10(config-router-bgpv4-af)#
```

Example (IPv6 Unicast)

```
OS10(config)# router bgp 4
OS10(config-router-bgp-4)# address-family ipv6 unicast
OS10(config-router-bgpv6-af)#
```

Supported Releases 10.3.0E or later

advertisement-interval

Sets the minimum time interval for advertisement between the BGP neighbors or within a BGP peer group.

Syntax	<code>advertisement-interval seconds</code>
Parameters	<i>seconds</i> —Enter the time interval value (in seconds) between BGP advertisements, from 1 to 600.
Default	EBGP 30 seconds, IBGP 5 seconds
Command Mode	ROUTER-NEIGHBOR
Usage Information	The time interval applies to all peer group members of the template in ROUTER-TEMPLATE mode. The <code>no</code> version of this command resets the advertisement-interval value to the default.
Example	<pre>OS10(conf-router-neighbor)# advertisement-interval 50</pre>
Supported Releases	10.3.0E or later

advertisement-start

Delays initiating the OPEN message for the specified time.

Syntax	<code>advertisement-start seconds</code>
Parameters	<i>seconds</i> —Enter the time interval value, in seconds, before starting to send the BGP OPEN message, from 0 to 240.
Default	Not configured
Command Mode	ROUTER-NEIGHBOR
Usage Information	The time interval applies to all the peer group members of the template in ROUTER-TEMPLATE mode. The <code>no</code> version of this command disables the advertisement-start time interval.
Example	<pre>OS10(conf-router-neighbor)# advertisement-start 30</pre>
Supported Releases	10.3.0E or later

aggregate-address

Summarizes a range of prefixes to minimize the number of entries in the routing table.

Syntax	<code>aggregate-address address/mask [as-set] [summary-only] [advertise-map map-name] {attribute-map route-map-name} [suppress-map route-map-name]</code>
Parameters	<ul style="list-style-type: none">• <i>address/mask</i> — Enter the IP address and mask.• <i>as-set</i> — (Optional) Generates AS set-path information.• <i>summary-only</i> — (Optional) Filters more specific routes from updates.• <i>advertise-map map-name</i> — (Optional) Enter the map name to advertise.• <i>attribute-map route-map-name</i> — (Optional) Enter the route-map name to set aggregate attributes.• <i>suppress-map route-map-name</i> — (Optional) Enter the route-map name to conditionally filters specific routes from updates.
Default	None
Command Mode	ROUTER-BGPv4-AF
Usage Information	At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active. If routes within the aggregate are constantly changing, do

not add the `as-set` parameter to the aggregate because the aggregate flaps to track changes in the AS_PATH. The `no` version of this command disables the aggregate-address configuration.

Example

```
OS10(conf-router-bgpv4-af)# aggregate-address 6.1.0.0/16 summary-only
```

Supported Releases

10.3.0E or later

allowas-in

Sets the number of times a local AS number appears in the AS path.

Syntax

`allowas-in as-number`

Parameters

`as-number`—Enter the number of occurrences for a local AS number, from 1 to 10.

Default

Disabled

Command Mode

ROUTER-BPG-TEMPLATE-AF

Usage Information

Use this command to enable the BGP speaker to allow the AS number to be present for the specified number of times in updates received from the peer. You cannot set this configuration for a peer associated with a peer group. You cannot associate a peer to a peer group that is already configured with an AS number. The `no` version of this command resets the value to the default.

Example ((IPv4))

```
OS10(conf-router-template)# address-family ipv4 unicast
OS10(conf-router-bgp-template-af)# allowas-in 5
```

Example (IPv6)

```
OS10(conf-router-template)# address-family ipv6 unicast
OS10(conf-router-bgp-template-af)# allowas-in 5
```

Supported Releases

10.3.0E or later

always-compare-med

Compares MULTI_EXIT_DISC (MED) attributes in the paths received from different neighbors.

Syntax

`always-compare-med`

Parameters

None

Default

Disabled

Command Mode

ROUTER-BGP

Usage Information

After you use this command, use the `clear ip bgp *` command to recompute the best path. The `no` version of this command resets the value to the default.



NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-10)# always-compare-med
```

Supported Releases

10.2.0E or later

as-notation

Changes the AS number notation format (requires four-octet-assupport).

Syntax `as-format {asdot | asdot+ | asplain}`

- Parameters**
- `asdot` — Specify the AS number notation in asdot format.
 - `asdot+` — Specify the AS number notation in asdot+ format.
 - `asplain` — Specify the AS number notation in asplain format.

Defaults `asplain`

Command Modes `ROUTER-BGP`

Usage Information

- NOTE:** To configure these settings for a non default VRF instance, you must first enter the `ROUTER-CONFIG-VRF` sub mode using the following commands:
1. Enter the `ROUTER BGP` mode using the `router bgp as-number` command.
 2. From the `ROUTER BGP` mode, enter the `ROUTER BGP VRF` mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-2)# as-notation asdot
OS10(conf-router-bgp-2)# as-notation asdot+
OS10(conf-router-bgp-2)# as-notation asplain
```

Supported Releases 10.1.0E or later

bestpath as-path

Configures the AS path selection criteria for best path computation.

Syntax `bestpath as-path {ignore | mutlipath-relax}`

- Parameters**
- `ignore` — Enter to ignore the AS PATH in BGP best path calculations.
 - `mutlipath-relax` — Enter to include prefixes received from different AS paths during multipath calculation.

Default `Enabled`

Command Mode `ROUTER-BGP`

Usage Information

To enable load-balancing across different EBGP peers, configure the `mutlipath-relax` option. If you configure both `ignore` or `mutlipath-relax` options at the same time, a system-generated error message appears. The `no` version of this command disables configuration.

- NOTE:** To configure these settings for a non default VRF instance, you must first enter the `ROUTER-CONFIG-VRF` sub mode using the following commands:
1. Enter the `ROUTER BGP` mode using the `router bgp as-number` command.
 2. From the `ROUTER BGP` mode, enter the `ROUTER BGP VRF` mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-10)# bestpath as-path mutlipath-relax
```

Supported Releases 10.3.0E or later

bestpath med

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

Syntax `bestpath med {confed | missing-as-worst}`

Parameters	<ul style="list-style-type: none"> • <code>confed</code> — Compare MED among BGP confederation paths. • <code>missing-as-worst</code> — Treat missing MED as the least preferred path.
Default	Disabled
Command Mode	ROUTER-BGP
Usage Information	<p>Before you apply this command, use the <code>always-compare-med</code> command. The <code>no</code> version of this command resets the MED comparison influence.</p> <p>NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:</p> <ol style="list-style-type: none"> 1. Enter the ROUTER BGP mode using the <code>router bgp as-number</code> command. 2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the <code>vrf vrf-name</code> command.
Example	<pre>OS10(conf-router-bgp-2)# bestpath med confed</pre>
Supported Releases	10.3.0E or later

bestpath router-id

Ignores comparing router-id information for external paths during the best path selection.

Syntax	<code>bestpath router-id {ignore}</code>
Parameters	<code>ignore</code> — Enter to ignore AS path for best-path computation.
Default	Enabled
Command Mode	ROUTER-BGP
Usage Information	<p>Select the path that you received first if you do not receive the same the router ID for multiple paths. Ignore the path information if you received the same router ID for multiple paths. The <code>no</code> version of this command resets the value to the default.</p> <p>NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:</p> <ol style="list-style-type: none"> 1. Enter the ROUTER BGP mode using the <code>router bgp as-number</code> command. 2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the <code>vrf vrf-name</code> command.
Example	<pre>OS10(conf-router-bgp-2)# bestpath router-id ignore</pre>
Supported Releases	10.3.0E or later

clear ip bgp

Resets BGP IPv4 or IPv6 neighbor sessions.

Syntax	<code>clear ip bgp [vrf vrf-name] {ipv4-address ipv6-address * }</code>
Parameters	<ul style="list-style-type: none"> • <code>vrf vrf-name</code> — (OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to clear IPv4 or IPv6 BGP neighbor sessions corresponding to that VRF. • <code>IPv4-address</code> — Enter an IPv4 address to clear a BGP neighbor configuration. • <code>IPv6-address</code> — Enter an IPv6 address to clear a BGP neighbor configuration. • <code>*</code> — Clears all BGP sessions.
Default	Not configured

Command Mode	EXEC
Usage Information	To reset BGP IPv4 or IPv6 neighbor sessions, use this command.
Example	<pre>OS10# clear ip bgp 1.1.15.4</pre>
Supported Releases	10.3.0E or later

clear ip bgp *

Resets BGP sessions. The soft parameter (BGP soft reconfiguration) clears policies without resetting the TCP connection.

Syntax	<code>clear ip bgp * [vrf vrf-name] [ipv4 unicast ipv6 unicast soft [in out]]</code>
Parameters	<ul style="list-style-type: none"> • <code>*</code> — Enter to clear all BGP sessions. • <code>vrf vrf-name</code> — (OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to clear BGP session information corresponding to that VRF. • <code>ipv4 unicast</code> — Enter to clear IPv4 unicast configuration. • <code>ipv6 unicast</code> — Enter to clear IPv6 unicast configuration. • <code>soft</code> — (Optional) Enter to configure and activate policies without resetting the BGP TCP session — BGP soft reconfiguration. • <code>in</code> — (Optional) Enter to activate only ingress (inbound) policies. • <code>out</code> — (Optional) Enter to activate only egress (outbound) policies.
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to reset BGP sessions.
Example	<pre>OS10# clear ip bgp * ipv6 unicast</pre>
Supported Releases	10.3.0E or later

clear ip bgp dampening

Clears the dampened paths information of the given prefix and undampened prefixes.

Syntax	<code>clear ip bgp dampening [vrf vrf-name] [ipv4-prefix ipv6-prefix]</code>
Parameters	<ul style="list-style-type: none"> • <code>vrf vrf-name</code> — (OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to clear dampened paths information corresponding to that VRF. • <code>ipv4-prefix</code> — (Optional) Enter an IPv4 prefix of the dampened path. • <code>ipv6-prefix</code> — (Optional) Enter an IPv6 prefix of the dampened path.
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	<pre>OS10# clear ip bgp dampening 1.1.15.5</pre>
Supported Releases	10.3.0E or later

clear ip bgp flap-statistics

Clears all or specific IPv4 or IPv6 flap counts of prefixes.

Syntax	<code>clear ip bgp [vrf vrf-name] [ipv4-address ipv6-address] flap-statistics [ipv4-prefix ipv6-prefix]</code>
Parameters	<ul style="list-style-type: none">• <code>vrf vrf-name</code> — (OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to clear flap statistics information corresponding to that VRF.• <code>ipv4-address</code> — (Optional) Enter an IPv4 address to clear the flap counts of the prefixes learned from the given peer.• <code>ipv6-address</code> — (Optional) Enter an IPv6 address to clear the flap counts.• <code>ipv4-prefix</code> — (Optional) Enter an IPv6 prefix to clear the flap counts of the given prefix.• <code>ipv6-prefix</code> — (Optional) Enter an IPv6 prefix to clear the flap counts of the given prefix.
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example (All Prefixes)	<pre>OS10# clear ip bgp flap-statistics</pre>
Example (IPv4)	<pre>OS10# clear ip bgp 1.1.15.4 flap-statistics</pre>
Example (Given Prefix)	<pre>OS10# clear ip bgp flap-statistics 1.1.15.0/24</pre>
Supported Releases	10.3.0E or later

connection-retry-timer

Configures the timer to retry the connection to BGP neighbor or peer group.

Syntax	<code>connection-retry-timer retry-timer-value</code>
Parameters	<code>retry-timer-value</code> — Enter the time interval in seconds, ranging from 10 to 65535.
Defaults	60 seconds
Command Modes	CONFIG-ROUTER-NEIGHBOR CONFIG-ROUTER-TEMPLATE
Usage Information	The <code>no</code> version of this command resets the timer to default value..
Example	<pre>OS10(config-router-neighbor)# connection-retry-timer 1000 OS10(config-router-template)# connection-retry-timer 100</pre>
Supported Releases	10.3.0E or later

confederation

Configures an identifier for a BGP confederation.

Syntax	<code>confederation {identifier as-num peers as-number}</code>
---------------	--

Parameters

- `identifier as-num` —Enter an AS number, from 0 to 65535 for 2 bytes, 1 to 4294967295 for 4 bytes, or 0.1 to 65535.65535 for dotted format.
- `peers as-number`—Enter an AS number for peers in the BGP confederation, from 1 to 4294967295.

Default Not configured

Command Mode ROUTER-BGP

Usage Information

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 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. OS10 sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ. The `no` version of this command deletes the confederation configuration.

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example (Identifier)

```
OS10(conf-router-bgp-2)# confederation identifier 1
```

Example (Peers)

```
OS10(conf-router-bgp-2)# confederation peers 2
```

Supported Releases 10.3.0E or later

client-to-client

Enables route reflection between clients in a cluster.

Syntax `client-to-client {reflection}`

Parameters `reflection` — Enter to enable reflection of routes allowed in a cluster.

Default Enabled

Command Mode ROUTER-BGP

Usage Information

Configure the route reflector to enable route reflection between all clients. You must fully mesh all clients before you disable route reflection. The `no` version of this command disables route reflection in a cluster.

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-2)# client-to-client reflection
```

Supported Releases 10.2.0E or later

cluster-id

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

Syntax	<code>cluster-id {number ip-address}</code>
Parameters	<ul style="list-style-type: none">• <i>number</i>—Enter a route reflector cluster ID as a 32-bit number, from 1 to 4294967295.• <i>ip-address</i>—Enter an IP address as the route-reflector cluster ID.
Default	Router ID
Command Mode	ROUTER-BGP
Usage Information	<p>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. If you enter the cluster ID as an integer, an integer displays. The <code>no</code> version of this command resets the value to the default.</p> <p>NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:</p> <ol style="list-style-type: none">1. Enter the ROUTER BGP mode using the <code>router bgp as-number</code> command.2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the <code>vrf vrf-name</code> command.

Example

```
OS10(conf-router-bgp-10)# cluster-id 3.3.3.3
```

Supported Releases

10.3.0E or later

bgp dampening

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

Syntax	<code>bgp dampening [half-life reuse-limit suppress-limit max-suppress-time route-map-name]</code>
Parameters	<ul style="list-style-type: none">• <i>half-life</i> — (Optional) Enter the 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, from 1 to 45.• <i>reuse-limit</i> — (Optional) Enter a reuse-limit 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, from 1 to 20000.• <i>suppress-limit</i> — (Optional) Enter a suppress-limit 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, from 1 to 20000.• <i>max-suppress-time</i> — (Optional) Enter the maximum number of minutes a route is suppressed, from 1 to 255.• <i>route-map-name</i> — (Optional) Enter the name of the route-map.
Defaults	<code>half-life 15; reuse-limit 750; suppress-limit 2000; max-suppress-time 60</code>
Command Mode	ROUTER-BGP-AF
Usage Information	<p>To reduce the instability fo the BGP process, setup route flap dampening parameters. After setting up the dampening parameters, clear information on route dampening and return suppressed routes to the Active state. You can also view statistics on route flapping or change the path selection from the default deterministic mode to non-deterministic. The <code>no</code> version of this command resets the value to the default.</p>
Example	<pre>OS10(conf-router-bgpv4-af)# dampening 2 751 2001 51 map1</pre>
Supported Releases	10.3.0E or later

description

Configures a description for the BGP neighbor or for peer template.

Syntax	<code>description text</code>
Parameters	<code>text</code> — Enter a description for the BGP neighbor or peer template.
Default	None
Command Mode	ROUTER-BGP-NEIGHBOR ROUTER-BGP-TEMPLATE

Usage Information The `no` version of this command removes the description.

Example

```
OS10# configure terminal
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 8.8.8.8
OS10(config-router-neighbor)# description n1_abcd
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# template t1
OS10(config-router-template)# description peer_template_1_abcd
```

Supported Releases 10.4.1.0 or later

default-metric

Assigns a default-metric of redistributed routes to locally originated routes.

Syntax	<code>default-metric number</code>
Parameters	<code>number</code> — Enter a number as the metric to assign to routes from other protocols, from 1 to 4294967295.
Default	Disabled
Command Mode	ROUTER-BGP
Usage Information	Assigns a metric for locally-originated routes such as redistributed routes. After you redistribute routes in BGP, use this command to reset the metric value — the new metric does not immediately take effect. The new metric takes effect only after you disable and re-enable route redistribution for a specified protocol. To re-enable route distribution use the <code>redistribute {connected [route-map map-name] ospf process-id static [route-map map-name]}</code> command, or use the <code>clear ip bgp *</code> command after you reset BGP. The <code>no</code> version of this command removes the default metric value.

Example (IPv4)

```
OS10(conf-router-bgpv4-af)# default-metric 60
```

Example (IPv6)

```
OS10(conf-router-bgpv6-af)# default-metric 60
```

Supported Releases 10.3.0E or later

default-originate

Configures the default route to a BGP peer or neighbor.

Syntax	<code>default-originate [route-map route-map-name]</code>
Parameters	<code>route-map route-map-name</code> —(Optional) Enter a route-map name. A maximum of 140 characters.

Default Enabled

Command Mode ROUTER-BGP-NEIGHBOR-AF
ROUTER-TEMPLATE-AF

Usage Information The `no` version of this command removes the default route.

Example

```
OS10(conf-router-bgp-10)# template lunar
OS10(conf-router-bgp-template)# address-family ipv6 unicast
OS10(conf-router-template-af)# default-originate route-map rmap-bgp
```

Supported Releases 10.4.1.0 or later

distribute-list

Distributes BGP information through an established prefix list.

Syntax `distribute-list prefix-list-name {in | out}`

Parameters

- *prefix-list-name*—Enter the name of established prefix list.
- *in*—Enter to distribute inbound traffic.
- *out*—Enter to distribute outbound traffic.

Defaults None

Command Modes ROUTER-BGP-NEIGHBOR-AF
ROUTER-TEMPLATE-AF

Usage Information The `no` version of this command removes the `route-map`.

Example

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# distribute-list inbgg in
```

```
OS10(conf-router-template)# address-family ipv4 unicast
OS10(conf-router-bgp-template-af)# distribute-list outbgg out
```

Supported Releases 10.4.1.0 or later

bgp default local-preference

Changes the default local preference value for routes exchanged between internal BGP peers.

Syntax `default local-preference number`

Parameters *number* — Enter a number as the metric to assign to routes as the degree of preference for those routes. When routes compare, the route with the higher degree of preference or the local preference value is most preferred, from 1 to 4294967295.

Default 100

Command Mode ROUTER-BGP

Usage Information All routers apply this command setting within the AS. The `no` version of this command removes local preference value.

Example

```
OS10(conf-router-bgp-1)# default local-preference 200
```

Supported Releases 10.3.0E or later

ebgp-multihop

Allows EBGP neighbors on indirectly connected networks.

Syntax `ebgp-multihop hop count`

Parameters `hop count` — Enter a value for the number of hops, from 1 to 255.

Default 1

Command Mode ROUTER-NEIGHBOR

Usage Information This command avoids installation of default multihop peer routes to prevent loops and creates neighbor relationships between peers. Networks indirectly connected are not valid for best path selection. The `no` version of this command removes multihop session.

Example

```
OS10(conf-router-neighbor)# ebgp-multihop 2
```

Supported Releases 10.3.0E 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.

Syntax `enforce-first-as`

Parameters None

Default Enabled

Command Mode ROUTER-BGP

Usage Information To verify statistics of routes rejected, use the `show ip bgp neighbors` command. 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. The `no` version of this command turns off the default.

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-1)# enforce-first-as
```

Supported Releases 10.3.0E or later

fall-over

Enables or disables BGP session fast fall-over for BGP neighbors.

Syntax `fall-over`


Parameters None

Default Disabled

Command Mode	ROUTER-NEIGHBOR
Usage Information	Configure the BGP fast fall-over on a per-neighbor or peer-group basis. When you enable this command on a template, it simultaneously enables on all peers that inherit the peer group template. When you enable fall-over, BGP tracks IP reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable — no active route exists in the routing table for peer IPv6 destinations or local address — BGP brings down the session with the peer. The <code>no</code> version of this command disables fall-over.
Example	<pre>OS10(conf-router-neighbor)# fall-over</pre>
Supported Releases	10.3.0E or later

fast-external-fallover

Resets BGP sessions immediately when a link to a directly connected external peer fails.

Syntax	<code>fast-external-fallover</code>
Parameters	None
Default	Not configured
Command Mode	ROUTER-BGP
Usage Information	Fast external fall-over terminates the EBGP session immediately after the IP unreachability or link failure is detected. This only applies after you manually reset all existing BGP sessions. For the configuration to take effect, use the <code>clear ip bgp</code> command. The <code>no</code> version of this command disables fast external fallover.
	<p> NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:</p> <ol style="list-style-type: none"> 1. Enter the ROUTER BGP mode using the <code>router bgp as-number</code> command. 2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the <code>vrf vrf-name</code> command.
Example	<pre>OS10(conf-router-bgp-10)# fast-external-fallover</pre>
Supported Releases	10.3.0E or later

inherit template

Configures a peer group template name that the neighbors use to inherit peer-group configuration.

Syntax	<code>inherit template <i>template-name</i></code>
Parameters	<i>template-name</i> — Enter a template name, up to 16 characters.
Default	Not configured
Command Mode	ROUTER-NEIGHBOR
Usage Information	When network neighbors inherit a template, all features enabled on the template are also supported on the neighbors. The <code>no</code> version of this command disables the peer group template configuration.
Example	<pre>OS10(conf-router-neighbor)# inherit template zanzibar</pre>
Supported Releases	10.2.0E or later

listen

Enables peer listening and sets the prefix range for dynamic peers.

Syntax	<code>listen ip-address [limit count]</code>
Parameters	<ul style="list-style-type: none">• <code>ip-address</code>—Enter the BGP neighbor IP address.• <code>limit count</code>—(Optional) Enter a maximum dynamic peer count, from 1 to 4294967295.
Default	Not configured
Command Mode	ROUTER-TEMPLATE
Usage Information	Enables a passive peering session for listening. The <code>no</code> version of this command disables a passive peering session.
Example	<pre>OS10(conf-router-template)# listen 1.1.0.0/16 limit 4</pre>
Supported Releases	10.2.0E or later


local-as

Configures a local AS number for a peer.

Syntax	<code>local-as as-number [no-prepend]</code>
Parameters	<ul style="list-style-type: none">• <code>as-number</code>—Enter the local AS number, from 1 to 4294967295.• <code>no-prepend</code>—(Optional) Enter so that local AS values are not prepended to announcements from the neighbor.
Default	Disabled
Command Mode	ROUTER-NEIGHBOR or ROUTER-TEMPLATE
Usage Information	Facilitates the BGP network migration operation and allows you to maintain existing AS numbers. The <code>no</code> version of this command resets the value to the default.
Example (Neighbor)	<pre>OS10(conf-router-bgp-10)# neighbor lunar OS10(conf-router-neighbor)# local-as 20</pre>
Example (Template)	<pre>OS10(conf-router-bgp-10)# template solar OS10(conf-router-template)# local-as 20</pre>
Supported Releases	10.3.0E or later

log-neighbor-changes

Enables logging for changes in neighbor status.

Syntax	<code>log-neighbor-changes</code>
Parameters	None
Default	Enabled
Command Mode	ROUTER-BGP
Usage Information	OS10 saves logs which includes the neighbor operational status and reset reasons. To view the logs, use the <code>show bgp config</code> command. The <code>no</code> version of this command disables the feature.  NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-10)# log-neighbor-changes
```

Supported Releases

10.3.0E or later

maximum-paths

Configures the maximum number of equal-cost paths for load sharing.

Syntax `maximum-paths [ebgp number | ibgp number] maxpaths`

- Parameters**
- `ebgp`—Enable multipath support for external BGP routes.
 - `ibgp`—Enable multipath support for internal BGP routes.
 - `number`—Enter the number of parallel paths, from 1 to 64.

Default 64 paths

Command Mode ROUTER-BGP

Usage Information Dell EMC recommends not using multipath and add path simultaneously in a route reflector. To recompute the best path, use the `clear ip bgp *` command. The `no` version of this command resets the value to the default

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example (EBGP)

```
OS10(conf-router-bgp-2)# maximum-paths ebgp 2 maxpaths
```

Example (IBGP)

```
OS10(conf-router-bgp-2)# maximum-paths ibgp 4 maxpaths
```

Supported Releases

10.3.0E or later

maximum-prefix

Configures the maximum number of prefixes allowed from a peer.

Syntax `maximum-prefix {number [threshold] [warning]}`

- Parameters**
- `number`—Enter a maximum prefix number, from 1 to 4294967295.
 - `threshold`—(Optional) Enter a threshold percentage, from 1 to 100
 - `warning-only` — (Optional) Enter to set the router to send a log message (warning) when the maximum limit is exceeded. If you do not set this parameter, the router stops peering when the maximum prefixes limit exceeds.

Default 75% threshold

Command Mode ROUTER-BGP-NEIGHBOR-AF

Usage Information If you configure this command and the neighbor receives more prefixes than the configuration allows, the neighbor goes down. To view the prefix information, use the `show ip bgp summary` command output. The neighbor remains down until you use the `clear ip bgp` command for the neighbor or the peer group to which the neighbor belongs. The `no` version of this command resets the value to the default.

Example

```
OS10 (conf-router-bgp-neighbor-af) # maximum-prefix 20 100 warning-only
```

Supported Releases

10.3.0E or later

neighbor

Creates a remote peer for the BGP neighbor and enters BGP Neighbor mode.

Syntax

```
neighbor ip address
```

Parameters

ip address — Enter the IP address of the neighbor in dotted decimal format.

Default

Not configured

Command Mode

CONFIG-ROUTER-BGP

Usage Information

Create a remote peer with the BGP neighbor. Always enter the IP address of a BGP peer with this command. The command does not validate if the configured peer address is a local IP address. The `no` version of this command disables the BGP neighbor configuration.

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10 (conf-router-bgp-2) # neighbor 32.1.1.0.0
OS10 (conf-router-neighbor) #
```

Supported Releases

10.3.0E or later

next-hop-self

Disables the next-hop calculation for a neighbor.

Syntax

```
next-hop-self
```

Parameters

None

Default

Enabled

Command Mode

ROUTER-NEIGHBOR-AF

Usage Information

Influences next-hop processing of EBGP routes to IBGP peers. The `no` version of this command disables the next-hop calculation.

Example

```
OS10 (conf-router-neighbor-af) # next-hop-self
```

Supported Releases

10.3.0E or later

non-deterministic-med

Compares paths in the order they arrive.

Syntax

```
non-deterministic-med
```

Parameters

None

Default

Disabled

Command Mode ROUTER-BGP

Usage Information Paths compare in the order they arrive. OS10 uses this method to choose different best paths from a set of paths, depending on the order they are received from the neighbors. MED may or may not be compared between adjacent paths. When you change the path selection from deterministic to non-deterministic, the path selection for the existing paths remains deterministic until you use the `clear ip bgp` command to clear the existing paths. The `no` version of this command configures BGP bestpath selection as non-deterministic.

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10 (conf-router-bgp-10) # non-deterministic-med
```

Supported Releases 10.2.0E or later

outbound-optimization

Enables outbound optimization for IBGP peer-group members.

Syntax `outbound-optimization`

Parameters None

Default Not configured

Command Mode ROUTER-BGP

Usage Information Enable or disable outbound optimization dynamically to reset all neighbor sessions. When you enable outbound optimization, all peers receive the same update packets. The next-hop address chosen as one of the addresses of neighbor's reachable interfaces is also the same for the peers. The `no` version of this command disables outbound optimization.

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10 (conf-router-bgp-10) # outbound-optimization
```

Supported Releases 10.3.0E or later

password

Configures a password for message digest 5 (MD5) authentication on the TCP connection between two neighbors.

Syntax `password {9 encrypted password-string| password-string}`

- Parameters**
- `9 encrypted password-string`—Enter 9 followed by encrypted password.
 - `password-string`—Enter a password for authentication, up to 128 characters.

Default Disabled

Command Mode ROUTER-NEIGHBOR
ROUTER-TEMPLATE

Usage Information You can enter the password either as plain text or in encrypted format. The password provided in ROUTER-NEIGHBOR mode gets more preference than the password in ROUTER-TEMPLATE mode. The no version of this command disables authentication.

Example

```
OS10(conf-router-neighbor)# password abcde11
```

```
OS10(conf-router-neighbor)# password 9
f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
```

Supported Releases 10.3.0E or later

redistribute

Redistributes connected, static, and OSPF routes in BGP.

Syntax `redistribute {connected [route-map map name] | ospf process-id | static [route-map map name]}`

- Parameters**
- `connected` — Enter to redistribute routes from physically connected interfaces.
 - `route-map map name` — (Optional) Enter the name of a configured route-map.
 - `ospf process-id` — Enter a number for the OSPF process (1 to 65535).
 - `static` — Enter to redistribute manually configured routes.

Default Disabled

Command Mode ROUTER-BGPv4-AF or ROUTER-BGPv6-AF

Usage Information Static routes are treated as incomplete routes. When you use the `redistribute ospf process-id` command without other parameters, the system redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. The no version of this command resets the value to the default.

Example (Connected)

```
OS10(conf-router-bgp-102)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# redistribute connected route-map mapbgp1
```

Example (Static — IPv4)

```
OS10(conf-router-bgp-102)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# redistribute static route-map mapbgp2
```

Example (Static — IPv6)

```
OS10(conf-router-bgp-102)# address-family ipv6 unicast
OS10(conf-router-bgpv6-af)# redistribute static
```

Example (OSPF — IPv4)

```
OS10(conf-router-bgp-102)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# redistribute ospf 1
```

Example (OSPF — IPv6)

```
OS10(conf-router-bgp-102)# address-family ipv6 unicast
OS10(conf-router-bgpv6-af)# redistribute ospf 1
```

Supported Releases 10.2.0E or later

remote-as

Adds a remote AS to the specified BGP neighbor or peer group.

Syntax `remote-as as-number`

Parameters `as-number` — Specify AS number ranging from 1 to 65535 for 2 byte or 1 to 4294967295 for 4 byte.

Defaults	None
Command Modes	CONFIG-ROUTER-NEIGHBOR CONFIG-ROUTER-TEMPLATE
Usage Information	The no version of this command deletes the remote AS.
Example	<pre>OS10(config)# router bgp 300 OS10(config-router-bgp-300)# template ebgppg OS10(config-router-template)# remote-as 100</pre>
Supported Releases	10.4.1.0 or later

remove-private-as

Removes private AS numbers from receiving outgoing updates.

Syntax	<code>remove-private-as</code>
Parameters	None
Defaults	Disabled
Command Mode	CONFIG-ROUTER-NEIGHBOR CONFIG-ROUTER-TEMPLATE
Usage Information	None
Example	<pre>OS10(config)# router bgp 300 OS10(config-router-bgp-300)# template ebgppg OS10(config-router-template)# remove-private-as</pre>
Supported Releases	10.4.1.0 or later

route-map

Applies an established route-map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax	<code>route-map <i>route-map-name</i> {in out}</code>
Parameters	<ul style="list-style-type: none"> • <i>route-map-name</i> — Enter the name of the configured route-map. • <i>in</i> — attaches the route-map as the inbound policy • <i>out</i> — attaches the route-map as the outbound policy
Defaults	None
Command Modes	ROUTER-BGP-TEMPLATE-AF
Usage Information	The no version of this command deletes the route-map.
Example	<pre>OS10(conf-router-neighbor)# address-family ipv4 unicast OS10(conf-router-bgp-neighbor-af)# route-map bgproutemap in</pre> <pre>OS10(conf-router-template)# address-family ipv4 unicast OS10(conf-router-bgp-template-af)# route-map bgproutemap in</pre>

Supported Releases 10.4.1.0 or later

route-reflector-client

Configures a neighbor as a member of a route-reflector cluster.

Syntax `route-reflector-client`

Parameters None

Default Not configured

Command Mode ROUTER-TEMPLATE

Usage Information The device configures as a route reflector, and the BGP neighbors configure as clients in the route-reflector cluster. The `no` version of this command removes all clients of a route reflector—the router no longer functions as a route reflector.

Example

```
OS10(conf-router-template)# route-reflector-client
```

Supported Releases 10.3.0E or later

router bgp

Enables BGP and assigns an AS number to the local BGP speaker.

Syntax `router bgp as-number`

Parameters *as-number*—Enter the AS number range.

- 1 to 65535 in 2-byte
- 1 to 4294967295 in 4-byte

Default None

Command Mode CONFIGURATION

Usage Information The AS number can be a 16-bit integer. The `no` version of this command resets the value to the default.

Example

```
OS10(config)# router bgp 3
OS10(conf-router-bgp-3)#
```

Supported Releases 10.3.0E or later

router-id

Assigns a user-given ID to a BGP router.


Syntax `router-id ip-address`

Parameters *ip-address* — Enter an IP address in dotted decimal format.

Default First configured IP address or random number

Command Mode ROUTER-BGP

Usage Information Change the router ID of a BGP router to reset peer-sessions. The `no` version of this command resets the value to the default.

 **NOTE:** To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-10)# router-id 10.10.10.40
```

Supported Releases

10.3.0E or later

send-community

Sends a community attribute to a BGP neighbor or peer group.

Syntax `send-community {extended | standard}`

- Parameters**
- `extended` — Enter an extended community attribute.
 - `standard` — Enter a started community attribute.

Default Not configured

Command Mode ROUTER-NEIGHBOR

Usage Information A community attribute indicates that all routes with the same attributes belong to the same community grouping. All neighbors belonging to the template inherit the feature when configured for a template. The `no` version of this command disables sending a community attribute to a BGP neighbor or peer group.

Example

```
OS10(conf-router-neighbor)# send-community extended
```

Supported Releases

10.3.0E or later

sender-side-loop-detection

Enables the sender-side loop detection process for a BGP neighbor.

Syntax `sender-side-loop-detection`

Parameters None

Default Enabled

Command Mode ROUTER-BGP-NEIGHBOR-AF

Usage Information This command helps detect routing loops, based on the AS path before it starts advertising routes. To configure a neighbor to accept routes use the `neighbor allowas-in` command. The `no` version of this command disables sender-side loop detection for that neighbor.

Example (IPv4)

```
OS10(conf-router-bgp-102)# neighbor 3.3.3.1
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# sender-side-loop-detection
```

Example (IPv6)

```
OS10(conf-router-bgp-102)# neighbor 32::1
OS10(conf-router-neighbor)# address-family ipv6 unicast
OS10(conf-router-bgp-neighbor-af)# no sender-side-loop-detection
```

Supported Releases

10.3.0E or later

show ip bgp

Displays information that BGP neighbors exchange.

- Syntax** `show ip bgp [vrf vrf-name] ip-address/mask`
- Parameters**
- `vrf vrf-name` — (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view route information corresponding to that VRF.
 - `ip-address/mask` — Enter the IP address and mask in A.B.C.D/x format.
- Default** Not configured
- Command Mode** EXEC
- Usage Information** This command displays BGP neighbor information.
- Example**

```
OS10# show ip bgp 1.1.1.0/24
BGP routing table entry for 1.1.1.0/24
Paths: (1 available, table Default-IP-Routing-Table.)

Received from :
3.1.1.1(3.3.3.33) Best

AS_PATH : 100
Next-Hop : 3.1.1.1, Cost : 0

Origin INCOMPLETE, Metric 0, LocalPref 100, Weight 0, confed-external
Route-reflector origin : 0.0.0.0
```

Supported Releases 10.3.0E or later

show ip bgp dampened-paths

Displays BGP routes that are dampened (non-active).

- Syntax** `show ip bgp [vrf vrf-name] dampened-paths`
- Parameters** None
- Default** Not configured
- Command Mode** EXEC
- Usage Information**
- `vrf vrf-name` — (OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view routes that are affected by a specific community list corresponding to that VRF.
 - `Network` — Displays the network ID to which the route is dampened.
 - `From` — Displays the IP address of the neighbor advertising the dampened route.
 - `Reuse` — Displays the HH:MM:SS until the dampened route is available.
 - `Path` — Lists all AS the dampened route passed through to reach the destination network.

Example

```
OS10# show ip bgp dampened-paths

BGP local router ID is 80.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
          Network          From           Reuse           Path
d*       3.1.2.0/24         80.1.1.2       00:00:12       800 9 8 i
d*       3.1.3.0/24         80.1.1.2       00:00:12       800 9 8 i
d*       3.1.4.0/24         80.1.1.2       00:00:12       800 9 8 i
d*       3.1.5.0/24         80.1.1.2       00:00:12       800 9 8 i
d*       3.1.6.0/24         80.1.1.2       00:00:12       800 9 8 i
Total number of prefixes: 5
```


Supported Releases 10.3.0E or later

show ip bgp flap-statistics

Displays BGP flap statistics on BGP routes.

Syntax show ip bgp [*vrf vrf-name*] flap-statistics

Parameters None

Default Not configured

Command Mode EXEC

Usage Information

- *vrf vrf-name* — (OPTIONAL) Enter the keywords *vrf* and then the name of the VRF to view flap statistics on BGP routes corresponding to that VRF.
- *Network* — Displays the network ID to which the route is flapping.
- *From* — Displays the IP address of the neighbor advertising the flapping route
- *Duration* — Displays the HH:MM:SS since the route first flapped.
- *Flaps* — Displays the number of times the route flapped.
- *Reuse* — Displays the HH:MM:SS until the flapped route is available.
- *Path* — Lists all AS the flapping route passed through to reach the destination network.

Example

```
OS10# show ip bgp flap-statistics
BGP local router ID is 80.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network      From      Flaps  Duration  Reuse      Path
*>  3.1.2.0/24    80.1.1.2    1      00:00:11  00:00:00   800 9 8 i
*>  3.1.3.0/24    80.1.1.2    1      00:00:11  00:00:00   800 9 8 i
*>  3.1.4.0/24    80.1.1.2    1      00:00:11  00:00:00   800 9 8 i
*>  3.1.5.0/24    80.1.1.2    1      00:00:11  00:00:00   800 9 8 i
*>  3.1.6.0/24    80.1.1.2    1      00:00:11  00:00:00   800 9 8 i
Total number of prefixes: 5
```

Supported Releases 10.3.0E or later

show ip bgp ipv4 unicast

Displays route information for BGP IPv4 routes.

Syntax show ip bgp [*vrf vrf-name*] ipv4 unicast {*ip-address/mask* | *summary*}
[*denied-routes*]

Parameters

- *vrf vrf-name* — (OPTIONAL) Enter the keyword *vrf* followed by the name of the VRF to view IPv4 unicast summary information corresponding to that VRF.
- *unicast ip-address/mask* — Displays IPv4 unicast route information.
- *summary* — Displays IPv4 unicast summary information.
- *denied-routes* — (Optional) Displays the configured denied routes.

Default Not configured

Command Mode EXEC

Usage Information This command provides output which displays locally advertised BGPv4 routes configured using the *network* command. These routes show as *r* for redistributed/network-learned routes.

Example

```
OS10# show ip bgp ipv4 unicast summary
BGP router identifier 80.1.1.1 local AS number 102
```

Neighbor	AS	MsgRcvd	MsgSent	Up/Down	State/Pfx
80.1.1.2	800	8	4	00:01:10	5

Supported Releases 10.3.0E or later

show ip bgp ipv6 unicast

Displays route information for BGP IPv6 routes.

Syntax `show ip bgp [vrf vrf-name] ipv6 unicast [neighbors] {ip-address/mask | summary} | multicast {ip-address/mask | neighbors} [denied-routes]`

- Parameters**
- `vrf vrf-name` — (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IPv6 unicast information corresponding to that VRF.
 - `neighbors` — Displays IPv6 neighbor information.
 - `ip-address/mask` — Displays information about IPv6 unicast routes.
 - `summary` — Displays IPv6 unicast summary information.
 - `multicast ip-address/mask` — Displays IPv6 multicast routes information.
 - `denied-routes` — (Optional) Displays the configured IPv6 denied routes.

Default Not configured

Command Mode EXEC

Usage Information This command displays IPv6 BGP routing information.

Example

```
OS10# show ip bgp ipv6 unicast summary
BGP router identifier 80.1.1.1 local AS number 102
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
80.1.1.2 800 8 4 00:01:10 5
```

Supported Releases 10.3.0E or later

show ip bgp neighbors

Displays information that BGP neighbors exchange.

Syntax `show ip bgp [vrf vrf-name] neighbors ip-address [denied-routes]`

- Parameters**
- `vrf vrf-name` — (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view information exchanged between BGP neighbors corresponding to that VRF.
 - `ip-address` — Enter the IP address for a specific neighbor.
 - `denied-routes` — (Optional) Displays the list of routes denied by policy.
 - `advertised-routes`—Displays the routes advertised to neighbor
 - `dampened-routes`—Displays the suppressed routes received from neighbor
 - `flap-statistics`—Displays the route's flap statistics received from neighbor
 - `received-routes`—Displays the routes received from neighbor
 - `routes`—Displays routes learned from neighbor

Default Not configured

Command Mode EXEC

- Usage Information**
- `BGP neighbor` — Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, the link is internal; otherwise the link is external.
 - `BGP version` — Displays the BGP version (always version 4) and the remote router ID.

- **BGP state** — Displays the neighbor's BGP state and the amount of time in hours:minutes: seconds it has been in that state.
- **Last read** — Displays the information included in the last read:
 - Last read is the time (hours:minutes: seconds) the router read a message from its neighbor.
 - Hold time is the number of seconds configured between messages from its neighbor.
 - Keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.
- **Received messages** — Displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
- **Sent messages** — Displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
- **Description** — Displays the descriptive name configured for the BGP neighbor. This field is displayed only when the description is configured.
- **Local host** — Displays the peering address of the local router and the TCP port number.
- **Foreign host** — Displays the peering address of the neighbor and the TCP port number.

Although the status codes for routes received from a BGP neighbor may not display in `show ip bgp neighbors ip-address received-routes` output, they display correctly in `show ip bgp` output.

Example

```
OS10# show ip bgp neighbors
BGP neighbor is 80.1.1.2, remote AS 800, local AS 102  external link

  BGP version 4, remote router ID 12.12.0.2
  BGP state ESTABLISHED, in this state for 00:02:51
  Last read 00:18:23 seconds
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Fall-over disabled

  Received 11 messages
    1 opens, 0 notifications, 3 updates
    7 keepalives, 0 route refresh requests
  Sent 8 messages
    1 opens, 0 notifications, 0 updates
    7 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Description: nl_abcd
  Capabilities received from neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)MULTIPROTO_EXT(1)MULTIPROTO_EXT(1)ROUTE_REFRESH(2)
  Capabilities advertised to neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)MULTIPROTO_EXT(1)ROUTE_REFRESH(2)CISCO_ROUTE_REFRESH
(128)4_OCTET_AS(65)
  Prefixes accepted 5, Prefixes advertised 0
  Connections established 1; dropped 1
  Closed by neighbor sent 00:02:51 ago
  For address family: IPv4 Unicast
  Next hop set to self
  Allow local AS number 0 times in AS-PATH attribute

  For address family: IPv6 Unicast
  Next hop set to self
  Allow local AS number 0 times in AS-PATH attribute

  Local host: 80.1.1.1, Local port: 57812
  Foreign host: 80.1.1.2, Foreign port: 179
```

Example advertised-routes

```
OS10# show ip bgp ipv6 unicast neighbors 192:168:1::2 advertised-routes
BGP local router ID is 100.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric      LocPrf      Weight      Path
*>55::/64        192:168:1::1     0           0           0           100i
```

```

*>55:0:0:1::/64 192:168:1::1 0 0 0 100i
*>55:0:0:2::/64 192:168:1::1 0 0 0 100i
*>55:0:0:3::/64 192:168:1::1 0 0 0 100i
*>55:0:0:4::/64 192:168:1::1 0 0 0 100i
*>55:0:0:5::/64 192:168:1::1 0 0 0 100i
*>55:0:0:6::/64 192:168:1::1 0 0 0 100i
*>55:0:0:7::/64 192:168:1::1 0 0 0 100i
*>55:0:0:8::/64 192:168:1::1 0 0 0 100i
*>55:0:0:9::/64 192:168:1::1 0 0 0 100i
*>172:16:1::/64 192:168:1::1 0 0 0 100?

Total number of prefixes: 11
OS10#

```

Example received-routes

```

OS10# show ip bgp ipv6 unicast neighbors 172:16:1::2 received-routes
BGP local router ID is 100.1.1.1
Status codes: D denied
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network      Next Hop      Metric    LocPrf    Path
D 55::/64      172:16:1::2  0         0         i
  55:0:0:1::/64 172:16:1::2  0         0         i
  55:0:0:2::/64 172:16:1::2  0         0         i
D 55:0:0:3::/64 172:16:1::2  0         0         i
D 55:0:0:4::/64 172:16:1::2  0         0         i
D 55:0:0:5::/64 172:16:1::2  0         0         i
D 55:0:0:6::/64 172:16:1::2  0         0         i
  55:0:0:7::/64 172:16:1::2  0         0         i
D 55:0:0:8::/64 172:16:1::2  0         0         i
D 55:0:0:9::/64 172:16:1::2  0         0         i
Total number of prefixes: 10
OS10#

```

Example denied-routes

```

OS10# show ip bgp ipv6 unicast neighbors 172:16:1::2 denied-routes
BGP local router ID is 100.1.1.1
Status codes: D denied
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network      Next Hop      Metric    LocPrf    Path
D 55::/64      172:16:1::2  0         0         100 200 300 400i
D 55:0:0:1::/64 172:16:1::2  0         0         100 200 300 400i
D 55:0:0:2::/64 172:16:1::2  0         0         100 200 300 400i

Total number of prefixes: 3
OS10#

```

Example routes

```

OS10# show ip bgp ipv6 unicast neighbors 172:16:1::2 routes
BGP local router ID is 100.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric    LocPrf    Weight  Path
*>55::/64      172:16:1::2  44        55        0       i
*>55:0:0:1::/64 172:16:1::2  44        55        0       i
*>55:0:0:2::/64 172:16:1::2  44        55        0       i

```

```

*>55:0:0:3::/64      172:16:1::2      44      55      0      i
*>55:0:0:4::/64      172:16:1::2      44      55      0      i
*>55:0:0:5::/64      172:16:1::2      44      55      0      i
*>55:0:0:6::/64      172:16:1::2      44      55      0      i
*>55:0:0:7::/64      172:16:1::2      44      55      0      i
*>55:0:0:8::/64      172:16:1::2      44      55      0      i
*>55:0:0:9::/64      172:16:1::2      44      55      0      i

Total number of prefixes: 10
OS10#

```

Supported Releases 10.3.0E or later

show ip bgp peer-group

Displays information on BGP peers in a peer-group.

Syntax `show ip bgp [vrf vrf-name] peer-group peer-group-name`

Parameters

- `vrf vrf-name` — (OPTIONAL) Enter the keyword `vrf` to view information on BGP peers in a peer group corresponding to that VRF.
- `peer-group-name` — (Optional) Enter the peer group name to view information about that peer-group only.

Default Not configured

Command Mode EXEC

Usage Information

- `Peer-group` — Displays the peer group name. Minimum time displays the time interval between BGP advertisements.
- `Administratively shut` — Displays the peer group's status if you do not enable the peer group. If you enable the peer group, this line does not display.
- `BGP version` — Displays the BGP version supported.
- `Description` — Displays the descriptive name configured for the BGP peer template. This field is displayed only when the description is configured.
- `For address family` — Displays IPv4 unicast as the address family.
- `BGP neighbor` — Displays the name of the BGP neighbor.
- `Number of peers` — Displays the number of peers currently configured for this peer group.
- `Peer-group members` — Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, an * displays next to the IP address.

Example

```

OS10# show ip bgp peer-group bgppg
Peer-group bgppg, remote AS 103
  BGP version 4
  Minimum time between advertisement runs is 30 seconds
  Description: peer_template_1_abcd
  For address family: Unicast
  BGP neighbor is bgppg, peer-group external
  Update packing has 4_OCTET_AS support enabled

```

Example (Summary)

```

OS10# show ip bgp peer-group ebgp summary
BGP router identifier 32.1.1.1 local AS number 6
Neighbor      AS      MsgRcvd  MsgSent  Up/Down  State/Pfx
17.1.1.2      7       7        6        00:01:54 5

```

Supported Releases 10.2.0E or later

show ip bgp summary

Displays the status of all BGP connections.

Syntax	<code>show ip bgp [vrf vrf-name] summary</code>
Parameters	<code>vrf vrf-name</code> — (OPTIONAL) Enter the keyword <code>vrf</code> and then the name of the VRF to view the status of all BGP connections corresponding to that VRF.
Default	Not configured
Command Mode	EXEC
Usage Information	<ul style="list-style-type: none">• <code>Neighbor</code>—Displays the BGP neighbor address.• <code>AS</code>—Displays the AS number of the neighbor• <code>MsgRcvd</code>—Displays the number of BGP messages that the neighbor received.• <code>MsgSent</code>—Displays the number of BGP messages that the neighbor sent.• <code>Up/Down</code>—Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word <code>never</code> displays. The output format is:

```
1 day = 00:12:23 (hours:minutes:seconds), 1 week = 1d21h (DaysHours),
1 week + 11w2d (WeeksDays)
```

- `State/PfxRcd`—If the neighbor is in the Established stage, the number of network prefixes received. If a maximum limit was configured with the neighbor maximum-prefix command, `prfxd` appears in this column. If the neighbor is not in the Established stage, the current stage - Idle, Connect, Active, OpenSent, OpenConfirm displays. When the peer is transitioning between states and clearing the routes received, the phrase `Purging` may appear in this column. If the neighbor is disabled, the phrase `Admin shut` appears in this column.

The suppressed status of aggregate routes may not display in the command output.

Example

```
OS10# show ip bgp summary
BGP router identifier 80.1.1.1 local AS number 102
Neighbor    AS      MsgRcvd  MsgSent  Up/Down    State/Pfx
80.1.1.2    800    24       23       00:09:15   5
```

Supported Releases 10.2.0E or later

soft-reconfiguration inbound

Enables soft-reconfiguration for a neighbor.

Syntax	<code>soft-reconfiguration inbound</code>
Parameters	None
Default	Not configured
Command Modes	ROUTER-BGP-NEIGHBOR-AF
Usage Information	This command is not supported on a peer-group level. To enable soft-reconfiguration for peers in a peer-group, this command must be enabled at a per-peer level. With soft-reconfiguration inbound, all updates received from this neighbor are stored unmodified, regardless of the inbound policy. When inbound soft-reconfiguration is performed later, the stored information is used to generate a new set of inbound updates. The <code>no</code> version of this command disables soft-reconfiguration inbound for a BGP neighbor.

Example (IPv4)

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
```

Example (IPv6)

```
OS10(conf-router-neighbor)# address-family ipv6 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
```

Supported Releases 10.3.0E or later

template

Creates a peer-group template to assign it to BGP neighbors.

Syntax `template template-name`

Parameters `template-name` — Enter a peer-group template name (up to 16 characters).

Default Not configured

Command Mode CONFIG-ROUTER-BGP

Usage Information Members of a peer-group template inherit the configuration properties of the template and share the same update policy. The `no` version of this command removes a peer-template configuration.

NOTE: To configure these settings for a non default VRF instance, you must first enter the ROUTER-CONFIG-VRF sub mode using the following commands:

1. Enter the ROUTER BGP mode using the `router bgp as-number` command.
2. From the ROUTER BGP mode, enter the ROUTER BGP VRF mode using the `vrf vrf-name` command.

Example

```
OS10(conf-router-bgp-10)# template solar
OS10(conf-router-bgp-template)#
```

Supported Releases 10.3.0E or later

timers

Adjusts BGP keepalive and holdtime timers.

Syntax `timers keepalive holdtime`

- Parameters**
- `keepalive`—Enter the time interval (in seconds) between keepalive messages sent to the neighbor routers, from 1 to 65535.
 - `holdtime`—Enter the time interval (in seconds) between the last keepalive message and declaring a router dead, from 3 to 65535.

Default `keepalive 60 seconds; holdtime 180 seconds`

Command Mode ROUTER-BGP

Usage Information The configured timer value becomes effective after a BGP hard reset. The timer values negotiate from peers. The `no` version of this command resets the value to the default.

Example

```
OS10(conf-router-bgp)# timers 30 90
```

Supported Releases 10.3.0E or later

vrf

Enters the CONFIG-ROUTER-VRF command mode.

Syntax `vrf vrf-name`

Parameters None

Default None

Command Mode ROUTER-BGP

Usage Information This mode enables you to apply BGP configurations to non default VRFs.

Example

```
OS10(config)#router bgp 100
OS10(config-router-bgp-100)#
OS10(config-router-bgp-100)#vrf vrf_test1

OS10(config-router-bgp-100-vrf)#
```

Supported Releases 10.3.0E or later

weight

Assigns a default weight for routes from the neighbor interfaces.

Syntax `weight number`

Parameters *number*—Enter a number as the weight for routes, from 1 to 4294967295.

Default 0

Command Mode ROUTER-BGP-NEIGHBOR

Usage Information The path with the highest weight value is preferred in the best-path selection process. The `no` version of this command resets the value to the default.

Example

```
OS10(conf-router-bgp-neighbor)# weight 4096
```

Supported Releases 10.3.0E or later

Equal cost multi-path

ECMP is a routing technique where next-hop packet forwarding to a single destination occurs over multiple best paths. OS10 uses a hashing algorithm to determine the next-hop when you enable ECMP. The hashing algorithm makes hashing decisions based on values in various packet fields as well as some internal values.

- Configure the hash algorithm in CONFIGURATION mode.

```
hash-algorithm ecmp crc
```

Change hash algorithm

```
OS10(config)# hash-algorithm ecmp crc
```

Load balancing

RTAG7 is a hashing algorithm that load balances traffic within a trunk group in a controlled manner. To effectively increase the bandwidth of ECMP routes, traffic is balanced across member links. The balancing is performed by using the RTAG7 hashing, which is designed to have the member links used effectively as the traffic profile gets more diverse.

The RTAG7 hash scheme generates a hash that consists of two parts:

- The first part is primarily generated from packet headers to identify micro-flows in traffic. By default, all listed parameters are enabled for load balancing except the ingress port.

```
OS10# show load-balance

Load-Balancing Configuration For LAG and ECMP:
```



```

-----
IPV4 Load Balancing      : Enabled
IPV6 Load Balancing      : Enabled
MAC Load Balancing       : Enabled
TCP-UDP Load Balancing   : Enabled
Ingress Port Load Balancing : Disabled
IPV4 FIELDS      : source-ip destination-ip protocol vlan-id l4-destination-port l4-
source-port
IPV6 FIELDS      : source-ip destination-ip protocol vlan-id l4-destination-port l4-
source-port
MAC FIELDS       : source-mac destination-mac  ethertype  vlan-id
TCP-UDP FIELDS: l4-destination-port  l4-source-port

```

- The second part comes from static physical configuration such as ingress and egress port numbers.

You can change the hash field to generate load balancing based on any parameters using the `load-balance` command.

ECMP commands

hash-algorithm

Changes the hash algorithm that distributes traffic flows across ECMP paths and the LAG.

Syntax `hash-algorithm {ecmp | lag} crc`

- Parameters**
- `ecmp` — Enables ECMP hash configuration.
 - `lag` — Enables LAG hash configuration for L2 only.
 - `crc` — Enables CRC polynomial for hash computation.

Default `crc`

Command Mode CONFIGURATION

Usage Information The hash value calculated with this command is unique to the entire system. Different hash algorithms are based on the number of port-channel members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, use this command to designate another algorithm.

When a port-channel member leaves or is added to the port-channel, the hash algorithm is recalculated to balance traffic across the members. The `no` version of this command returns the value to the default.

Example

```
OS10(config)# hash-algorithm lag crc
```

Supported Releases 10.3.0E or later

link-bundle-utilization trigger-threshold

Configures a threshold value to trigger monitoring of traffic distribution on an ECMP link bundle.

Syntax `link-bundle-trigger-threshold value`

Parameters `value` — Enter a link bundle trigger threshold value (0 to 100).

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables the configuration.

Example

```
OS10(config)# link-bundle-trigger-threshold 80
```

Supported Releases 10.2.0E or later

load-balancing

Distributes or load balances incoming traffic using the default parameters in the hash algorithm.

Syntax	<code>load-balancing {ingress-port enable [tcp-udp-selection l4-destination-port l4-source-port] [ip-selection destination-ip source-ip protocol vlan-id l4-destination-port l4-source-port] [ipv6-selection destination-ip source-ip protocol vlan-id l4-destination-port l4-source-port] [mac-selection destination-mac source-mac ethertype vlan-id]}</code>
Parameters	<ul style="list-style-type: none">• <code>ingress-port enable</code> — Enables load-balancing on ingress ports.• <code>tcp-udp-selection</code> — Enables the TCP UDP port for load-balancing configuration.• <code>ip-selection</code> — Enables IPv4 key parameters to use in the hash computation.• <code>ipv6-selection</code> — Enables IPV6 key parameters to use in hash computation.• <code>destination-ip</code> — Enables the destination IP address in the hash calculation.• <code>source-ip</code> — Enables the source IP address in the hash calculation.• <code>protocol</code> — Enables the protocol information in the hash calculation.• <code>vlan-id</code> — Enables the VLAN ID information in the hash calculation.• <code>l4-destination-port</code> — Enables the L4 destination port information in the hash calculation.• <code>l4-source-port</code> — Enables the L4 source port information in the hash calculation.• <code>mac-selection</code> — Enables MAC load-balancing configurations.• <code>destination-mac</code> — Enables the destination MAC information in hash the calculation.• <code>source-mac</code> — Enables the source MAC information in the hash calculation.• <code>ethertype</code> — Enables the Ethernet type information in the hash calculation.
Default	<ul style="list-style-type: none">• <code>ip-selelection-source-ip dest-ip vlan-id l4-source-port l4-dest-port ipv4 protocol</code>• <code>ipv6-selection-source-ipv6 dest-ipv6 vlan-id l4-source-port l4-dest-port ipv6 protocol</code>• <code>mac-selection-source-mac destination-mac vlan-id ethertype</code>• <code>tcp-udp-selection-l4-source-port l4-dest-port</code>
Command Mode	CONFIGURATION
Usage Information	<ul style="list-style-type: none">• IPv4- selection: <code>source-ip destination-ip protocol vlan-id l4-destination-port l4-source-port</code>• IPv6 destination address: <code>source-ip destination-ip protocol vlan-id l4-destination-port l4-source-port</code>• MAC parameters: <code>source-mac destination-mac ethertype vlan-id</code>• TCP/UDP parameters: <code>l4-destination-port l4-source-port</code> <p>The no version of this command resets the value to the default.</p>
Example (Ingress)	<pre>OS10(config)# load-balancing ingress-port enable</pre>
Example (IP Selection)	<pre>OS10(config)# load-balancing ip-selection destination-ip source-ip</pre>
Supported Releases	10.2.0E or later

show hash-algorithm

Displays the hash-algorithm information.

Syntax	<code>show hash-algorithm</code>
Parameters	None
Default	Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show hash-algorithm
      EcmpAlgo - crc LabAlgo - crc
```

Supported Releases 10.3.0E or later

IPv4 routing

OS10 supports IPv4 addressing including variable-length subnetting mask (VLSM), Address Resolution Protocol (ARP), static routing, and routing protocols. With VLSM, you can configure one network with different masks. You can also use supernetting, which increases the number of subnets. You can add a mask to the IP address to separate the network and host portions of the IP address to add a subnet.

You need to configure IPv4 routing for IP hosts to communicate with one another in the same network, or in different networks.

Assign interface IP address

You can assign primary and secondary IP addresses to a physical or logical interface to enable IP communication between the system and hosts connected to a specific interface. Assign one primary address and secondary IP addresses to each interface. By default, all ports are in the default VLAN—VLAN 1.

1. Enter the interface type information to assign an IP address in CONFIGURATION mode.

```
interface interface
```

- ethernet—Physical interface
- port-channel—Port-channel ID number
- vlan—VLAN ID number
- loopback—Loopback interface ID
- mgmt—Management interface

2. Enable the interface in INTERFACE mode.

```
no shutdown
```

3. Remove the interface from the default VLAN in INTERFACE mode.

```
no switchport
```

4. Configure a primary IP address and mask on the interface in INTERFACE mode.

```
ip address ip-address mask [secondary]
```

- *ip-address mask*—Enter the IP address in dotted decimal format—A.B.C.D. and mask in slash prefix-length format (/24).
- *secondary*—Enter a secondary backup IP address for the interface.

Assign interface IP address to interface

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# ip address 10.10.1.4/8
```

View interface configuration

```
OS10# show interface ethernet 1/1/1
Ethernet 1/1/1 is up, line protocol is up
```

```

Hardware is Dell EMC Eth, address is 00:0c:29:98:1b:79
  Current address is 00:0c:29:98:1b:79
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
  Wavelength is 64
  SFP receive power reading is 0.0
Interface index is 16866084
Internet address is not set
Mode of IPv4 Address Assignment: not set
MTU 1532 bytes
LineSpeed 40G, Auto-Negotiation on
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 3 weeks 1 day 23:12:50
Queuing strategy: fifo
Input statistics:
  0 packets, 0 octets
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output statistics:
  0 packets, 0 octets
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
  Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
  Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 3 weeks 1 day 20:54:37

```

Configure static routing

You can configure a manual or static route for OSPF.

- Configure a static route in CONFIGURATION mode.

```
ip route ip-prefix/mask {next-hop | interface interface [route-preference]}
```

- *ip-prefix*—IPv4 address in dotted decimal format—A.B.C.D.
- *mask*—Mask in slash prefix-length format (/X).
- *next-hop*—Next-hop IP address in dotted decimal format—A.B.C.D.
- *interface*—Interface type with the node/slot/port information
- *route-preference*—(Optional) Route-preference range—1 to 255.

Configure static routes

```
OS10(config)# ip route 200.200.200.0/24 10.1.1.2
```

View configured static routes

```

OS10# show ip route static
Codes: C - connected
       S - static
       B - BGP, IN - internal BGP, EX - external BGP
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
Destination          Gateway                Dist/Metric Last Change
-----
S 200.200.200.0/24 via 10.1.1.2 ethernet1/1/1 0/0      00:00:03

```

OS10 installs a static route if the next hop is on a directly connected subnet. A next-hop that is not on the directly connected subnet which recursively resolves to a next-hop on the interface's configured subnet is also automatically configured. For

example, if interface `ethernet 1/1/5` has IP address on subnet `100.0.0.0/8`, and if `10.1.1.0/24` recursively resolves to `100.1.1.1`, the system installs the static route:

- When the interface goes down, OS10 withdraws the route.
- When the interface comes up, OS10 reinstalls the route.
- When the recursive resolution is *broken*, OS10 withdraws the route.
- When the recursive resolution is satisfied, OS10 reinstalls the route.

Address Resolution Protocol

Address Resolution Protocol (ARP) runs over Ethernet and enables end stations to learn the MAC addresses of neighbors on an IP network. Using ARP, OS10 automatically updates the *ARP cache* table which maps the MAC addresses to their corresponding IP addresses. The *ARP cache* enables dynamically learned addresses to be removed after a configured period.

Configure static ARP entries

You can manually configure static entries in the ARP mapping table. Dynamic ARP is vulnerable to spoofing. To avoid spoofing, configure static entries. Static entries take precedence over dynamic ARP entries.

1. Configure an IP address and MAC address mapping for an interface in INTERFACE mode.

```
ip arp ip-address mac address
```

- *ip-address*—IP address in dotted decimal format—A.B.C.D.
- *mac address*—MAC address in nnnn.nnnn.nnnn format

These entries do not age, and you can only remove them manually. To remove a static ARP entry, use the `no arp ip-address` command.

Configure static ARP entries

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ip arp 10.1.1.5 08:00:20:b7:bd:32
```

View ARP entries

```
OS10# show ip arp interface ethernet 1/1/6
!
interface ethernet1/1/6
ip arp 10.1.1.5 08:00:20:b7:bd:32
no shutdown
!
```

IPv4 routing commands

clear ip arp

Clears the dynamic ARP entries from a specific interface or optionally delete (no-refresh) ARP entries from the content addressable memory (CAM).

Syntax `clear ip arp [vrf vrf-name] [interface interface | ip ip-address] [no-refresh]`

- Parameters**
- *vrf vrf-name* — Enter the keyword `vrf` followed by the name of the VRF to clear ARP entries corresponding to that VRF.
 - *interface interface*— (Optional) Specify an interface type:
 - `ethernet` — Physical interface.
 - `port-channel` — Port-channel identifier.
 - `vlan` — VLAN identifier.
 - `loopback` — Loopback interface identifier.
 - *ip ip-address* — (Optional) Specify the IP address of the ARP entry you want to clear.

- `no-refresh` — (Optional) Specify to delete the ARP entry from CAM. You can also use this option with `interface` or `ip ip-address` to specify which dynamic ARP entries you want to delete.

Default Not configured

Command Mode EXEC

Usage Information Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and re-installed in CAM. Use this option with extreme caution.

Example

```
OS10# clear ip arp interface ethernet 1/1/5
```

Supported Releases 10.2.0E or later

clear ip route

Clears the specified routes from the IP routing table.

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

- Parameters**
- `vrf vrf-name` — (Optional) Enter the keyword `vrf` and then the name of the VRF to clear the routes corresponding to that VRF.
 - `*` — Specify to clear the entire IP routing table. This option refreshes all the routes in the routing table and the traffic flow is affected for all the routes in the switch.
 - `A.B.C.D/mask` — Specify the IP route to be removed from the IP routing table. This option refreshes all the routes in the routing table, but the traffic flow is affected only for the specified route in the switch.

Default Not configured

Command Mode EXEC

Usage Information This command does not remove the static routes from the routing table.

Example

```
OS10# clear ipv6 route 10.1.1.0/24
```

Supported Releases 10.3.0E or later

ip address

Configures IP address to an interface.

Syntax `ip address ip-address/mask`

Parameters `ip-address/mask` — Enter the IP address.

Defaults None

Command Mode INTERFACE

Usage Information The `no` version of this command removes the IP address set for the interface.

Example

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# ip address 10.1.1.0/24
```

Supported Releases 10.3.0E or later

ip address dhcp

Enables DHCP client operations on the interface.

Syntax	<code>ip address dhcp</code>
Parameters	None
Defaults	None
Command Mode	INTERFACE
Usage Information	The <code>no</code> version of this command disables the DHCP operations on the interface.

Example

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# ip address dhcp
```

Supported Releases	10.3.0E or later
---------------------------	------------------

ip arp

Configures static ARP and maps the IP address of the neighbor to a MAC address.

Syntax	<code>ip arp mac-address</code>
Parameters	<code>mac-address</code> — Enter the MAC address of IP neighbor in A.B.C.D format.
Default	Not configured
Command Mode	INTERFACE
Usage Information	Do not use Class D (multicast) or Class E (reserved) IP addresses. Zero MAC addresses (00:00:00:00:00:00) are also invalid. The <code>no</code> version of this command disables IP ARP configuration.

Example

```
OS10(conf-if-eth1/1/6)# ip arp 10.1.1.5 08:00:20:b7:bd:32
```

Supported Releases	10.2.0E or later
---------------------------	------------------

ip route

Assigns a static route on the network device.

Syntax	<code>ip route [dst-vrf vrf-name] ip-prefix mask {next-hop interface interface-type [route-preference]}</code>
Parameters	<ul style="list-style-type: none">• <code>dst-vrf vrf-name</code> — (Optional) Enter the keyword <code>vrf</code> and then the name of the VRF to configure a static route corresponding to that VRF. Use this VRF option after the <code>ip route</code> keyword to configure a static route on that specific VRF.• <code>ip-prefix</code> — Enter the IP prefix in dotted decimal format (A.B.C.D).• <code>mask</code> — Enter the mask in slash prefix-length format (/x).• <code>next-hop</code> — Enter the next-hop IP address in dotted decimal format (A.B.C.D).• <code>interface interface-type</code> — Enter the interface type and interface information. The interface types supported are: Ethernet, port-channel, VLAN, and Null.• <code>route-preference</code> — (Optional) Enter the range (1 to 255).
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes a static route configuration.

Example

```
OS10(config)# ip route 200.200.200.0/24 10.1.1.2
```

```
OS10(config)# ip route 200.200.200.0/24 interface null 0
```

Supported Releases

10.2.0E or later

show ip arp

Displays the ARP table entries for specific a IP address or MAC address, static, dynamic, and a summary of all ARP entries.

Syntax

```
show ip arp [vrf vrf-name] [interface [ethernet | vlan | port-channel] | ip-address | mac-address | static | dynamic | summary]
```

Parameters

- *vrf vrf-name* — Enter the keyword *vrf* followed by the name of the VRF to display ARP entries correspond VRF.
- *interface* — (Optional) Enter the keyword and interface information:
 - *ethernet* — Enter the node/slot/port[:subport] information.
 - *vlan* — Enter the VLAN ID number (1 to 4093).
 - *port-channel* — Enter the port-channel ID number (1 to 128).
- *ip-address* — (Optional) Enter the IP address for the ARP entry in A.B.C.D format.
- *mac-address* — (Optional) Enter the MAC address in nn:nn:nn:nn:nn:nn format.
- *static* — (Optional) Enter the keyword to display static ARP entries.
- *dynamic* — (Optional) Enter the keyword to display dynamic ARP entries.
- *summary* — (Optional) Enter the keyword to display a summary of all ARP entries.

Default

Not configured

Command Mode

EXEC

Usage Information

This command shows both static and dynamic ARP entries.

Example (IP Address)

```
OS10# show ip arp ip 192.168.2.2
```

```
Protocol Address Age(min) Hardware Address Interface VLAN CPU
-----
Internet 192.168.2.2 98 00:01:e8:8b:3c:01 Te 1/0 V1 101 CP
```

Example (Static)

```
OS10# show ip arp summary
```

```
Total Entries          Static Entries          Dynamic Entries
-----
          3994                  0                  3994
```

```
OS10# show ip arp 100.1.2.1
```

```
Protocol Address          Hardware Address          Interface
-----
Internet 100.1.2.1          00:a0:c9:00:01:04          port-channel11
```

```
OS10# show ip arp dynamic
```

```
Protocol Address          Hardware Address          Interface
-----
Internet 9.0.0.2            00:24:00:00:00:00          ethernet1/1/10
Internet 100.1.1.1          00:a0:c9:00:01:04          port-channel11
Internet 100.1.2.1          00:a0:c9:00:01:04          port-channel11
Internet 100.1.3.1          00:a0:c9:00:01:04          port-channel11
Internet 100.1.4.1          00:a0:c9:00:01:04          port-channel11
Internet 100.1.5.1          00:a0:c9:00:01:04          port-channel11
Internet 100.1.6.1          00:a0:c9:00:01:04          port-channel11
Internet 100.1.7.1          00:a0:c9:00:01:04          port-channel11
Internet 100.1.8.1          00:a0:c9:00:01:04          port-channel11
```


Example (Dynamic)

```
OS10# show ip arp dynamic

Protocol Address Age(min) Hardware Address Interface VLAN CPU
-----
Internet 10.16.127.143 163 00:01:e8:75:c1:bb Ma 1/0 - CP
Internet 10.16.127.254 63 00:01:e8:75:c1:bb Ma 1/0 - CP
Internet 10.16.131.4 62 00:01:e8:8b:3b:e3 Ma 1/0 - CP
Internet 10.16.131.254 19 00:01:e8:75:c1:bb Ma 1/0 - CP
Internet 192.168.1.1 - 00:01:e8:8b:39:43 - Vl 100 CP
Internet 192.168.1.2 99 00:01:e8:8b:3c:01 Te 1/0 Vl 100 CP
```

Supported Releases

10.2.0E or later

show ip route

Displays IP route information.

Syntax

```
show ip route [vrf vrf-name] [all | bgp | connected | ospf process-id |
static | ip-prefix/mask | summary]
```

Parameters

- `vrf vrf-name` — (Optional) Enter the keyword `vrf` and then the VRF name to list the routes in the route table of a specific VRF.
- `all` — (Optional) Displays both active and non-active IP routes.
- `bgp` — (Optional) Displays BGP route information.
- `connected` — (Optional) Displays only the directly connected routes.
- `ospf process-id` — (Optional) Displays route information for the OSPF process (1 to 65535).
- `static` — (Optional) Displays static route information.
- `ip-prefix/mask` — (Optional) Displays routes for the destination prefix-list.
- `summary` — (Optional) Displays an IP route summary.

Defaults

Not configured

Command Mode

EXEC

Usage

None

Information

Example

```
OS10# show ip route
Codes: C - connected
       S - static
       B - BGP, IN - internal BGP, EX - external BGP
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
Destination          Gateway                Dist/Metric  Last Change
-----
C    10.1.1.0/24      via 10.1.1.1  vlan100      0/0          01:16:56
B EX 10.1.2.0/24      via 10.1.2.1  vlan101      20/0         01:16:56
O    10.1.3.0/24      via 10.1.3.1  vlan102     110/2        01:16:56
B IN 10.1.4.0/24      via 10.1.4.1  vlan103     200/0        01:16:56
```

Supported Releases

10.2.0E or later

IPv6 routing

OS10 supports IPv6 routing and addressing, including the Neighbor Discovery Protocol (NDP), stateless IPv6 address autoconfiguration, and stateful IPv6 address configuration. Configure IPv6 routing for IP hosts to communicate with one another in the same network, or in different networks.

Enable or disable IPv6

By default:

- IPv6 forwarding is enabled on physical Ethernet interfaces, VLANs, and port groups. IPv6 forwarding is disabled only when you enable IPv6 address autoconfiguration on an interface and set it in host mode (`ipv6 address autoconfig`).
- IPv6 forwarding is permanently disabled on the management Ethernet interface so that it remains in Host mode and does not operate as a router regardless of the `ipv6 address autoconfig` setting.

If necessary, you can manually disable IPv6 processing on an interface so that the configured IPv6 addresses do not take effect. The IPv6 addresses take effect again when you re-enable IPv6.

If you disable IPv6 and configure a L2 interface in L3 mode, IPv6 is not automatically re-enabled on the interface. You must manually re-enable it.

A link-local address is automatically generated when you re-enable IPv6 on an interface with the `ipv6 enable` command.

Disable and enable IPv6

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address 2111:dddd:0eee::22/64
OS10(conf-if-eth1/1/8)# no ipv6 address autoconfig
OS10(conf-if-eth1/1/8)# no ipv6 enable
OS10(conf-if-eth1/1/8)# ipv6 enable
```

Display IPv6 status

```
OS10# show interface ethernet 1/1/20
Ethernet 1/1/20 is up, line protocol is up
Hardware is Dell EMC Eth, address is ec:f4:bb:fb:fa:30
  Current address is ec:f4:bb:fb:fa:30
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
  Wavelength is 850
  Receive power reading is 0.0
Interface index is 17305562
Internet address is 20.20.20.1/24
Mode of IPv4 Address Assignment: MANUAL
Interface IPv6 oper status: Enabled
Link local IPv6 address: fe80::eef4:bbff:fe80:fa30/64
Global IPv6 address: 2020::1/64
...
```

```
OS10# show ipv6 interface brief
Interface Name      admin/protocol  IPv6 Address/Link-Local Address  IPv6 Oper Status
=====
Ethernet 1/1/1:1    up / up        fe80::eef4:bbff:fe80:f9f0/64
                  2017::1/64
                  Enabled
Ethernet 1/1/20    up / up        fe80::eef4:bbff:fe80:fa30/64
                  2020::1/64
                  Enabled
Management 1/1/1   up / up        fe80::eef4:bbff:fe80:f9ef/64
                  Enabled
Vlan 1             up / up        fe80::eef4:bbff:fe80:fa59/64
                  Enabled
```

IPv6 addresses

An IPv6 address consists of a 48-bit global routing prefix, optional 16-bit subnet ID, and a 64-bit interface identifier in the extended universal identifier (EUI)-64 format.

IPv6 128-bit addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons: `x:x:x:x:x:x:x`.

```
2001:0db8:0000:0000:0000:0000:1428:57a
```

Leading zeros in each field are optional. You can also use two colons (`::`) to represent successive hexadecimal fields of zeros, but you can use this short version only once in each address:

```
2001:db8::1428:57ab
```

In the following example, all the addresses are valid and equivalent:

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8:0000:0000:0000::1428:57ab
- 2001:0db8:0:0:0:0:1428:57ab
- 2001:0db8:0:0::1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8::1428:57ab

IPv6 networks are written using CIDR notation. An IPv6 network (or subnet) is a contiguous group of IPv6 addresses the size of which must be a power of two. The initial bits of addresses, which are identical for all hosts in the network, are the network's prefix.

A network is denoted by the first address in the network and the size in bits of the prefix (in decimal), separated with a slash. Because a single host is seen as a network with a 128-bit prefix, host addresses may be written with a following /128.

For example, 2001:0db8:1234::/48 stands for the network with addresses 2001:0db8:1234:0000:0000:0000:0000 through 2001:0db8:1234:ffff:ffff:ffff:ffff:ffff.

As soon as an IPv6 address is assigned, IPv6 packet processing is enabled on an interface. You can manually disable and re-enable IPv6 processing on an interface configured with an IPv6 address using the `no ipv6 enable` and `ipv6 enable` commands.

To remove all IPv6 addresses from an interface, use the `no ipv6 address` command. To remove a specific IPv6 address, use the `ipv6 address ipv6-address/mask` command.

Link-local addresses

When an OS10 switch boots up, an IPv6 unicast link-local address is automatically assigned to an interface using stateless configuration. A link-local address allows IPv6 devices on a local link to communicate without requiring a globally unique address. IPv6 reserves the address block FE80::/10 for link-local unicast addressing.

Global addresses

To enable stateless autoconfiguration of an IPv6 global address and set the interface to Host mode, use the `ipv6 address autoconfig` command. The router receives network prefixes in IPv6 router advertisements (RAs). An interface ID is appended to the prefix. In Host mode, IPv6 forwarding is disabled.

The `no ipv6 address autoconfig` command disables IPv6 global address autoconfiguration, and sets the interface to Router mode with IPv6 forwarding enabled.

DHCP-assigned addresses

As an alternative to stateless autoconfiguration, you can enable a network host to obtain IPv6 addresses using a DHCP server via stateful autoconfiguration using the `ipv6 address dhcp` command. A DHCPv6 server uses a prefix pool to configure a network address on an interface. The interface ID is automatically generated.

Manally configured addresses

An interface can have multiple IPv6 addresses. To configure an IPv6 address in addition to the link-local address, use the `ipv6 address ipv6-address/mask` command. Enter the full 128-bit IPv6 address, including the network prefix and a 64-bit interface ID.

You can also manually configure an IPv6 address by assigning:

- A network prefix with the EUI-64 parameter using the `ipv6 address ipv6-prefix eui64` command. A 64-bit interface ID is automatically generated based on the MAC address.
- A link-local address to use instead of the link-local address that is automatically configured when you enable IPv6 using the `ipv6 address link-local` command.

Configure IPv6 address

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address 2001:dddd:0eee::4/64
```

Configure network prefix

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address 2001:FF21:1:1::/64 eui64
```

Configure link-local address

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address FE80::1/64 link-local
```

Stateless autoconfiguration

When an interface comes up, OS10 uses stateless autoconfiguration to generate a unique link-local IPv6 address with a FE80::/64 prefix and an interface ID generated from the MAC address. To use stateless autoconfiguration to assign a globally unique address using a prefix received in router advertisements, enter the `ipv6 address autoconfig` command.

Stateless autoconfiguration sets an interface in host mode, and allows the interface connected to an IPv6 network to autoconfigure IPv6 addresses and communicate with other IPv6 devices on local links. A DHCP server is not required for automatic IPv6 interface configuration. IPv6 devices on a local link send router advertisement (RA) messages in response to solicitation messages received at startup.

Stateless autoconfiguration of IPv6 addresses is performed using:

Prefix advertisement	Routers use router advertisement messages to advertise the network prefix. Hosts append their interface-identifier MAC address to generate a valid IPv6 address.
Duplicate address detection	An IPv6 host node checks whether that address is used anywhere on the network using this mechanism before configuring its IPv6 address.
Prefix renumbering	Transparent renumbering of hosts in the network when an organization changes its service provider.

IPv6 provides the flexibility to add prefixes on router advertisements in response to a router solicitation (RS). By default, RA response messages are sent when an RS message is received. The system manipulation of IPv6 stateless autoconfiguration supports the router side only. Neighbor Discovery (ND) messages advertise so the neighbor can use the information to auto-configure its address. Received ND messages are not used to create an IPv6 address.

Inconsistencies in router advertisement values between routers are logged. The values checked for consistency include:

- Current hop limit
- M and O flags
- Reachable time
- Retransmission timer
- MTU options
- Preferred and valid lifetime values for the same prefix

The router redirect functionality in the NDP is similar to IPv4 router redirect messages. NDP uses ICMPv6 redirect messages (Type 137) to inform nodes that a better router exists on the link.

Neighbor Discovery

The IPv6 NDP determines if neighboring IPv6 devices are reachable and receives the IPv6 addresses of IPv6 devices on local links. Using the link-layer and global prefixes of neighbor addresses, OS10 performs stateless autoconfiguration of IPv6 addresses on interfaces.

ICMPv6 Router Advertisement messages advertise the IPv6 addresses of IPv6-enabled interfaces and allow a router to learn of any address changes in IPv6 neighbors. By default, router advertisements are disabled on an interface.

Prerequisites

To enable RA messages, the switch must be in Router mode with IPv6 forwarding enabled and stateless autoconfiguration disabled (`no ipv6 address autoconfig` command).

Enable router advertisement messages

1. Enable IPv6 neighbor discovery and sending ICMPv6 RA messages in Interface mode.

```
ipv6 nd send-ra
```

2. (Optional) Configure IPv6 neighbor discovery options in Interface mode.

- `ipv6 nd hop-limit hops` — (Optional) Sets the hop limit advertised in RA messages and included in IPv6 data packets sent by the router (0 to 255; default 64). 0 indicates that no hop limit is specified by the router.
- `ipv6 nd managed-config-flag` — (Optional) Sent in RA messages to tell hosts to use stateful address autoconfiguration, such as DHCPv6, to obtain IPv6 addresses.
- `ipv6 nd max-ra-interval seconds` — (Optional) Sets the maximum time interval for sending RA messages (4 to 1800 seconds; default 600).
- `ipv6 nd mtu number` — (Optional) Sets the maximum transmission unit (MTU) used in RA messages on the link (1280 to 65535 bytes; default 1500). By default, no MTU setting is included in RA messages.
- `ipv6 nd other-config-flag` — (Optional) Tells hosts to use stateful autoconfiguration to obtain nonaddress-related information.
- `ipv6 nd ra-lifetime seconds` — (Optional) Sets the lifetime of a default router in RA messages (0 to 9000 milliseconds; default 3 times the `max-ra-interval` setting). 0 indicates that this router is not used as a default router.
- `ipv6 nd reachable-time milliseconds` — (Optional) Sets the advertised time for which the router sees that a neighbor is up after it receives neighbor reachability confirmation (0 to 3600000 milliseconds; default 0). 0 indicates that no reachable time is sent in RA messages.
- `ipv6 nd retrans-timer seconds` — (Optional) Sets the time between retransmitting neighbor solicitation messages (100 to 4292967295 milliseconds). By default, no retransmit timer is configured.

3. Configure the IPv6 prefixes that are advertised by IPv6 neighbor discovery in Interface mode.

```
ipv6 nd prefix {ipv6-prefix | default} [no-advertise] [no-autoconfig] [no-rtr-
address]
[off-link] [lifetime {valid-lifetime seconds | infinite}
{preferred-lifetime seconds | infinite}]
```

- `ipv6-prefix` — Enter an IPv6 prefix in `x:x::y/mask` format to include the prefix in RA messages. Include prefixes that are not already in the subnets configured on the interface.
- `default` — Configure the prefix parameters advertised in all subnets configured on the interface.
- `no-advertise` — (Optional) Do not advertise the specified prefix. By default, all prefixes in configured subnets are advertised.
- `no-autoconfig` — (Optional) Sets `AdvAutonomous` to `Off` for the specified prefix in the `radvd.conf` file. This setting tells hosts to not use this prefix for address autoconfiguration. By default, `AdvAutonomous` is `On`.
- `no-rtr-address` — (Optional) Sets `AdvRouterAddr` to `Off` for the prefix in the `radvd.conf` file. The `Off` setting tells hosts to not use the advertising router address for on-link determination. By default, `AdvRouterAddr` is `On`.
- `off-link` — (Optional) Sets `AdvOnLink` to `Off` for the prefix in the `radvd.conf` file. The `Off` setting tells hosts to not use this prefix for on-link determination. By default, `AdvOnLink` is `On`.
- `lifetime {valid-lifetime seconds | infinite}` — (Optional) Sets `AdvValidLifetime` (in seconds) for the prefix in the `radvd.conf` file. The prefix is valid for on-link determination only for the specified lifetime. The default is 86400 seconds (1 day). The `infinite` setting allows the prefix to be valid for on-link determination with no time limit.
- `lifetime {preferred-lifetime seconds | infinite}` — (Optional) Sets `AdvPreferredLifetime` (in seconds) for the prefix in the `radvd.conf` file. IPv6 addresses generated from the prefix using stateless autoconfiguration remain preferred for the configured lifetime. The default is 14400 seconds (4 hours). The `infinite` setting allows addresses that are autoconfigured using the prefix to be preferred with no time limit.

By default, all prefixes configured in IPv6 addresses on an interface are advertised. To modify the default values advertised for interface subnet prefixes, use the `ipv6 nd prefix default` command and specify new default settings.

On-link determination is the process used to forward IPv6 packets to a destination IPv6 address.

Configure neighbor discovery

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd mtu 1500
OS10(conf-if-eth1/1/1)# ipv6 nd send-ra
```

Configure advertised IPv6 prefixes

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd prefix default lifetime infinite infinite
OS10(conf-if-eth1/1/1)# ipv6 nd prefix 2002::/64
```

Duplicate address discovery

To determine if an IPv6 unicast address is unique before assigning it to an interface, an OS10 switch sends a neighbor solicitation message. If the process of duplicate address discovery (DAD) detects a duplicate address in the network, the address is not configured on the interface. DAD is enabled by default.

By default, IPv6 is not disabled when a duplicate address is detected. Only the duplicate address is not applied. Other IPv6 addresses are still active on the interface.

To disable IPv6 on an interface when a duplicate link-local address is detected, use the `ipv6 nd dad disable-ipv6-on-failure` command. To re-enable IPv6 after you resolve a duplicate link-local address, enter `no ipv6 enable`, followed by `ipv6 enable`.

- Disable or re-enable IPv6 duplicate address discovery in Interface mode.

```
ipv6 nd dad {disable | enable}
```

- Disable IPv6 on an interface if a duplicate link-local address is discovered in Interface mode.

```
ipv6 nd dad disable-ipv6-on-dad-failure
```

Disable duplicate address discovery

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd dad disable
```

Disable IPv6 for duplicate link-local address

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd dad disable-ipv6-on-dad-failure
```

Static IPv6 routing

To define an explicit route between two IPv6 networking devices, configure a static route on an interface. Static routing is useful for smaller networks with only one path to an outside network, or to provide security for certain traffic types in a larger network.

- Enter the static routing information including the IPv6 address and mask in `x:x:x:x` format in CONFIGURATION mode—prefix length 0 to 64.

```
ipv6 route ipv6-prefix/mask {next-hop | interface interface [route-preference]}
```

- *next-hop* — Enter the next-hop IPv6 address in `x:x:x:x` format.
- *interface interface* — Enter the interface type then the slot/port or number information.
- *route-preference* — (Optional) Enter a route-preference range—1 to 255.

After you configure a static IPv6 route, configure the forwarding router's address on the interface. The IPv6 neighbor interface must have an IPv6 address configured.

Configure IPv6 static routing and view configuration

```
OS10(config)# ipv6 route 2111:dddd:0eee::22/128 2001:db86:0fff::2
OS10(config)# do show ipv6 route static
Codes: C - connected
       S - static
       B - BGP, IN - internal BGP, EX - external BGP
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
  Destination          Gateway                Dist/Metric    Last Change
-----
S 2111:dddd:eee::22/12via 2001:db86:fff::2 ethernet1/1/1  1/1  00:01:24
```

IPv6 destination unreachable

By default, when no matching entry for an IPv6 route is found in the IPv6 routing table, a packet is dropped and no error message is sent. You can enable the capability to send an `IPv6 destination unreachable` error message to the source without dropping the packet.

Enable IPv6 unreachable destination messaging

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 unreachable
```

IPv6 hop-by-hop options

A hop-by-hop header extension in an IPv6 packet contains options that are processed by all IPv6 routers in the packet's path. By default, hop-by-hop header options in an IPv6 packet are not processed locally. To enable local processing of IPv6 hop-by-hop options on an interface, use the `ipv6 hop-by-hop` command.

Enable IPv6 hop-by-hop options forwarding

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 hop-by-hop
```

View IPv6 information

To view IPv6 configuration information, use the `show ipv6 route` command. To view IPv6 address information, use the `show address ipv6` command.

View IPv6 connected information

```
OS10# show ipv6 route connected
Codes: C - connected
       S - static
       B - BGP, IN - internal BGP, EX - external BGP
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
Destination          Gateway                Dist/Metric  Last Change
-----
C 2001:db86::/32    via 2001:db86:fff::1 ethernet1/1/1  0/0    00:03:24
```

View IPv6 static information

```
OS10# show ipv6 route static
Codes: C - connected
       S - static
       B - BGP, IN - internal BGP, EX - external BGP
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
Destination          Gateway                Dist/Metric  Last Change
-----
S 2111:dddd:eee::22/12 via 2001:db86:fff::2 ethernet1/1/1  1/1    00:01:24
```

IPv6 commands

clear ipv6 neighbors

Delete all entries in the IPv6 neighbor discovery cache or neighbors of a specific interface. Static entries are not removed using this command.

Syntax	<code>clear ipv6 neighbors [vrf vrf-name] [ipv6-address interface]</code>
Parameters	<ul style="list-style-type: none">• <code>vrf vrf-name</code> — (Optional) Enter the keyword <code>vrf</code> followed by the name of the VRF to clear the neighbor corresponding to that VRF. If you do not specify this option, the neighbors in the default VRF are cleared.• <code>ipv6-address</code> — Enter the IPv6 address of the neighbor in the <code>x:x:x::x</code> format to remove a specific IPv6 neighbor. The <code>::</code> notation specifies successive hexadecimal fields of zero.• <code>interface interface</code> — To remove all neighbor entries learned on a specific interface, enter the keyword <code>interface</code> then the interface type and slot/port or number information of the interface:<ul style="list-style-type: none">○ For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport[/subport] information.○ For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.○ For a port channel interface, enter the keywords <code>port-channel</code> then a number.○ For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4093.
Defaults	None.
Command Mode	EXEC
Usage Information	The <code>no</code> version of this command resets the value to the default.
Example	
Supported Releases	10.4.1.0 or later or later

clear ipv6 route

Clears routes from the IPv6 routing table.

Syntax	<code>clear ipv6 route [vrf vrf-name] {* A::B/mask}</code>
Parameters	<ul style="list-style-type: none">• <code>vrf vrf-name</code> — (Optional) Enter the keyword <code>vrf</code> followed by the name of the VRF to clear the IPv6 routes corresponding to that VRF.• <code>*</code> — Clears all routes and refreshes the IPv6 routing table. Traffic flow for all the routes in the switch is affected.• <code>A::B/mask</code> — Removes the IPv6 route and refreshes the IPv6 routing table. Traffic flow in the switch is affected only for the specified route.
Default	Not configured
Command Mode	EXEC
Usage Information	This command does not remove the static routes from the routing table.
Example	<pre>OS10# clear ipv6 route *</pre>
Supported Releases	10.3.0E or later

ipv6 address

Configures a global unicast IPv6 address on an interface.

Syntax	<code>ipv6 address ipv6-address/prefix-length</code>
Parameters	<code>ipv6-address/prefix-length</code> — Enter a full 128-bit IPv6 address with the network prefix length, including the 64-bit interface identifier.
Defaults	None
Command Mode	INTERFACE
Usage Information	<ul style="list-style-type: none">• An interface can have multiple IPv6 addresses. To configure an IPv6 address in addition to the link-local address, enter the <code>ipv6 address ipv6-address/mask</code> command and specify the complete 128-bit IPv6 address. To configure a globally unique IPv6 address by entering only the network prefix and length, use the <code>ipv6 address ipv6-prefix/prefix-length eui-64</code> command.• The <code>no</code> version of this command removes the IPv6 address on the interface.
Example	<pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# ipv6 address 2111:dddd:0eee::22/64</pre>
Supported Releases	10.3.0E or later

ipv6 address autoconfig

Acquires global IPv6 addresses by using the network prefix obtained from router advertisements.

Syntax	<code>ipv6 address autoconfig</code>
Parameters	None
Defaults	Disabled except on the management interface
Command Mode	INTERFACE
Usage Information	<ul style="list-style-type: none">• This command sets an interface in Host mode to perform IPv6 stateless auto-configuration by discovering prefixes on local links, and adding an EUI-64 based interface identifier to generate each IPv6 address. The command disables IPv6 forwarding. Addresses are configured depending on the prefixes received in router advertisement messages.• The <code>no</code> version of this command disables IPv6 address autoconfiguration, resets the interface in Router mode, and re-enables IPv6 forwarding.
Example	<pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# no switchport OS10(conf-if-eth1/1/1)# ipv6 address autoconfig OS10(conf-if-eth1/1/1)#</pre>
Supported Releases	10.3.0E or later

ipv6 address dhcp

Enables DHCP client operations on the interface.

Syntax	<code>ipv6 address dhcp</code>
Parameters	None
Defaults	None
Command Mode	INTERFACE
Usage Information	The <code>no</code> version of this command disables the DHCP operations on the interface.

Example

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# ipv6 address dhcp
```

Supported Releases 10.3.0E or later

ipv6 enable

Enables and disables IPv6 forwarding on an interface configured with an IPv6 address.

Syntax `ipv6 enable`

Parameters None

Defaults None

Command Mode INTERFACE

Usage Information

- The `no` version of this command disables IPv6 forwarding.
- Use this command to disable and re-enable IPv6 forwarding on an interface for security purposes or to recover from a duplicate address discovery (DAD) failure.

Example

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 address 2111:dddd:0eee::22/128
OS10(conf-if-eth1/1/1)# no ipv6 enable
OS10(conf-if-eth1/1/1)# ipv6 enable
```

Supported Releases 10.3.0E or later

ipv6 address eui-64

Configures a global IPv6 address on an interface by entering only the network prefix and length.

Syntax `ipv6 address ipv6-prefix/prefix-length eui-64`

Parameters *ipv6-prefix* — Enter an IPv6 prefix in `x::y/mask` format.

Defaults None

Command Mode INTERFACE

Usage Information Use this command to manually configure an IPv6 address in addition to the link-local address generated with stateless autoconfiguration. Specify only the network prefix and length. The 64-bit interface ID is automatically computed from the MAC address. This command enables IPv6 processing on the interface. The `no` version of this command removes the IPv6 address configuration.

Example

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# ipv6 address 2111:dddd:0eee::/64 eui-64
```

Supported Releases 10.4.0E(R1) or later

ipv6 address link-local

Configures a link-local IPv6 address on the interface to use instead of the link-local address that is automatically configured with stateless autoconfiguration.

Syntax `ipv6 address ipv6-prefix link-local`

Parameters *ipv6-prefix* — Enter an IPv6 prefix in `x::y/mask` format.

Defaults None

Command Mode	INTERFACE
Usage Information	<ul style="list-style-type: none"> An interface can have only one link-local address. By default, an IPv6 link-local address is automatically generated with a MAC-based EUI-64 interface ID when a router boots up and IPv6 is enabled. Use this command to manually configure a link-local address to replace the autoconfigured address. For example, to configure a more user-friendly link-local address, replace <code>fe80::eef4:bfff:febf:fa30/64</code> with <code>fe80::1/64</code>. The <code>no</code> version of this command removes the specified link-local address.
Example	<pre>OS10(config)# interface mgmt 1/1/1 OS10(conf-if-ma-1/1/1)# ipv6 address 2111:dddd:0eee::22/64 link-local</pre>
Supported Releases	10.4.0E(R1) or later

ipv6 hop-by-hop

Enables and disables processing hop-by-hop options in IPv6 packet headers.

Syntax	<code>ipv6 hop-by-hop</code>
Parameters	None
Defaults	Hop-by-hop header options in an IPv6 packet are not processed on an interface.
Command Mode	INTERFACE
Usage Information	<ul style="list-style-type: none"> Use this command to enable local processing of IPv6 packets with hop-by-hop options in conformance with RFC 8200, IPv6 Specification. The <code>no</code> version of this command disables IPv6 processing of hop-by-hop header options.
Example: Disable hop-by-hop option processing	<pre>OS10(config)# interface ethernet 1/2/3 OS10(conf-if-eth1/2/3)# no ipv6 hop-by-hop</pre>
Supported Releases	10.4.0E(R1) or later

ipv6 nd dad

Disables or re-enables IPv6 duplicate address discovery (DAD).

Syntax	<code>ipv6 nd dad {disable enable disable-ipv6-on-dad-failure}</code>
Parameters	<ul style="list-style-type: none"> <code>disable</code> — Disable duplicate address discovery on the interface. <code>enable</code> — Re-enable IPv6 duplicate address discovery if you have disabled it. <code>disable-ipv6-on-dad-failure</code> — Enable duplicate address discovery on the existing autoconfigured link-local address.
Defaults	Duplicate address discovery is enabled on an interface.
Command Mode	INTERFACE
Usage Information	<ul style="list-style-type: none"> An OS10 switch sends a neighbor solicitation message to determine if an autoconfigured IPv6 unicast link-local address is unique before assigning it to an interface. If the process of duplicate address discovery (DAD) detects a duplicate address in the network, the link-local address is not configured. Other IPv6 addresses are still active on the interface. By default, DAD does not disable IPv6 if a duplicate link-local address is detected in the network. To disable IPv6 on an interface when a duplicate link-local address is detected, use the <code>ipv6 nd dad disable-ipv6-on-failure</code> command.
Example: Disable DAD	<pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# ipv6 nd dad disable</pre>

Example: Enable DAD on link-local address

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd dad disable-ipv6-on-dad-failure
```

Supported Releases

10.4.0E(R1) or later

ipv6 nd hop-limit

Sets the hop limit advertised in RA messages and included in IPv6 data packets sent by the router.

Syntax

```
ipv6 nd hop-limit hops
```

Parameters

- `hop-limit hops` — Enter the maximum number of hops allowed for RA messages (0 to 255).

Defaults

64 hops

Command Mode

INTERFACE

Usage Information

The configured hop limit is advertised in RA messages and included in IPv6 data packets sent by the router. 0 indicates that no hop limit is specified by the router.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd hop-limit 100
```

Supported Releases

10.4.0E(R1) or later

ipv6 nd managed-config-flag

Sends RA messages that tell hosts to use stateful address autoconfiguration, such as DHCPv6, to obtain IPv6 addresses.

Syntax

```
ipv6 nd managed-config-flag
```

Parameters

None

Defaults

Not configured

Command Mode

INTERFACE

Usage Information

The no version of this command disables the `managed-config-flag` option in RA messages.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd managed-config-flag
```

Supported Releases

10.4.0E(R1) or later

ipv6 nd max-ra-interval

Sets the maximum time interval between sending RA messages.

Syntax

```
ipv6 nd max-ra-interval seconds
```

Parameters

- `max-ra-interval seconds` — Enter a time interval in seconds (4 to 1800).

Defaults

600 seconds

Command Mode

INTERFACE

Usage Information

The no version of this command restores the default time interval used to send RA messages.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd max-ra-interval 300
```

Supported Releases

10.4.0E(R1) or later

ipv6 nd mtu

Sets the maximum transmission unit (MTU) used on a local link in RA messages.

Syntax

```
ipv6 nd mtu number
```

Parameters

- *mtu number* — Enter the MTU size in bytes (1280 to 65535).

Defaults

1500 bytes

Command Mode

INTERFACE

Usage Information

The `no` version of this command restores the default MTU value advertised in RA messages.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd mtu 2500
```

Supported Releases

10.4.0E(R1) or later

ipv6 nd other-config-flag

Sends RA messages that tell hosts to use stateful autoconfiguration to obtain nonaddress-related information.

Syntax

```
ipv6 nd other-config-flag
```

Parameters

None

Defaults

Not configured

Command Mode

INTERFACE

Usage Information

The `no` version of this command disables the `other-config-flag` option in RA messages.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd other-config-flag
```

Supported Releases

10.4.0E(R1) or later

ipv6 nd prefix

Configures the IPv6 prefixes that are included in Router Advertisement (RA) messages to neighboring IPv6 routers.

Syntax

```
ipv6 nd prefix {ipv6-prefix | default} [no-advertise] [no autoconfig]
[no-rtr-address] [off-link] [lifetime {valid-lifetime seconds | infinite}
{preferred-lifetime seconds | infinite}]
```

Parameters

- *ipv6-prefix* — Enter an IPv6 prefix in `x::y/mask` format to include the prefix in RA messages. Include prefixes that are not already in the subnets configured on the interface.
- `default` — Configure the prefix parameters advertised in all subnets configured on the interface.
- `no-advertise` — (Optional) Do not advertise the specified prefix. By default, all prefixes in configured subnets are advertised.

- `no-autoconfig` — (Optional) Sets `AdvAutonomous` to `Off` for the specified prefix in the `radvd.conf` file. This setting tells hosts to not use this prefix for address autoconfiguration. By default, `AdvAutonomous` is `On`.
- `no-rtr-address` — (Optional) Sets `AdvRouterAddr` to `Off` for the prefix in the `radvd.conf` file. The `Off` setting tells hosts to not use the advertising router's address for on-link determination. By default, `AdvRouterAddr` is `On`.
- `off-link` — (Optional) Sets `AdvOnLink` to `Off` for the prefix in the `radvd.conf` file. The `Off` setting tells hosts to not use this prefix for on-link determination. By default, `AdvOnLink` is `On`.
- `lifetime {valid-lifetime seconds | infinite}` — (Optional) Sets `AdvValidLifetime` (in seconds) for the prefix in the `radvd.conf` file. The prefix is valid for on-link determination only for the specified lifetime. The default is 86400 seconds (1 day). The `infinite` setting allows the prefix to be valid for on-link determination with no time limit.
- `lifetime {preferred-lifetime seconds | infinite}` — (Optional) Sets `AdvPreferredLifetime` (in seconds) for the prefix in the `radvd.conf` file. IPv6 addresses generated from the prefix using stateless autoconfiguration remain preferred for the configured lifetime. The default is 14400 seconds (4 hours). The `infinite` setting allows addresses that are autoconfigured using the prefix to be preferred with no time limit.

Defaults All prefixes in IPv6 subnets configured on an interface are advertised.

Command Mode INTERFACE

- Usage Information**
- By default, all prefixes configured in IPv6 addresses on an interface are advertised. To advertise all default parameters in the subnet prefixes on an interface, enter the `default` keyword.
 - If you configure a prefix with valid or preferred lifetime values, the `ipv6 nd prefix default no autoconfig` command does not apply the default prefix values.
 - On-link determination is used to forward IPv6 packets to a destination IPv6 address.

Examples

Enable router advertisements

```
OS10(conf-if-eth1/1/1)# ipv6 address 2001:0db8:2000::1/64
OS10(conf-if-eth1/1/1)# ipv6 nd send-ra
```

Change default settings for interface subnet prefixes

```
OS10(conf-if-eth1/1/1)# ipv6 nd prefix default lifetime infinite infinite
```

Disable advertising an interface subnet prefix

```
OS10(conf-if-eth1/1/1)# ipv6 nd prefix 2001:0db8:2000::/64 no-advertise
```

Advertise prefix for which there is no interface address

```
OS10(conf-if-eth1/1/1)# ipv6 nd prefix 2001:0db8:3000::/64 no-autoconfig
```

Supported Releases 10.4.0E(R1) or later

ipv6 nd ra-lifetime

Sets the lifetime of the default router in RA messages.

Syntax `ipv6 nd ra-lifetime seconds`

Parameters • `ra-lifetime seconds` — Enter a lifetime value in milliseconds (0 to 9000 milliseconds).

Defaults 3 times the `max-ra-interval` value

Command Mode INTERFACE

Usage Information The `no` version of this command restores the default lifetime value. 0 indicates that this router is not used as the default router.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd max-ra-interval 300
```

Supported Releases 10.4.0E(R1) or later

ipv6 nd reachable-time

Sets the advertised time for which the router sees a neighbor to be up after it receives a reachability confirmation.

Syntax `ipv6 nd reachable-time milliseconds`

Parameters • `reachable-time milliseconds` — Enter the reachable time in milliseconds (0 to 3600000).

Defaults 0

Command Mode INTERFACE

Usage Information The `no` version of this command restores the default reachable time. 0 indicates that no reachable time is sent in RA messages.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd reachable-time 1000
```

Supported Releases 10.4.0E(R1) or later

ipv6 nd retrans-timer

Sets the time between retransmitting neighbor solicitation messages.

Syntax `ipv6 nd retrans-timer seconds`

Parameters • `retrans-timer seconds` — Enter the retransmission time interval in milliseconds (100 to 4292967295).

Defaults Not configured

Command Mode INTERFACE

Usage Information The `no` version of this command disables the configured retransmission timer.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd retrans-timer 1000
```

Supported Releases 10.4.0E(R1) or later

ipv6 nd send-ra

Enables the sending of ICMPv6 Router Advertisement messages.

Syntax `ipv6 nd send-ra`

Parameters None

Defaults RA messages are disabled.

Command Mode INTERFACE

Usage Information • Using ICMPv6 Router Advertisement messages, the NDP advertises the IPv6 addresses of IPv6-enabled interfaces and learns of any address changes in IPv6 neighbors. Before you enable sending

RA messages, the switch must be in Router mode with IPv6 forwarding enabled and stateless autoconfiguration disabled (`no ipv6 address autoconfig` command).

- The `no ipv6 nd send-ra` command disables RA messages.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd send-ra
```

Supported Releases

10.4.0E(R1) or later

ipv6 route

Configures a static IPv6 static route.

Syntax

```
ipv6 route [dst-vrf vrf-name] ipv6-prefix mask {next-hop | interface
interface-type [route-preference]}
```

Parameters

- `dst-vrf vrf-name` — (Optional) Enter the keyword `vrf` followed by the name of the VRF to install IPv6 routes in that VRF.
- `ipv6-prefix` — Enter the IPv6 address in `x:x:x:x` format
- `mask` — Enter the mask in slash prefix-length format (`/x`)
- `next-hop` — Enter the next-hop IPv6 address in `x:x:x:x` format.
- `interface interface-type` — Enter the interface type then the slot/port or number information. The interface types supported are: Ethernet, port-channel, VLAN, and Null.
- `route-preference` — (Optional) Enter a route-preference range (1 to 255).

Default

Not configured

Command Mode

CONFIGURATION

Usage Information

- When the interface fails, the system withdraws the route. The route reinstalls when the interface comes back up. When a recursive resolution is broken, the system withdraws the route. The route reinstalls when the recursive resolution is satisfied. After you create an IPv6 static route interface, if you do not assign an IP address to a peer interface, you must manually ping the peer to resolve the neighbor information.
- The `no` version of this command deletes the IPv6 route configuration.

Example

```
OS10(config)# ipv6 route 2111:ddd:0ee::22/128 2001:db86:0fff::2
```

```
OS10(config)# ipv6 route 2111:ddd:0ee::22/128 interface null 0
```

Supported Releases

10.2.0E or later

ipv6 unreachable

Enables the generation of error messages on an interface for IPv6 packets with unreachable destinations.

Syntax

```
ipv6 unreachable
```

Parameters

None

Defaults

ICMPv6 unreachable messages are not sent.

Command Mode

INTERFACE

Usage Information

- By default, when no matching entry for an IPv6 route is found in the IPv6 routing table, the packet is dropped and no error message is sent. Use this command to enable sending an `IPv6 destination unreachable` error message to the source without dropping the packet.
- The `no` version of this command disables the generation of unreachable destination messages.

Example

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 unreachable
```

Supported Releases

10.4.0E(R1) or later

show ipv6 neighbors

Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the control processor (CP).

Syntax

```
show ipv6 neighbors [vrf vrf-name] [ipv6-address| interface interface]
```

Parameters

- `vrf vrf-name` — (Optional) Enter the keyword `vrf` and the name of the VRF to display the neighbors corresponding to that VRF. If you do not specify this option, neighbors corresponding to the default VRF are displayed.
- `ipv6-address` — Enter the IPv6 address of the neighbor in the `x:x:x::x` format. The `::` notation specifies successive hexadecimal fields of zero.
- `interface interface` — Enter the keyword `interface` then the interface type and slot/port or number information:
 - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port/subport[/subport] information.
 - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
 - For a port channel interface, enter the keywords `port-channel` then a number.
 - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4093.

Defaults

None.

Command Mode

EXEC

Usage

Information

The `no` version of this command resets the value to the default.

Example

```
OS10# show ipv6 neighbors
IPv6 Address Expires(min) Hardware Address State Interface VLAN CPU
-----
100::1 0.03 00:00:00:00:00:22 DELAY Te 1/12 - CP
fe80::200:ff:fe00:22 232 00:00:00:00:00:22 STALE Te 1/12 - CP
500::1 0.60 00:01:e8:17:5c:af REACH Te 1/13 - CP
fe80::200:ff:fe00:17 232 00:00:00:00:00:29 REACH Te 1/14 - CP
900::1 0.60 00:01:e8:17:5c:b1 STALE Po 23 - CP
400::1 0.60 00:01:e8:17:5c:ae REACH Te 1/2 V1 100 CP
OS10#
```

Supported Releases

10.4.1.0 or later or later

show ipv6 route

Displays IPv6 routes.

Syntax

```
show ipv6 route [vrf vrf-name] [all | bgp | connected | static | A::B/mask
| summary]
```

Parameters

- `vrf vrf-name` — (Optional) Enter the keyword `vrf` followed by the name of the VRF to display IPv6 routes corresponding to that VRF. If you do not specify this option, routes corresponding to the default VRF are displayed.
- `all`—(Optional) Displays all routes including nonactive routes.
- `bgp`—(Optional) Displays BGP route information.
- `connected`—(Optional) Displays only the directly connected routes.
- `static`—(Optional) Displays all static routes.

- *A::B/mask*—(Optional) Enter the IPv6 destination address and mask.
- *summary*—(Optional) Displays the IPv6 route summary.

Default Not configured

Command Mode EXEC

Usage Information None

Example (All)

```
OS10# show ipv6 route all
Codes: C - connected
       S - static
       B - BGP, IN - internal BGP, EX - external BGP
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
  Destination          Gateway                Dist/Metric    Last Change
-----
-----
```

Example (Connected)

```
OS10# show ipv6 route connected
Codes: C - connected
       S - static
       B - BGP, IN - internal BGP, EX - external BGP
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
  Destination          Gateway                Dist/Metric    Last Change
-----
-----
C    2001:db86::/32 via 2001:db86:fff::1 ethernet1/1/1 0/0 00:03:24
```

Example (Summary)

```
OS10# show ipv6 route summary
Route Source          Active Routes  Non-Active Routes
-----
Ospf                  0              0
Bgp                   0              0
Connected             0              0
Static                0              0
Ospf Inter-area      0              0
NSSA External-1      0              0
NSSA External-2      0              0
Ospf External-1      0              0
Ospf External-2      0              0
Bgp Internal          0              0
Bgp External          0              0
Ospf Intra-area      0              0
Total                 0              0
```

Supported Releases 10.2.0E or later

show ipv6 interface brief

Displays IPv6 interface information.

Syntax show ipv6 interface brief

Parameters brief — Displays a brief summary of IPv6 interface information.

Defaults None

Command Mode EXEC

Usage Information Use the do show ipv6 interface brief command to view IPv6 interface information in other modes.

Example (Brief)

```
OS10# show ipv6 interface brief

Interface      admin/  IPV6 Address/      IPv6 Oper
Name           protocol Link-Local Address      Status
=====
Management 1/1/1 up/up fe80::20c:29ff:fe54:c852/64 Enabled
Vlan 1       up/up fe80::20c:29ff:fe54:c8bc/64 Enabled
Ethernet 1/1/2 up/up fe80::20c:29ff:fe54:c853/64
100::1/64
1001:1:1:1:20c:29ff:fe54:c853/64 Enabled
Ethernet 1/1/3 up/up fe80::4/64
3000::1/64
4000::1/64 Disabled
Ethernet 1/1/4 up/up fe80::4/64
4::1/64
5::1/64 Enabled
```

Supported Releases

10.2.0E or later or later

Internet Group Management Protocol

Internet Group Management Protocol (IGMP) is a communications protocol that hosts use on IPv4 networks to establish multicast group memberships.

OS10 supports IGMPv1, IGMPv2, and IGMPv3 to manage the multicast group memberships on IPv4 networks.

 **NOTE:** OS10 does not support IGMP snooping in VLT environments.

IGMP snooping

IGMP snooping enables switches to use the information in IGMP packets and generate a forwarding table that associates ports with multicast groups. When switches receive multicast frames, they forward them to their intended receivers.

OS10 supports IGMP snooping on VLAN interfaces.

Configure IGMP snooping

- Enable IGMP snooping globally with the `ip igmp snooping enable` command in the CONFIGURATION mode. This command enables IGMP snooping on all VLAN interfaces.
- (Optional) You can disable IGMP snooping on specific VLAN interfaces using the `no ip igmp snooping` command in the VLAN INTERFACE mode.
- In a network, the snooping switch is connected to a multicast Router that sends IGMP queries. On a Layer 2 network that does not have a multicast router, you can configure the snooping switch to act as querier. Use the `ip igmp snooping querier` command in the VLAN INTERFACE mode to send the queries.
- OS10 learns the multicast router interface dynamically based on the interface on which IGMP membership query is received. To assign a multicast router interface statically, use the `ip igmp snooping mrouter interface interface-type` command in VLAN INTERFACE mode.
- (Optional) Configure the IGMP version using the `ip igmp version version-number` command in the VLAN INTERFACE mode.
- (Optional) The fast leave option allows the IGMP snooping switch to remove an interface from the multicast group immediately on receiving the leave message. Enable fast leave with the `ip igmp snooping fast-leave` command in VLAN INTERFACE mode.
- (Optional) Configure the time interval for sending IGMP general queries with the `ip igmp snooping query-interval query-interval-time` command in VLAN INTERFACE mode.
- (Optional) Configure the maximum time for responding to a query advertised in IGMP queries using the `ip igmp snooping query-max-resp-time query-response-time` command in VLAN INTERFACE mode.
- (Optional) Configures the time interval between group-specific IGMP query messages with the `ip igmp snooping last-member-query-interval query-interval-time` command in VLAN INTERFACE mode.

IGMP snooping configuration

```
OS10(config)# ip igmp snooping enable
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping mrouter interface ethernet 1/1/32
OS10(conf-if-vl-100)# ip igmp snooping querier
OS10(conf-if-vl-100)# ip igmp version 3
OS10(conf-if-vl-100)# ip igmp snooping fast-leave
OS10(conf-if-vl-100)# ip igmp snooping query-interval 60
OS10(conf-if-vl-100)# ip igmp snooping query-max-resp-time 10
OS10(conf-if-vl-100)# ip igmp snooping last-member-query-interval 1000
```

View IGMP snooping information

```
OS10# show ip igmp snooping groups
Total Number of Groups: 480
IGMP Connected Group Membership
Group Address          Interface          Mode              Expires
225.1.0.0              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.1              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.2              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.3              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.4              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.5              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.6              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.7              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.8              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.9              vlan3531          IGMPv2-Compat    00:01:35
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
--more--
```

<<Output Truncated>>

```
OS10# show ip igmp snooping interface
Vlan100 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface
```

```
show ip igmp snooping mrouter
Interface      Router Ports
Vlan 100      ethernet 1/1/32
```

IGMP snooping commands

ip igmp snooping

Enables IGMP snooping on the specified VLAN interface.

Syntax ip igmp snooping

Parameters	None
Default	Depends on the global configuration.
Command Mode	VLAN INTERFACE
Usage Information	When you enable IGMP snooping globally, the configuration is applied to all the VLAN interfaces. You can disable the IGMP snooping on specified VLAN interfaces. The <code>no</code> version of this command disables the IGMP snooping on the specified VLAN interface.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# no ip igmp snooping</pre>
Supported Releases	10.4.0E(R1) or later

ip igmp snooping enable

Enables IGMP snooping globally.

Syntax	<code>ip igmp snooping enable</code>
Parameters	None
Default	Disabled
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command disables the IGMP snooping.
Example	<pre>OS10(config)# ip igmp snooping enable</pre>
Supported Releases	10.4.0E(R1) or later

ip igmp snooping fast-leave

Enables fast leave in IGMP snooping for specified VLAN.

Syntax	<code>ip igmp snooping fast-leave</code>
Parameters	None
Default	Disabled
Command Mode	VLAN INTERFACE
Usage Information	The fast leave option allows the IGMP snooping switch to remove an interface from the multicast group immediately on receiving the leave message. The <code>no</code> version of this command disables the fast leave functionality.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ip igmp snooping fast-leave</pre>
Supported Releases	10.4.1.0 or later

ip igmp snooping last-member-query-interval

Configures the time interval between group-specific IGMP query messages.

Syntax	<code>ip igmp snooping last-member-query-interval <i>query-interval-time</i></code>
---------------	---

Parameters	<i>query-interval-time</i> —Enter the query time interval in milliseconds, ranging from 100 to 65535.
Default	1000 milliseconds
Command Mode	VLAN INTERFACE
Usage Information	The <code>no</code> version of this command resets the last member query interval time to the default value.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ip igmp snooping last-member-query-interval 2500</pre>
Supported Releases	10.4.1.0 or later

ip igmp snooping mrouter

Enables IGMP querier on the specified VLAN interface.

Syntax	<code>ip igmp snooping mrouter interface <i>interface-type</i></code>
Parameters	<i>interface-type</i> —Enter the interface type details. The interface should be a member of the VLAN.
Default	Not configured
Command Mode	VLAN INTERFACE
Usage Information	The <code>no</code> version of this command removes the multicast router configuration from the VLAN member port.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ip igmp snooping mrouter interface ethernet 1/1/1</pre>
Supported Releases	10.4.0E(R1) or later

ip igmp snooping querier

Enables IGMP querier processing for the specified VLAN interface.

Syntax	<code>ip igmp snooping querier</code>
Parameters	None
Default	Not configured
Command Mode	VLAN INTERFACE
Usage Information	The <code>no</code> version of this command disables the IGMP querier on the VLAN interface..
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ip igmp snooping querier</pre>
Supported Releases	10.4.0E(R1) or later

ip igmp snooping query-interval

Configures time interval for sending IGMP general queries.

Syntax	<code>ip igmp snooping query-interval <i>query-interval-time</i></code>
Parameters	<i>query-interval-time</i> —Enter the interval time in seconds, ranging from 2 to 18000.

Default	60 seconds
Command Mode	VLAN INTERFACE
Usage Information	The <code>no</code> version of this command resets the query interval to the default value.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ip igmp snooping query-interval 120</pre>
Supported Releases	10.4.1.0 or later

ip igmp query-max-resp-time

Configures the maximum time for responding to a query advertised in IGMP queries.

Syntax	<code>ip igmp snooping query-max-resp-time <i>query-response-time</i></code>
Parameters	<i>query-response-time</i> —Enter the query response time in seconds, ranging from 1 to 25.
Default	10 seconds
Command Mode	VLAN INTERFACE
Usage Information	The <code>no</code> version of this command resets the query response time to default value.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ip igmp snooping query-max-resp-time 15</pre>
Supported Releases	10.4.1.0 or later

ip igmp version

Configures IGMP version.

Syntax	<code>ip igmp version <i>version-number</i></code>
Parameters	<i>version-number</i> —Enter the version number as 2 or 3.
Default	3
Command Mode	VLAN INTERFACE
Usage Information	The <code>no</code> version of this command resets the version number to the default value.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ip igmp version 2</pre>
Supported Releases	10.4.1.0 or later

show ip igmp snooping groups

Displays the details of IGMP snooping group membership.

Syntax	<code>show ip igmp snooping groups [vlan <i>vlan-id</i> [<i>ip-address</i>]]</code>
Parameters	<ul style="list-style-type: none"> <i>vlan-id</i>—(Optional) Enter the VLAN ID, ranging from 1 to 4093. <i>ip-address</i>—(Optional) Enter the IP address of the multicast group.

Default Not configured
Command Mode EXEC
Usage Information None

Example

```
OS10# show ip igmp snooping groups
Total Number of Groups: 480
IGMP Connected Group Membership
Group Address          Interface          Mode
Expires
225.1.0.0              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.1              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.2              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.3              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.4              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.5              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.6              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.7              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.8              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.9              vlan3031          IGMPv2-Compat
00:01:26
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.10             vlan3031          IGMPv2-Compat
00:01:26
--more--
<<Output Truncated>>
```

Example (with VLAN)

```
OS10# show ip igmp snooping groups vlan 3031
Total Number of Groups: 12
IGMP Connected Group Membership
Group Address          Interface          Mode
Expires
225.1.0.0              vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.1              vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.2              vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.3              vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.4              vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.5              vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
```



```

225.1.0.6          vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.7          vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.8          vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.9          vlan3031          IGMPv2-Compat
00:01:30
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.10         vlan3031          IGMPv2-Compat
00:01:30
--more--

```

Example (with VLAN and multicast IP address)

```

OS10# show ip igmp snooping groups vlan 3031 225.1.0.0
IGMP Connected Group Membership
Group Address          Interface          Mode
Expires
225.1.0.0             vlan3031          IGMPv2-Compat
00:01:44
  Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1

```

Supported Releases

10.4.0E(R1) or later

show ip igmp snooping groups detail

Displays the IGMP source information along with detailed member port information. .

Syntax

```

show ip igmp snooping groups [vlan vlan-id [ip-address]]show ip igmp
snooping groups [vlan vlan-id] [group ip-address] detail

```

Parameters

- *vlan-id*—(Optional) Enter the VLAN ID, ranging from 1 to 4093.
- *ip-address*—(Optional) Enter the IP address of the multicast group.

Default

Not configured

Command Mode

EXEC

Usage Information

None

Example

```

OS10# show ip igmp snooping groups detail
Interface          vlan3041
Group              232.11.0.0
Source List
101.41.0.21
  Member Port      Mode          Uptime          Expires
  port-channel51   Include       1d:20:26:07    00:01:41
  ethernet1/1/51:1 Include       1d:20:26:05    00:01:46
  ethernet1/1/52:1 Include       1d:20:26:08    00:01:46

Interface          vlan3041
Group              232.11.0.1
Source List
101.41.0.21
  Member Port      Mode          Uptime          Expires
  port-channel51   Include       1d:20:26:07    00:01:41
  ethernet1/1/51:1 Include       1d:20:26:05    00:01:46
  ethernet1/1/52:1 Include       1d:20:26:08    00:01:46

Interface          vlan3041
Group              232.11.0.2
Source List
101.41.0.21

```

```

Member Port      Mode      Uptime      Expires
port-channel51  Include  1d:20:26:07 00:01:41
--more-- <<Output Truncated>>

```

Example (with VLAN)

```

OS10# show ip igmp snooping groups vlan 3041 detail
Interface      vlan3041
Group          232.11.0.0
Source List
101.41.0.21
Member Port      Mode      Uptime      Expires
port-channel51  Include  1d:20:26:07 00:01:41
ethernet1/1/51:1 Include  1d:20:26:05 00:01:46
ethernet1/1/52:1 Include  1d:20:26:08 00:01:46

Interface      vlan3041
Group          232.11.0.1
Source List
101.41.0.21
Member Port      Mode      Uptime      Expires
port-channel51  Include  1d:20:26:07 00:01:41
ethernet1/1/51:1 Include  1d:20:26:05 00:01:46
ethernet1/1/52:1 Include  1d:20:26:08 00:01:46

Interface      vlan3041
Group          232.11.0.2
Source List
101.41.0.21
Member Port      Mode      Uptime      Expires
port-channel51  Include  1d:20:26:07 00:01:41
--more--

```

Example (with VLAN and multicast IP address)

```

OS10# show ip igmp snooping groups vlan 3041 232.11.0.0 detail
Interface      vlan3041
Group          232.11.0.0
Source List
101.41.0.21
Member Port      Mode      Uptime      Expires
port-channel51  Include  1d:20:27:36 00:01:09
ethernet1/1/51:1 Include  1d:20:27:34 00:01:07
ethernet1/1/52:1 Include  1d:20:27:37 00:01:07

```

Supported Releases 10.4.1.0 or later

show ip igmp snooping interface

Displays the details of IGMP snooping interfaces.

Syntax `show ip igmp snooping interface [vlan vlan-id]`

Parameters *vlan-id*—(Optional) Enter the VLAN ID, ranging from 1 to 4093.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```

OS10# show ip igmp snooping interface
Vlan3031 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms

```

```

IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface

Vlan3032 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface

Vlan3033 is up, line protocol is up
IGMP version is 3
--more--
<<Output Truncated>>

```

Example (with VLAN)

```

OS10# show ip igmp snooping interface vlan 3031
Vlan3031 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface

```

Supported Releases

10.4.0E(R1) or later

show ip igmp snooping mrouter

Displays the details of multicast router ports.

Syntax	show ip igmp snooping mrouter [vlan <i>vlan-id</i>]
Parameters	<i>vlan-id</i> —(Optional) Enter the VLAN ID, ranging from 1 to 4093.
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	

```

OS10# show ip igmp snooping mrouter
Interface Router Ports
vlan3031 port-channel31
vlan3032 port-channel31
vlan3033 port-channel31
vlan3034 port-channel31
vlan3035 port-channel31
vlan3036 port-channel31
vlan3037 port-channel31
vlan3038 port-channel31
vlan3039 port-channel31
vlan3040 port-channel31
vlan3041 port-channel31
vlan3042 port-channel31
vlan3043 port-channel31
vlan3044 port-channel31
vlan3045 port-channel31
vlan3046 port-channel31
vlan3047 port-channel31
vlan3048 port-channel31

```

```
vlan3049    port-channel31
vlan3050    port-channel31
vlan3051    port-channel31
vlan3052    port-channel31
--more--
```

<<Output Truncated>>

Example (with VLAN)


```
OS10# show ip igmp snooping mrouter vlan 3031
Interface   Router Ports
vlan3031    port-channel31
```

Supported Releases 10.4.0E(R1) or later

Multicast Listener Discovery Protocol

IPv6 networks use Multicast Listener Discovery (MLD) Protocol to manage multicast groups.

OS10 supports MLDv1 and MLDv2 to manage the multicast group memberships on IPv6 networks.

 **NOTE:** OS10 does not support MLD snooping in VLT environments.

MLD snooping

MLD snooping enables switches to use the information in MLD packets and generate a forwarding table that associates ports with multicast groups. When switches receive multicast frames, they forward them to their intended receivers.

OS10 supports MLD snooping on VLAN interfaces.

Configure MLD snooping

- Enable MLD snooping globally with the `ipv6 mld snooping enable` command in the CONFIGURATION mode. This command enables both MLDv2 and MLDv1 snooping on all VLAN interfaces.
- (Optional) You can disable MLD snooping on specific VLAN interfaces using the `no ipv6 mld snooping` command in the VLAN INTERFACE mode.
- In a network, the snooping switch is connected to a multicast Router that sends MLD queries. On a Layer 2 network that does not have a multicast router, you can configure the snooping switch to act as querier. Use the `ipv6 mld snooping querier` command in the VLAN INTERFACE mode to send the queries.
- OS10 learns the multicast router interface dynamically based on the interface on which MLD membership query is received. To assign a multicast router interface statically, use the `ipv6 mld snooping mrouter interface interface-type` command in VLAN INTERFACE mode.
- (Optional) Configure the MLD version using the `ipv6 mld version version-number` command in the VLAN INTERFACE mode.
- (Optional) The fast leave option allows the MLD snooping switch to remove an interface from the multicast group immediately on receiving the leave message. Enable fast leave with the `ipv6 mld snooping fast-leave` command in VLAN INTERFACE mode.
- (Optional) Configure the time interval for sending MLD general queries with the `ipv6 mld snooping query-interval query-interval-time` command in VLAN INTERFACE mode.
- (Optional) Configure the maximum time for responding to a query advertised in MLD queries using the `ipv6 mld snooping query-max-resp-time query-response-time` command in VLAN INTERFACE mode.
- (Optional) Configures the time interval between group-specific MLD query messages with the `ipv6 mld snooping last-member-query-interval query-interval-time` command in VLAN INTERFACE mode.

MLD snooping configuration

```
OS10(config)# ipv6 mld snooping enable
OS10(config)# interface vlan 11
OS10(conf-if-vl-11)# ipv6 mld snooping mrouter interface ethernet 1/1/32
OS10(conf-if-vl-11)# ipv6 mld snooping querier
OS10(conf-if-vl-11)# ipv6 mld version 1
```

```

OS10(conf-if-vl-11)# ipv6 mld snooping fast-leave
OS10(conf-if-vl-11)# ipv6 mld snooping query-interval 60
OS10(conf-if-vl-11)# ipv6 mld snooping query-max-resp-time 10
OS10(conf-if-vl-11)# ipv6 mld snooping last-member-query-interval 1000

```

View MLD snooping information

```

OS10# show ipv6 mld snooping groups
Total Number of Groups: 280
MLD Connected Group Membership
Group Address          Interface          Mode
Expires
ff02::2                vlan3531          Exclude
 00:01:38
ff0e:225:1::          vlan3531          MLDv1-Compat
 00:01:52
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::1        vlan3531          MLDv1-Compat
 00:01:52
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::2        vlan3531          MLDv1-Compat
 00:01:52
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::3        vlan3531          MLDv1-Compat
 00:01:52
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::4        vlan3531          MLDv1-Compat
 00:01:52
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::5        vlan3531          MLDv1-Compat
 00:01:52
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff02::2                vlan3532          Exclude
 00:01:47
ff0e:225:2::          vlan3532          MLDv1-Compat
 00:01:56
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:2::1        vlan3532          MLDv1-Compat
 00:01:56
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:2::2        vlan3532          MLDv1-Compat
 00:01:56
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
--more--
<<Output Truncated>>

```

```

OS10# show ipv6 mld snooping interface vlan 3031
Vlan3031 is up, line protocol is up
MLD version is 2
MLD snooping is enabled on interface
MLD snooping query interval is 60 seconds
MLD snooping querier timeout is 130 seconds
MLD snooping last member query response interval is 1000 ms
MLD snooping max response time is 10 seconds
MLD snooping fast-leave is disabled on this interface
MLD snooping querier is disabled on this interface

```

```

OS10# show ipv6 mld snooping mrouter vlan 11
Interface    Router Ports
Vlan 11     ethernet 1/1/32

```

MLD snooping commands

ipv6 mld snooping

Enables MLD snooping on the specified VLAN interface.

Syntax	<code>ipv6 mld snooping</code>
Parameters	None
Default	Depends on the global configuration.
Command Mode	VLAN INTERFACE
Usage Information	When you enable MLD snooping globally, the configuration is applied to all the VLAN interfaces. You can disable the MLD snooping on specified VLAN interfaces. The <code>no</code> version of this command disables the MLD snooping on the specified VLAN interface.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# no ipv6 mld snooping</pre>
Supported Releases	10.4.1.0 or later

ipv6 mld snooping enable

Enables MLD snooping globally.

Syntax	<code>ipv6 mld snooping enable</code>
Parameters	None
Default	Disabled
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command disables the MLD snooping.
Example	<pre>OS10(config)# ipv6 mld snooping enable</pre>
Supported Releases	10.4.1.0 or later

ipv6 mld snooping fast-leave

Enables fast leave in MLD snooping for specified VLAN.

Syntax	<code>ipv6 mld snooping fast-leave</code>
Parameters	None
Default	Disabled
Command Mode	VLAN INTERFACE
Usage Information	The fast leave option allows the MLD snooping switch to remove an interface from the multicast group immediately on receiving the <code>leave</code> message. The <code>no</code> version of this command disables the fast leave functionality.
Example	<pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ipv6 mld snooping fast-leave</pre>

Supported Releases 10.4.1.0 or later

ipv6 mld snooping last-member-query-interval

Configures the time interval between group-specific MLD query messages.

Syntax `ipv6 mld snooping last-member-query-interval query-interval-time`
Parameters *query-interval-time*—Enter the query time interval in milliseconds, ranging from 100 to 65535.
Default 1000 milliseconds
Command Mode VLAN INTERFACE
Usage Information The `no` version of this command resets the last member query interval time to the default value.

Example

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping last-member-query-interval 2500
```

Supported Releases 10.4.1.0 or later

ipv6 mld snooping mrouter

Configures the specified VLAN member port as a multicast router interface.

Syntax `ipv6 mld snooping mrouter interface interface-type`
Parameters *interface-type*—Enter the interface type details. The interface should be a member of the VLAN.
Default Not configured
Command Mode VLAN INTERFACE
Usage Information The `no` version of this command removes the multicast router configuration from the VLAN member port.

Example

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping mrouter interface ethernet 1/1/1
```

Supported Releases 10.4.1.0 or later

ipv6 mld snooping querier

Enables MLD querier on the specified VLAN interface.

Syntax `ipv6 mld snooping querier`
Parameters None
Default Not configured
Command Mode VLAN INTERFACE
Usage Information The `no` version of this command disables the MLD querier on the VLAN interface.

Example

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping querier
```

Supported Releases 10.4.1.0 or later

ipv6 mld snooping query-interval

Configures the time interval for sending MLD general queries.

Syntax `ipv6 mld snooping query-interval query-interval-time`
Parameters *query-interval-time*—Enter the interval time in seconds, ranging from 2 to 18000.
Default 60 seconds
Command Mode VLAN INTERFACE
Usage Information The `no` version of this command resets the query interval to the default value.

Example

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping query-interval 120
```

Supported Releases 10.4.1.0 or later

ipv6 mld query-max-resp-time

Configures the maximum time for responding to a query advertised in MLD queries.

Syntax `ipv6 mld snooping query-max-resp-time query-response-time`
Parameters *query-response-time*—Enter the query response time in seconds, ranging from 1 to 25.
Default 10 seconds
Command Mode VLAN INTERFACE
Usage Information The `no` version of this command resets the query response time to default value.

Example

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping query-max-resp-time 15
```

Supported Releases 10.4.1.0 or later

ipv6 mld version

Configures the MLD version.

Syntax `ipv6 mld version version-number`
Parameters *version-number*—Enter the version number as 1 or 2.
Default 2
Command Mode VLAN INTERFACE
Usage Information The `no` version of this command resets the version number to the default value.

Example

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld version 1
```


Supported Releases 10.4.1.0 or later

show ipv6 mld snooping groups

Displays the details of MLD snooping group membership.

Syntax show ipv6 mld snooping groups [vlan *vlan-id*] [*ipv6-address*]

- Parameters**
- *vlan-id*—(Optional) Enter the VLAN ID, ranging from 1 to 4093.
 - *ipv6-address*—(Optional) Enter the IPv6 address of the multicast group.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show ipv6 mld snooping groups
Total Number of Groups: 280
MLD Connected Group Membership
Group Address          Expires          Interface          Mode
-----
ff02::2                00:01:38        vlan3531           Exclude
ff0e:225:1::          00:01:52        vlan3531           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::1        00:01:52        vlan3531           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::2        00:01:52        vlan3531           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::3        00:01:52        vlan3531           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::4        00:01:52        vlan3531           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::5        00:01:52        vlan3531           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff02::2                00:01:47        vlan3532           Exclude
ff0e:225:2::          00:01:56        vlan3532           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:2::1        00:01:56        vlan3532           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:2::2        00:01:56        vlan3532           MLDv1-Compat
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
--more--
```

Example (with VLAN)

```
OS10# show ipv6 mld snooping groups vlan 3531
Total Number of Groups: 7
MLD Connected Group Membership
Group Address          Interface          Mode
-----
ff02::2                vlan3531          Exclude
00:02:08
ff0e:225:1::          vlan3531          MLDv1-Compat
00:02:12
    Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::1        vlan3531          MLDv1-Compat
```

```

00:02:12
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::2          vlan3531          MLDv1-Compat
00:02:12
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::3          vlan3531          MLDv1-Compat
00:02:12
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::4          vlan3531          MLDv1-Compat
00:02:12
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::5          vlan3531          MLDv1-Compat
00:02:12
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52

```

Example (with VLAN and multicast IP address)

```

OS10# show ipv6 mld snooping groups vlan 3531 ff0e:225:1::
MLD Connected Group Membership
Group Address          Interface          Mode
Expires
ff0e:225:1::          vlan3531          MLDv1-Compat
00:01:30
  Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52

```

Supported Releases

10.4.0E(R1) or later

show ipv6 mld snooping groups detail

Displays the MLD source information along with detailed member port information.

Syntax `show ipv6 mld snooping groups [vlan vlan-id] [group ipv6-address] detail`

- Parameters**
- *vlan-id*—(Optional) Enter the VLAN ID, ranging from 1 to 4093.
 - *ipv6-address*—(Optional) Enter the IPv6 address of the multicast group.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```

OS10# show ipv6 mld snooping groups detail
Interface          vlan3041
Group              ff02::2
Source List
--
  Member Port      Mode          Uptime          Expires
  port-channel31   Exclude       2d:11:57:08     00:01:44

Interface          vlan3041
Group              ff3e:232:b::
Source List
  2001:101:29::1b
    Member Port      Mode          Uptime          Expires
    port-channel31   Include       2d:11:50:17     00:01:42
    ethernet1/1/51:1 Include       2d:11:50:36     00:01:38
    ethernet1/1/52:1 Include       2d:11:50:36     00:01:25

Interface          vlan3041
Group              ff3e:232:b::1
Source List
  2001:101:29::1b
    Member Port      Mode          Uptime          Expires
    port-channel31   Include       2d:11:50:17     00:01:29
    ethernet1/1/51:1 Include       2d:11:50:36     00:01:25

```

```

    ethernet1/1/52:1    Include                2d:11:50:36        00:01:38
--more--

```

Example (with VLAN)

```

OS10# show ipv6 mld snooping groups vlan 3041 detail
Interface          vlan3041
Group              ff02::2
Source List
--
  Member Port      Mode          Uptime           Expires
  port-channel31   Exclude       2d:11:57:08      00:01:44

Interface          vlan3041
Group              ff3e:232:b::
Source List
2001:101:29::1b
  Member Port      Mode          Uptime           Expires
  port-channel31   Include       2d:11:50:17      00:01:42
  ethernet1/1/51:1 Include       2d:11:50:36      00:01:38
  ethernet1/1/52:1 Include       2d:11:50:36      00:01:25

Interface          vlan3041
Group              ff3e:232:b::1
Source List
2001:101:29::1b
  Member Port      Mode          Uptime           Expires
  port-channel31   Include       2d:11:50:17      00:01:29
  ethernet1/1/51:1 Include       2d:11:50:36      00:01:25
  ethernet1/1/52:1 Include       2d:11:50:36      00:01:38
--more--

```

Example (with VLAN and multicast IP address)

```

OS10# show ipv6 mld snooping groups vlan 3041 ff3e:232:b:: detail
Interface          vlan3041
Group              ff3e:232:b::
Source List
2001:101:29::1b
  Member Port      Mode          Uptime           Expires
  port-channel31   Include       2d:11:50:53      00:02:01
  ethernet1/1/51:1 Include       2d:11:51:11      00:02:01
  ethernet1/1/52:1 Include       2d:11:51:12      00:01:52

```

Supported Releases 10.4.1.0 or later

show ipv6 mld snooping interface

Displays the details of MLD snooping interfaces.

- Syntax** `show ipv6 mld snooping interface [vlan vlan-id]`
- Parameters** *vlan-id*—(Optional) Enter the VLAN ID, ranging from 1 to 4093.
- Default** Not configured
- Command Mode** EXEC
- Usage Information** None

Example

```

OS10# show ipv6 mld snooping interface vlan 3031
Vlan3031 is up, line protocol is up
MLD version is 2
MLD snooping is enabled on interface
MLD snooping query interval is 60 seconds
MLD snooping querier timeout is 130 seconds
MLD snooping last member query response interval is 1000 ms
MLD snooping max response time is 10 seconds

```

```
MLD snooping fast-leave is disabled on this interface
MLD snooping querier is disabled on this interface
```

Supported Releases 10.4.1.0 or later

show ipv6 mld snooping mrouter

Displays the details of multicast router ports.

Syntax `show ipv6 mld snooping mrouter [vlan vlan-id]`

Parameters *vlan-id*—(Optional) Enter the VLAN ID, ranging from 1 to 4093.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show ipv6 mld snooping mrouter vlan 11
Interface      Router Ports
Vlan 11        ethernet 1/1/32
```

Supported Releases 10.4.1.0 or later

Open shortest path first

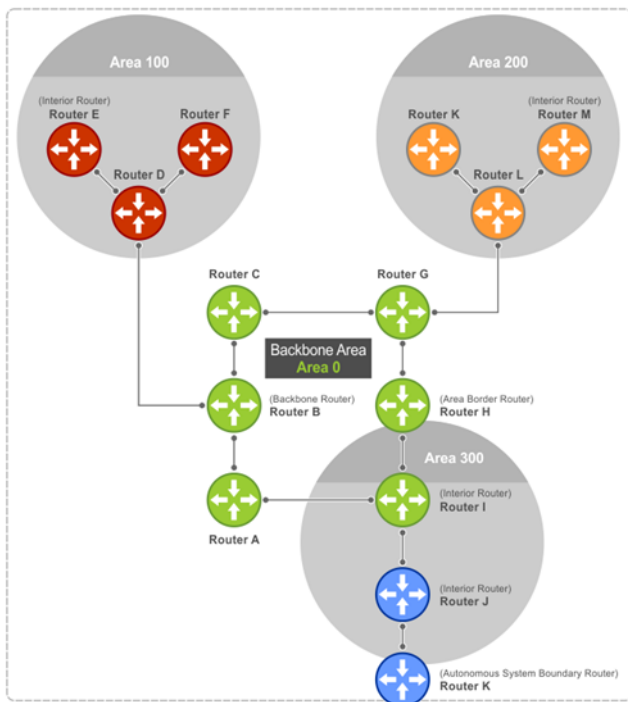
OSPF routing is a link-state routing protocol that allows sending of link-state advertisements (LSAs) to all other routers within the same autonomous system (AS) area. Information about attached interfaces, metrics used, and other attributes are included in OSPF LSAs. OSPF routers accumulate link-state information, and use the shortest path first (SPF) algorithm to calculate the shortest path to each node.

Autonomous system areas

OSPF operates in a type of hierarchy. The largest entity within the hierarchy is the autonomous system (AS). The AS is a collection of networks under a common administration that share a common routing strategy. OSPF is an intra-AS, Interior Gateway Routing Protocol (IGRP) that receives routes from and sends routes to other AS.

You can divide an AS into several areas, which are groups of contiguous networks and attached hosts administratively grouped. Routers with multiple interfaces can participate in multiple areas. These routers, called area border routers (ABRs), maintain separate databases for each area. Areas are a logical grouping of OSPF routers that an integer or dotted-decimal number identifies.

Areas allow you to further organize routers within the AS with one or more areas within the AS. Areas are valuable in that they allow subnetworks to *hide* within the AS—minimizing the size of the routing tables on all routers. An area within the AS may not see the details of another area's topology. An area number or the router's IP address identifies AS areas.



Areas, networks, and neighbors

The backbone of the network is Area 0, also called Area 0.0.0.0, the core of any AS. All other areas must connect to Area 0. An OSPF backbone is responsible for distributing routing information between areas. It consists of all area border routers, networks not wholly contained in any area and their attached routers.

The backbone is the only area with a default area number. You configure all other areas Area ID. If you configure two nonbackbone areas, you must enable the B bit in OSPF. Routers, A, B, C, G, H, and I are the backbone, see [Autonomous system areas](#).

- A stub area (SA) does not receive external route information, except for the default route. These areas do receive information from interarea (IA) routes.
- A not-so-stubby area (NSSA) can import AS external route information and send it to the backbone as type-7 LSA.
- Totally stubby areas are also known as no summary areas.

Configure all routers within an assigned stub area as stubby and do not generate LSAs that do not apply. For example, a Type 5 LSA is intended for external areas and the stubby area routers may not generate external LSAs. A virtual link cannot traverse stubby areas.

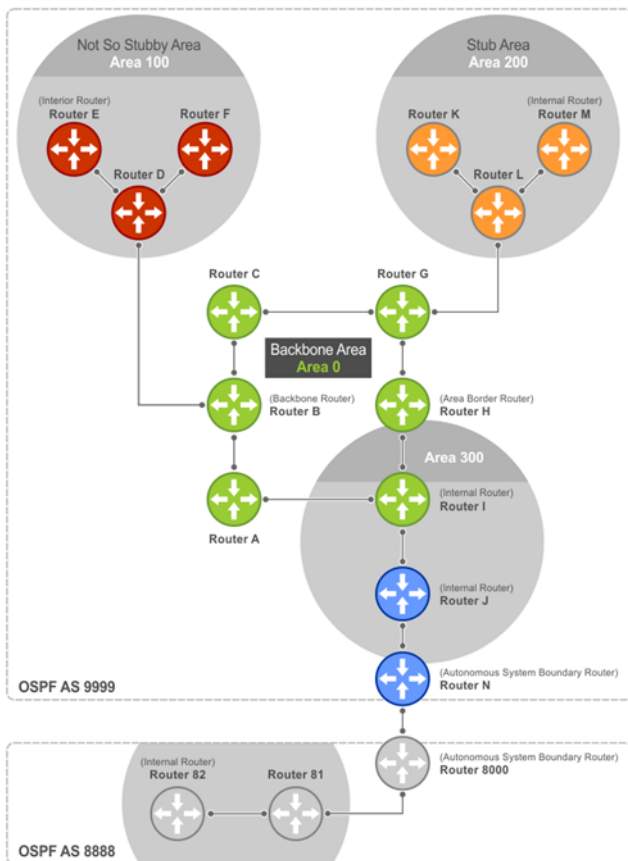
Networks and neighbors

As a link-state protocol, OSPF sends routing information to other OSPF routers concerning the state of the links between them. The up or down state of those links is important. Routers that share a link become neighbors on that segment. OSPF uses the `hello` protocol as a neighbor discovery and `keepalive` mechanism. After two routers are neighbors, they may proceed to exchange and synchronize their databases, which creates an adjacency.

Router types

Router types are attributes of the OSPF process—multiple OSPF processes may run on the same router. A router connected to more than one area, receiving routing from a BGP process connected to another AS, acts as both an area border router and an autonomous system border router.

Each router has a unique ID, written in decimal format—A.B.C.D. You do not have to associate the router ID with a valid IP address. To make troubleshooting easier, ensure the router ID is identical to the router's IP address.



- Backbone router** A backbone router (BR) is part of the OSPF Backbone, Area 0, and includes all ABRs. The BR includes routers connected only to the backbone and another ABR, but are only part of Area 0—shown as Router I in the example.
- Area border router** Within an AS, an area border router (ABR) connects one or more areas to the backbone. The ABR keeps a copy of the link-state database for every area it connects to. It may keep multiple copies of the link state database. An ABR summarizes learned information from one of its attached areas before it is sent to other connected areas. An ABR can connect to many areas in an AS and is considered a member of each area it connects to—shown as Router H in the example.
- Autonomous system border router** The autonomous system border router (ASBR) connects to more than one AS and exchanges information with the routers in other ASs. The ASBR connects to a non-IGP such as BGP or uses static routes—shown as Router N in the example.
- Internal router** The internal router (IR) has adjacencies with ONLY routers in the same area—shown as Routers E, F, I, K, and M in the example.

Designated and backup designated routers

OSPF elects a designated router (DR) and a backup designated router (BDR). The DR is responsible for generating LSAs for the entire multiaccess network. Designated routers allow a reduction in network traffic and in the size of the topological database.

- Designated router** Maintains a complete topology table of the network and sends updates to the other routers via multicast. All routers in an area form a slave/master relationship with the DR. Every time a router sends an update, the router sends it to the DR and BDR. The DR sends the update out to all other routers in the area.
- Backup designated router** Router that takes over if the DR fails.

Each router exchanges information with the DR and BDR. The DR and BDR relay information to other routers. On broadcast network segments, the number of OSPF packets reduces by the DR sending OSPF updates to a multicast IP address that all OSPF routers on the network segment are listening on.

The DRs and BDRs are configurable. If you do not define DR or BDR, OSPF assigns them per the protocol. To determine which routers are the DR and BDR, the OSPF looks at the priority of the routers on the segment —default router priority is 1. The router with the highest priority is elected the DR. If there is a tie, the router with the higher router ID takes precedence. After the DR is elected, the BDR is elected the same way. A router with a router priority set to zero cannot become the DR or BDR.

Link-state advertisements

A link-state advertisement (LSA) communicates the router’s routing topology to all other routers in the network.

Type 1—Router LSA	Router lists links to other routers or networks in the same area. Type 1 LSAs flood across their own area only. The link-state ID of the Type 1 LSA is the originating router ID.
Type 2—Network LSA	DR in an area lists which routers are joined within the area. Type 2 LSAs flood across their own area only. The link-state ID of the Type 2 LSA is the IP interface address of the DR.
Type 3—Summary LSA (OSPFv2), Inter-Area Prefix LSA (OSPFv3)	ABR takes information it has learned on one of its attached areas and summarizes it before sending it out on other areas it connects to. The link-state ID of the Type 3 LSA is the destination network's IP address.
Type 4—AS Border Router Summary LSA (OSPFv2), Inter-Area-Router LSA (OSPFv3)	In some cases, Type 5 External LSAs flood to areas where the detailed next-hop information may not be available, because it may be using a different routing protocol. The ABR floods the information for the router—the ASBR where the Type 5 originated. The link-state ID for Type 4 LSAs is the router ID of the described ASBR.
Type 5—AS-External LSA	LSAs contain information imported into OSPF from other routing processes. Type 5 LSAs flood to all areas except stub areas. The link-state ID of the Type 5 LSA is the external network number.
Type 7—NSSA-External LSA (OSPFv2), LSA (OSPFv3)	Routers in an NSSA do not receive external LSAs from ABRs but send external routing information for redistribution. They use Type 7 LSAs to tell the ABRs about these external routes, which the ABR then translates to Type 5 external LSAs and floods as normal to the rest of the OSPF network.
Type 8—Link LSA (OSPFv3)	Type 8 LSA carries the IPv6 address information of the local links.
Type 9—Link-Local Opaque LSA (OSPFv2), Intra-Area Prefix LSA (OSPFv3)	Link-local <i>opaque</i> LSA as defined by RFC2370 for OSPFv2. Intra-Area-Prefix LSA carries the IPv6 prefixes of the router and network links for OSPFv3.
Type 11—Grace LSA (OSPFv3)	Link-local <i>opaque</i> LSA for OSPFv3 only is sent during a graceful restart by an OSPFv3 router.

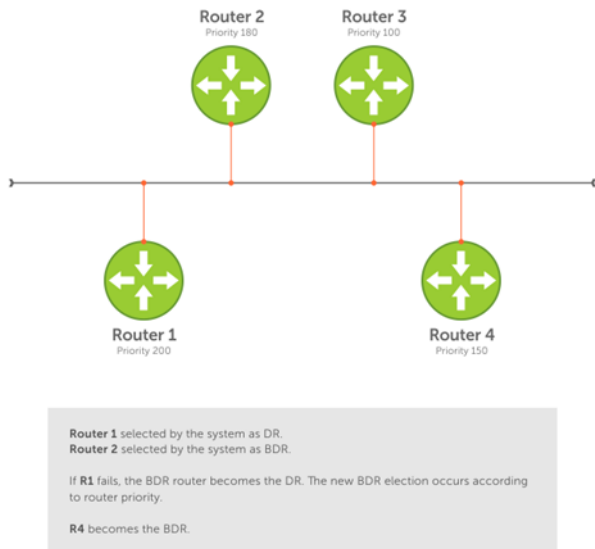
The LSA header is common to LSA types. Its size is 20 bytes. One of the fields of the LSA header is the link-state ID. Each router link is defined as one of four types—type 1, 2, 3, or 4. The LSA includes a link ID field that identifies the object this link connects to, by the network number and mask. Depending on the type, the link ID has different meanings.

1	Point-to-point connection to another router or neighboring router
2	Connection to a transit network IP address of the DR
3	Connection to a stub network IP network or subnet number
4	Virtual link neighboring router ID

Router priority

Router priority determines the designated router for the network. The default router priority is 1. When two routers are attached to a network, both attempt to become the designated router. The router 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 cannot become the designated router or backup designated router.

If not assigned, the system selects the router with the highest priority as the DR. The second highest priority is the BDR. Priority rates from 0 to 255, with 255 as the highest number with the highest priority.



OSPF route limit

OS10 supports up to 16,000 OSPF routes. Within this range, the only restriction is on intra-area routes that scale only up to 1000 routes. Other OSPF routes can scale up to 16 K.

Shortest path first throttling

Use shortest path first (SPF) throttling to delay SPF calculations during periods of network instability. In an OSPF network, a topology change event triggers an SPF calculation that is performed after a start time. When the start timer finishes, a hold time can delay the next SPF calculation for an additional time.

When the hold timer is running:

- Each time a topology change occurs, the SPF calculation is delayed for double the configured hold time up to maximum wait time.
- If no topology change occurs, an SPF calculation is performed and the hold timer is reset to its configured value.

Set the start, hold, and wait timers according to the stability of the OSPF network topology. Enter the values in milliseconds (ms). If you do not specify a start-time, hold-time or max-wait value, the default values are used.

OSPFv2 and OSPFv3 instances support SPF throttling. By default, SPF timers are disabled in an OSPF instance. Enter the `no` version of this command to remove the configured SPF timers and disable SPF throttling.

1. Configure an OSPF instance from CONFIGURATION mode (1 to 65535).

```
router {ospf | ospfv3} instance-number
```

2. Set OSPF throttling timers in OSPF INSTANCE mode.

```
timers spf [start-time [hold-time [max-wait]]]
```

- `start-time` — Configure the initial delay before performing an SPF calculation after a topology change (1 to 600000 milliseconds; default 1000).
- `hold-time` — Configure the additional delay before performing an SPF calculation when a new topology change occurs (1 to 600000 milliseconds; default 10000).
- `max-wait` — Configure the maximum amount of hold time that can delay an SPF calculation (1 to 600000 milliseconds; default 10000).

Enable SPF throttling (OSPFv2)

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# timers spf 1200 2300 3400
```


Enable SPF throttling (OSPFv3)

```
OS10(config)# router ospfv3 10
OS10(config-router-ospfv3-10)# timers spf 2000 3000 4000
```

View OSPFv2 SPF throttling

```
OS10(config-router-ospf-100)# do show ip ospf
Routing Process ospf 100 with ID 12.1.1.1
Supports only single TOS (TOS0) routes
It is Flooding according to RFC 2328
SPF schedule delay 1200 msecs, Hold time between two SPF's 2300 msecs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 1 times
```

View OSPFv3 SPF throttling

```
OS10(config-router-ospfv3-100)# timers spf 1345 2324 9234
OS10(config-router-ospfv3-100)# do show ipv6 ospf
Routing Process ospfv3 100 with ID 129.240.244.107
SPF schedule delay 1345 msecs, Hold time between two SPF's 2324 msecs
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 1, normal 1 stub 0 nssa
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 2 times
```

OSPFv2

OSPFv2 supports IPv4 address families. OSPFv2 routers initially exchange `hello` messages to set up adjacencies with neighbor routers. The `hello` process establishes adjacencies between routers of the AS. It is not required that every router within the AS areas establish adjacencies. If two routers on the same subnet agree to become neighbors through this process, they begin to exchange network topology information in the form of LSAs.

In OSPFv2, neighbors on broadcast and non-broadcast multiple access (NBMA) network links are identified by their interface addresses, while neighbors on other types of links are identified by router-identifiers (RID).

Enable OSPFv2

OSPFv2 is disabled by default. Configure at least one interface as either physical or LOOPBACK and assign an IP address to the interface. You can assign any area besides area 0 a number ID. The OSPFv2 process starts automatically when you configure it globally and you can enable it for one or more interfaces.

1. Enable OSPF globally and configure an OSPF instance in CONFIGURATION mode.

```
router ospf instance-number
```

2. Enter the interface information to configure the interface for OSPF in INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
```

3. Enable the interface in INTERFACE mode.

```
no shutdown
```

4. Disable the default switchport configuration and remove it from an interface or a LAG port in INTERFACE mode.

```
no switchport
```

5. Assign an IP address to the interface in INTERFACE mode.

```
ip address ip-address/mask
```

6. Enable OSPFv2 on an interface in INTERFACE mode.

```
ip ospf process-id area area-id
```

- *process-id*—Enter the OSPFv2 process ID for a specific OSPF process from 1 to 65535.
- *area-id*—Enter the OSPFv2 area ID as an IP address (A.B.C.D) or number from 1 to 65535.

Enable OSPFv2 configuration

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# exit
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip address 11.1.1.1/24
OS10(config-if-eth1/1/1)# ip ospf 100 area 0.0.0.0
```

View OSPFv2 configuration

```
OS10# show running-configuration ospf
!
interface ethernet1/1/1
 ip ospf 100 area 0.0.0.0
!
router ospf 100
...
```

Assign router identifier

For managing and troubleshooting purposes, you can assign a router ID for the OSPFv2 process. Use the router's IP address as the router ID.

- Assign the router ID for the OSPFv2 process in ROUTER-OSPF mode

```
router-id ip-address
```

Assign router ID

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# router-id 10.10.1.5
```

View OSPFv2 status

```
OS10# show ip ospf 10
Routing Process ospf 10 with ID 10.10.1.5
Supports only single TOS (TOS0) routes
It is an Autonomous System Boundary Router
It is Flooding according to RFC 2328
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
Area (0.0.0.0)
  Number of interface in this area is 3
  SPF algorithm executed 38 times
  Area ranges are
```

Stub areas

Type 5 LSAs are not flooded into stub areas. The ABR advertises a default route into the stub area to which it is attached. Stub area routers use the default route to reach external destinations.

1. Enable OSPF routing and enter ROUTER-OSPF mode, from 1 to 65535.

```
router ospf instance number
```

2. Configure an area as a stub area in ROUTER-OSPF mode.

```
area area-id stub [no-summary]
```

- *area-id*—Enter the OSPF area ID as an IP address (A.B.C.D) or number, from 1 to 65535.
- *no-summary*—(Optional) Enter to prevent an ABR from sending summary LSA to the stub area.

Configure stub area

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# area 10.10.5.1 stub
```

View stub area configuration

```
OS10# show ip ospf
Routing Process ospf 10 with ID 130.6.196.14
Supports only single TOS (TOS0) routes
It is Flooding according to RFC 2328
SPF schedule delay 1000 msec, Hold time between two SPF's 10000 msec
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 0 stub 1 nssa 0
  Area (10.10.5.1)
    Number of interface in this area is 0
    SPF algorithm executed 1 times
    Area ranges are
```

```
OS10# show running-configuration ospf
!
router ospf 10
 area 10.10.5.1 stub
```

Passive interfaces

A passive interface does not send or receive routing information. Configuring an interface as a passive interface suppresses both receiving and sending routing updates.

Although the passive interface does not send or receive routing updates, the network on that interface is included in OSPF updates sent through other interfaces.

1. Enter an interface type in INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
```

2. Configure the interface as a passive interface in INTERFACE mode.

```
ip ospf passive
```

Configure passive interfaces

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ip ospf passive
```

View passive interfaces

```
OS10# show running-configuration
!!!
!!
interface ethernet1/1/6
 ip address 10.10.10.1/24
 no switchport
 no shutdown
```


```
ip ospf 100 area 0.0.0.0
ip ospf passive
!!
!
```

You can disable a passive interface using the `no ip ospf passive` command.

Fast convergence

Fast convergence sets the minimum origination and arrival LSA parameters to zero (0), allowing rapid route calculation. A higher convergence level can result in occasional loss of OSPF adjacency.

Convergence level 1 meets most convergence requirements. The higher the number, the faster the convergence, and the more frequent the route calculations and updates. This impacts CPU utilization and may impact adjacency stability in larger topologies.

 **NOTE:** Select the higher convergence levels only after checking with Dell Technical Support.

When you disable fast-convergence, origination and arrival LSA parameters are set to 0 msec and 1000 msec, respectively. Setting the convergence parameter from 1 to 4 indicates the actual convergence level. Each convergence setting adjusts the LSA parameters to zero, but the `convergence-level` parameter changes the convergence speed. The higher the number, the faster the convergence.

- Enable OSPFv2 fast-convergence and enter the convergence level in ROUTER-OSPF mode from 1 to 4.

```
fast-converge convergence-level
```

Configure fast convergence

```
OS10(config)# router ospf 65535
OS10(conf-router-ospf-65535)# fast-converge 1
```

View fast convergence

```
OS10(conf-router-ospf-65535)# do show ip ospf

Routing Process ospf 65535 with ID 99.99.99.99
Supports only single TOS (TOS0) routes
It is an Autonomous System Border Router
It is an Area Border Router
It is Flooding according to RFC 2328
Convergence Level 1
Min LSA origination 0 msec, Min LSA arrival 0 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 3, normal 1 stub 1 nssa 1
  Area BACKBONE (0)
    Number of interface in this area is 1
    SPF algorithm executed 28 times
    Area ranges are

  Area (2)
    Number of interface in this area is 1
    SPF algorithm executed 28 times
    Area ranges are

  Area (3)
    Number of interface in this area is 1
    SPF algorithm executed 28 times
    Area ranges are
```

Disable fast convergence

```
OS10(conf-router-ospf-65535)# no fast-converge
```

Interface parameters

To avoid routing errors, interface parameter values must be consistent across all interfaces. For example, set the same time interval for the hello packets on all routers in the OSPF network to prevent misconfiguration of OSPF neighbors.

1. To change the OSPFv2 parameters in CONFIGURATION mode, enter the interface.

```
interface interface-name
```

2. Change the cost associated with OSPF traffic on the interface in INTERFACE mode, from 1 to 65535. The default depends on the interface speed.

```
ip ospf cost
```

3. Change the time interval, from 1 to 65535, that the router waits before declaring a neighbor dead in INTERFACE mode. The default time interval is 40. The dead interval must be four times the hello interval and must be the same on all routers in the OSPF network.

```
ip ospf dead-interval seconds
```

4. Change the time interval between hello-packet transmission in INTERFACE mode, from 1 to 65535. The default time interval is 10. The hello interval must be the same on all routers in the OSPF network.

```
ip ospf hello-interval seconds
```

5. Change the priority of the interface, which determines the DR for the OSPF broadcast network in INTERFACE mode, from 0 to 255. The default priority of the interface is 1.

```
ip ospf priority number
```

6. Change the retransmission interval time, in seconds, between LSAs in INTERFACE mode, from 1 to 3600. The default retransmission interval time is 5. The retransmit interval must be the same on all routers in the OSPF network.

```
ip ospf retransmit-interval seconds
```

7. Change the wait period between link state update packets sent out the interface in INTERFACE mode, from 1 to 3600. The default wait period is 1. The transmit delay must be the same on all routers in the OSPF network.

```
ip ospf transmit-delay seconds
```

Change parameters and view interface status

```
OS10(conf-if-eth1/1/1)# ip ospf hello-interval 5
OS10(conf-if-eth1/1/1)# ip ospf dead-interval 20
OS10(conf-if-eth1/1/1)# ip ospf retransmit-interval 30
OS10(conf-if-eth1/1/1)# ip ospf transmit-delay 200
```

View OSPF interface configuration

```
OS10(conf-if-eth1/1/1)# do show ip ospf interface

ethernet1/1/1 is up, line protocol is up
 Internet Address 11.1.1.1/24, Area 0.0.0.0
 Process ID 65535, Router ID 99.99.99.99, Network Type broadcast, Cost: 1
 Transmit Delay is 200 sec, State BDR, Priority 1
 Designated Router (ID) 150.1.1.1, Interface address 11.1.1.2
 Backup Designated router (ID) 99.99.99.99, Interface address 11.1.1.1
 Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 30
 Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 150.1.1.1(Designated Router)
```

Redistribute routes

Add routes from other routing instances or protocols to the OSPFv2 process and include BGP, static, or connected routes in the OSPFv2 process. Do not route IBGP routes to OSPFv2 unless there are route-maps associated with the OSPFv2 redistribution.

- Enter which routes redistribute into the OSPFv2 process in ROUTER-OSPF mode.

```
redistribute {bgp as-number | connected | static} [route-map map-name]
```

- `bgp | connected | static`—Enter a keyword to redistribute those routes.
- `route-map map-name`—Enter the name of a configured route map.

Configure redistribute routes

```
OS10(conf-router-ospf-10)# redistribute bgp 4 route-map aloha
OS10(conf-router-ospf-10)# redistribute connected route-map aloha
OS10(conf-router-ospf-10)# redistribute static route-map aloha
```

View OSPF configuration

```
OS10(conf-router-ospf-10)# do show running-configuration ospf
!
router ospf 10
 redistribute bgp 4 route-map aloha
 redistribute connected route-map aloha
 redistribute static route-map aloha
!
```

Default route

You can generate an external default route and distribute the default information to the OSPFv2 routing domain.

- To generate the default route, use the `default-information originate [always]` command in ROUTER-OSPF mode.

Configure default route

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# default-information originate always
```

View default route configuration

```
OS10(config-router-ospf-10)# show configuration
!
router ospf 10
 default-information originate always
```

Summary address

You can configure a summary address for an ASBR to advertise one external route as an aggregate, for all redistributed routes that are covered by specified address range.

- Configure the summary address in ROUTER-OSPF mode.
`summary-address ip-address/mask [not-advertise | tag tag-value]`

Configure summary address

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# summary-address 10.0.0.0/8 not-advertise
```

View summary address

```
OS10(config-router-ospf-100)# show configuration
!
router ospf 100
 summary-address 10.0.0.0/8 not-advertise
```

Graceful restart

When a networking device restarts, the adjacent neighbors and peers detect the condition. During a graceful restart, the restarting device and the neighbors continue to forward the packets without interrupting the network performance. The neighbors that help in the restart process are called as helper routers.

When graceful restart is enabled, the restarting device retains the routes learned by OSPF in the forwarding table. To re-establish OSPF adjacencies with neighbors, the restarting OSPF process sends a grace LSA to all neighbors. In response, the helper router enters helper mode and sends an acknowledgement back to the restarting device.

OS10 supports graceful restart helper mode. Use the `graceful-restart role helper-only` command to enable the helper mode in the ROUTER OSPF mode.

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# graceful-restart role helper-only
```

Use the `no` version of the command to disable the helper mode.

OSPFv2 authentication

You can enable OSPF authentication either with clear text or with MD5.

- Set a clear text authentication scheme on the interface in INTERFACE mode.
`ip ospf authentication-key key`
- Set MD5 authentication in INTERFACE mode.
`ip ospf message-digest-key keyid md5 key`

Configure text authentication

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip ospf authentication-key sample
```

View text authentication

```
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 ip address 10.10.10.2/24
 no switchport
 no shutdown
 ip ospf 100 area 0.0.0.0
 ip ospf authentication-key sample
```

Configure MD5 authentication

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip ospf message-digest-key 2 md5 sample12345
```

View MD5 authentication

```
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 ip address 10.10.10.2/24
 no switchport
 no shutdown
 ip ospf 100 area 0.0.0.0
 ip ospf message-digest-key 2 md5 sample12345
```

Troubleshoot OSPFv2

You can troubleshoot the OSPFv2 operations, and check questions for any typical issues that interrupt a process.

- Is OSPF enabled globally?

- Is OSPF enabled on the interface?
- Are adjacencies established correctly?
- Are the interfaces configured for L3 correctly?
- Is the router in the correct area type?
- Are the OSPF routes included in the OSPF database?
- Are the OSPF routes included in the routing table in addition to the OSPF database?
- Are you able to ping the IPv4 address of adjacent router interface?

Troubleshooting OSPF with show commands

- View a summary of all OSPF process IDs enabled in EXEC mode.

```
show running-configuration ospf
```

- View summary information of IP routes in EXEC mode.

```
show ip route summary
```

- View summary information for the OSPF database in EXEC mode.

```
show ip ospf database
```

- View the configuration of OSPF neighbors connected to the local router in EXEC mode.

```
show ip ospf neighbor
```

- View routes that OSPF calculates in EXEC mode.

```
show ip ospf routes
```

View OSPF configuration

```
OS10# show running-configuration ospf
!
interface ethernet1/1/1
ip ospf 100 area 0.0.0.0
!
router ospf 100
log-adjacency-changes
```

OSPFv2 commands

area default-cost

Sets the metric for the summary default route generated by the ABR and sends it to the stub area. Use the `area default-cost` command on the border routers at the edge of a stub area.

Syntax	<code>area area-id default-cost cost</code>
Parameters	<ul style="list-style-type: none"> • <code>area-id</code> — Enter the OSPF area in dotted decimal format (A.B.C.D.) or enter a number (0 to 65535). • <code>cost</code> — Enter a cost for the stub area's advertised external route metric (0 to 65535).
Default	Cost is 1
Command Mode	ROUTER-OSPF
Usage Information	The cost is also referred as <i>reference-bandwidth</i> or <i>bandwidth</i> . The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(conf-router-ospf-10)# area 10.10.1.5 default-cost 10</pre>
Supported Releases	10.2.0E or later

area nssa

Defines an area as a NSSA.

Syntax	<code>area area-id nssa [default-information-originate no-redistribution no-summary]</code>
Parameters	<ul style="list-style-type: none">• <code>area-id</code> — Enter the OSPF area ID as an IP address (A.B.C.D) or number (1 to 65535).• <code>no-redistribution</code> — (Optional) Prevents the <code>redistribute</code> command from distributing routes into the NSSA. Use <code>no-redistribution</code> command only in an NSSA ABR.• <code>no-summary</code> — (Optional) Ensures that no summary LSAs are sent into the NSSA.
Default	Not configured
Command Mode	ROUTER-OSPF
Usage Information	The <code>no</code> version of this command deletes an NSSA.
Example	<pre>OS10(conf-router-ospf-10)# area 10.10.1.5 nssa</pre>
Supported Releases	10.2.0E or later

area range

Summarizes routes matching an address/mask at an area in ABRs.

Syntax	<code>area area-id range ip-address [no-advertise]</code>
Parameters	<ul style="list-style-type: none">• <code>area-id</code> — Set the OSPF area ID as an IP address (A.B.C.D) or number (1 to 65535).• <code>ip-address</code> — (Optional) Enter an IP address/mask in dotted decimal format.• <code>no-advertise</code> — (Optional) Set the status to <i>Do Not Advertise</i>. The Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.
Default	Not configured
Command Mode	ROUTER-OSPF
Usage Information	The <code>no</code> version of this command disables the route summarizations.
Example	<pre>OS10(conf-router-ospf-10)# area 0 range 10.1.1.4/8 no-advertise</pre>
Supported Releases	10.2.0E or later

area stub

Defines an area as the OSPF stub area.

Syntax	<code>area area-id stub [no-summary]</code>
Parameters	<ul style="list-style-type: none">• <code>area-id</code>—Set the OSPF area ID as an IP address (A.B.C.D) or number (1 to 65535).• <code>no-summary</code>—(Optional) Prevents an area border router from sending summary link advertisements into the stub area.
Default	Not configured
Command Mode	ROUTER-OSPF
Usage Information	The <code>no</code> version of this command deletes a stub area.

Example

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# area 10.10.1.5 stub
```

Supported Releases 10.2.0E or later

auto-cost reference-bandwidth

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

Syntax `auto-cost reference-bandwidth value`

Parameters *value* — Enter the reference bandwidth value to calculate the OSPF interface cost in megabits per second (1 to 4294967).

Default 100000

Command Mode ROUTER-OSPF

Usage Information The value set by the `ip ospf cost` command in INTERFACE mode overrides the cost resulting from the `auto-cost` command. The `no` version of this command resets the value to the default.

Example

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# auto-cost reference-bandwidth 150
```

Supported Releases 10.2.0E or later

clear ip ospf process

Clears all OSPF routing tables.

Syntax `clear ip ospf {instance-number} process`

Parameters *instance-number* — Enter an OSPF instance number (1 to 65535).

Default Not configured

Command Mode EXEC

Usage Information This command clears all entries in the OSPF routing table.

Example

```
OS10# clear ip ospf 3 process
```

Supported Releases 10.2.0E or later

clear ip ospf statistics

Clears OSPF traffic statistics.

Syntax `clear ip ospf [instance-number] statistics`

Parameters *instance-number* — (Optional) Enter an OSPF instance number (1 to 65535).

Default Not configured

Command Mode EXEC

Usage Information This command clears the OSPF traffic statistics in a specified instance or in all the configured OSPF instances, and resets them to zero.

Example

```
OS10# clear ip ospf 10 statistics
```

Supported Releases

10.4.0E(R1) or later

default-information originate

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

Syntax `default-information originate [always]`

Parameters `always` — (Optional) Always advertise the default route.

Defaults Disabled

Command Mode ROUTER-OSPF

Usage Information The `no` version of this command disables the distribution of default route.

Example

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# default-information originate always
```

Supported Releases

10.3.0E or later

default-metric

Assigns a metric value to redistributed routes for the OSPF process.

Syntax `default-metric number`

Parameters `number` — Enter a default-metric value (1 to 16777214).

Default Not configured

Command Mode ROUTER-OSPF

Usage Information The `no` version of this command disables the default-metric configuration.

Example

```
OS10(conf-router-ospf-10)# default-metric 2000
```

Supported Releases

10.2.0E or later

fast-converge

Sets the minimum LSA origination and arrival times to zero (0) allowing more rapid route computation so that convergence takes less time.

Syntax `fast-converge convergence-level`

Parameters `convergence-level` — Enter a desired convergence level value (1 to 4).

Default Not configured

Command Mode ROUTER-OSPF

Usage Information Convergence level 1 (optimal) meets most convergence requirements. Only select higher convergence levels following consultation with Dell Technical Support. The `no` version of this command disables the fast-convergence configuration.

Example

```
OS10(conf-router-ospf-10)# fast-converge 3
```

Supported Releases

10.2.0E or later

graceful-restart

Enables the helper mode during a graceful or hitless restart.

Syntax `graceful-restart role helper-only`

Parameters None

Defaults Disabled

Command Mode ROUTER-OSPF

Usage Information The `no` version of this command disables the helper mode.

Example

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# graceful-restart role helper-only
```

Supported Releases

10.3.0E or later

ip ospf area

Attaches an interface to an OSPF area.

Syntax `ip ospf process-id area area-id`

Parameters

- `process-id` — Set an OSPF process ID for a specific OSPF process (1 to 65535)
- `area area-id` — Enter the OSPF area ID in dotted decimal format (A.B.C.D.) or enter an area ID number (1 to 65535).

Default Not configured

Command Mode INTERFACE

Usage Information The `no` version of this command removes an interface from an OSPF area.

Example

```
OS10(conf-if-vl-10)# ip ospf 10 area 5
```

Supported Releases

10.2.0E or later

ip ospf authentication-key

Configures a text authentication key to enable OSPF traffic on an interface.

Syntax `ip ospf authentication-key key`

Parameters `key` — Enter an eight-character string for the authentication key.

Defaults Not configured

Command Mode INTERFACE

Usage Information To exchange OSPF information, all neighboring routers in the same network must use the same authentication key. The `no` version of this command deletes the authentication key.

Example

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip ospf authentication-key sample
```

Supported Releases 10.3.0E or later

ip ospf cost

Changes the cost associated with the OSPF traffic on an interface.

Syntax `ip ospf cost cost`

Parameters *cost* — Enter a value as the OSPF cost for the interface (1 to 65535).

Default Based on bandwidth reference

Command Mode INTERFACE

Usage Information Interface cost is based on the `auto-cost` command if not configured. 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 the interface. The `no` version of this command removes the IP OSPF cost configuration.

Example

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-1)# ip ospf cost 10
```

Supported Releases 10.2.0E or later

ip ospf dead-interval

Sets the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

Syntax `ip ospf dead-interval seconds`

Parameters *seconds* — Enter the dead interval value in seconds (1 to 65535).

Default 40 seconds

Command Mode INTERFACE

Usage Information The dead interval is four times the default hello-interval by default. The `no` version of this command resets the value to the default.

Example

```
OS10(conf-if-vl-10)# ip ospf dead-interval 10
```

Supported Releases 10.2.0E or later

ip ospf hello-interval

Sets the time interval between the hello packets sent on the interface.

Syntax `ip ospf hello-interval seconds`

Parameters *seconds* — Enter the hello-interval value in seconds (1 to 65535).

Default 10 seconds

Command Mode INTERFACE

Usage Information All routers in a network must have the same hello time interval between the hello packets. The `no` version of the this command resets the value to the default.

Example

```
OS10(conf-if-vl-10)# ip ospf hello-interval 30
```

Supported Releases

10.2.0E or later

ip ospf message-digest-key

Enables OSPF MD5 authentication and sends an OSPF message digest key on the interface.

Syntax `ip ospf message-digest-key keyid md5 key`

Parameters

- *keyid* — Enter an MD5 key ID for the interface (1 to 255).
- *key* — Enter a character string as the password (up to 16 characters).

Defaults Not configured

Command Mode INTERFACE

Usage Information All neighboring routers in the same network must use the same key value to exchange OSPF information. The `no` version of this command deletes the authentication key.

Example

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip ospf message-digest-key 2 md5 sample12345
```

Supported Releases

10.3.0E or later

ip ospf mtu-ignore

Enables OSPF MTU mismatch detection on receipt of DBD packets.

Syntax `ip ospf mtu-ignore`

Parameters None

Default Not configured

Command Mode INTERFACE

Usage Information When neighbors exchange DBD packets, the OSPF process checks if the neighbors are using the same MTU on a common interface. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency does not establish. The `no` version of this command disables the IP OSPF mtu-ignore configuration.

Example

```
OS10(conf-if-vl-10)# ip ospf mtu-ignore
```

Supported Releases

10.2.0E or later

ip ospf network

Sets the network type for the interface.

Syntax `ip ospf network {point-to-point | broadcast}`

Parameters

- `point-to-point` — Sets the interface as part of a point-to-point network.
- `broadcast` — Sets the interface as part of a broadcast network.

Default Broadcast

Command Mode INTERFACE

Usage Information The `no` version of this command resets the value to the default.

Example

```
OS10(conf-if-eth1/1/1)# ip ospf network broadcast
```

Supported Releases

10.2.0E or later

ip ospf passive

Configures an interface as a passive interface and suppresses routing updates (both receiving and sending) to the passive interface.

Syntax `ip ospf passive`

Parameters None

Default Not configured

Command Mode INTERFACE

Usage Information You must configure the interface before setting the interface to Passive mode. The `no` version of the this command disables the passive interface configuration.

Example

```
OS10(conf-if-eth1/1/6)# ip ospf passive
```

Supported Releases

10.2.0E or later

ip ospf priority

Sets the priority of the interface to determine the designated router for the OSPF network.

Syntax `ip ospf priority number`

Parameters *number* — Enter a router priority number (0 to 255).

Default 1

Command Mode INTERFACE

Usage Information When two routers attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. The `no` version of this command resets the value to the default.

Example

```
OS10(conf-if-eth1/1/6)# ip ospf priority 4
```

Supported Releases

10.2.0E or later

ip ospf retransmit-interval

Sets the retransmission time between lost LSAs for adjacencies belonging to the interface.

Syntax `ip ospf retransmit-interval seconds`

Parameters *seconds* — Enter a value in seconds as the interval between retransmission (1 to 3600).

Default 5 seconds

Command Mode INTERFACE

Usage Information Set the time interval to a number large enough to avoid unnecessary retransmission. The `no` version of this command resets the value to the default.

Example

```
OS10(conf-if-eth1/1/6)# ip ospf retransmit-interval 20
```

Supported Releases 10.2.0E or later

ip ospf transmit-delay

Sets the estimated time required to send a link state update packet on the interface.

Syntax `ip ospf transmit-delay seconds`

Parameters *seconds* — Set the time (in seconds) required to send a link-state update (1 to 3600).

Default 1 second

Command Mode INTERFACE

Usage Information Set the estimated time required to send a link-state update packet. When you set the `ip ospf transmit-delay` value, take into account the transmission and propagation delays for the interface. The `no` version of this command resets the value to the default.

Example

```
OS10(conf-if-eth1/1/4)# ip ospf transmit-delay 5
```

Supported Releases 10.2.0E or later

log-adjacency-changes

Enables logging of syslog messages about changes in the OSPF adjacency state.

Syntax `log-adjacency-changes`

Parameters None

Default Disabled

Command Mode ROUTER-OSPF

Usage Information The `no` version of this command resets the value to the default.

Example

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# log-adjacency-changes
```

Supported Releases 10.2.0E or later

max-metric router-lsa

Configures OSPF to advertise a maximum metric on a router so that it is not desired as an intermediate hop from other routers.

Syntax `max-metric router-lsa`

Parameters None

Default Not configured

Command Mode ROUTER-OSPF

Usage Information Routers in the network do not prefer other routers as the next intermediate hop after they calculate the shortest path. The `no` version of this command disables maximum metric advertisement configuration.

Example

```
OS10(conf-router-ospf-10)# max-metric router-lsa
```

Supported Releases 10.2.0E or later

maximum-paths

Enables forwarding of packets over multiple paths.

Syntax	<code>maximum-paths number</code>
Parameters	<i>number</i> — Enter the number of paths for OSPF (1 to 128).
Default	64
Command Mode	ROUTER-OSPF
Usage Information	The <code>no</code> version of this command resets the value to the default.

Example

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# maximum-paths 1
```

Supported Releases	10.2.0E or later
---------------------------	------------------

redistribute

Redistributes information from another routing protocol or routing instance to the OSPFv2 process.

Syntax	<code>redistribute {bgp as-number connected static} [route-map map-name]</code>
Parameters	<ul style="list-style-type: none">• <i>as-number</i> — Enter an autonomous number to redistribute BGP routing information throughout the OSPF instance (1 to 4294967295).• <i>connected</i> — Enter the information from connected (active) routes on interfaces to redistribute.• <i>static</i> — Enter the information from static routes on interfaces redistribute.• <i>route-map name</i> — Enter the name of a configured route-map.
Defaults	Not configured
Command Mode	ROUTER-OSPF
Usage Information	When an OSPF redistributes, the process is not completely removed from the BGP configuration. The <code>no</code> version of this command disables the redistribute configuration.

Example

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# redistribute bgp 4 route-map dell1
```

Example (Connected)

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# redistribute connected route-map dell2
```

Supported Releases	10.2.0E or later
---------------------------	------------------

router-id

Configures a fixed router ID for the OSPF process.

Syntax	<code>router-id ip-address</code>
Parameters	<i>ip-address</i> — Enter the IP address of the router as the router ID.
Default	Not configured
Command Mode	ROUTER-OSPF
Usage Information	Configure an arbitrary value in the IP address format for each router. Each router ID must be unique. Use the fixed router ID for the active OSPF router process. Changing the router ID brings down the existing OSPF adjacency. The new router ID becomes effective immediately. The <code>no</code> version of this command disables the router ID configuration.

Example

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# router-id 10.10.1.5
```

Supported Releases

10.2.0E or later

router ospf

Enters Router OSPF mode and configures an OSPF instance.

Syntax `router ospf instance-number`

Parameters `instance-number`—Enter a router OSPF instance number, from 1 to 65535.

Default Not configured

Command Mode CONFIGURATION

Usage Information Assign an IP address to an interface before using this command. The `no` version of this command deletes an OSPF instance.

Example

```
OS10(config)# router ospf 10
```

Supported Releases

10.2.0E or later

show ip ospf

Displays OSPF instance configuration information.

Syntax `show ip ospf [instance-number]`

Parameters `instance-number` — View OSPF information for a specified instance number (1 to 65535)

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show ip ospf 10
Routing Process ospf 10 with ID 111.2.1.1
Supports only single TOS (TOS0) routes
It is an Autonomous System Boundary Router
It is Flooding according to RFC 2328
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
  Area (0.0.0.0)
    Number of interface in this area is 3
    SPF algorithm executed 38 times
    Area ranges are
```

Supported Releases

10.2.0E or later

show ip ospf asbr

Displays all the ASBR visible to OSPF.

Syntax `show ip ospf [process-id] asbr`

Parameters *process-id*—(Optional) Displays information based on the process ID.

Default Not configured

Command Mode EXEC

Usage Information You can isolate problems with external routes. External OSPF routes are calculated by adding the LSA cost to the cost of reaching the ASBR router. If an external route does not have the correct cost, this command determines if the path to the originating router is correct. ASBRs that are not in directly connected areas display. You can determine if an ASBR is in a directly connected area or not by the flags. For ASBRs in a directly connected area, E flags are set.

Example

```
OS10# show ip ospf 10 asbr

RouterID      Flags      Cost      Nexthop      Interface      Area
112.2.1.1    E/-/-/    1         110.1.1.2    vlan3050      0.0.0.0
111.2.1.1    E/-/-/    0         0.0.0.0      -              -
```

Supported Releases 10.2.0E or later

show ip ospf database

Displays all LSA information. You must enable OSPF to generate output.

Syntax `show ip ospf [process-id] database`

Parameters *process-id* — (Optional) View LSA information for a specific OSPF process ID. If you do not enter a process ID, the command applies to all the configured OSPF processes.

Default Not configured

Command Mode EXEC

Usage Information

- *Link ID* — Identifies the router ID.
- *ADV Router* — Identifies the advertising router's ID.
- *Age* — Displays the link state age.
- *Seq#* — Identifies the link state sequence number (identifies old or duplicate LSAs).
- *Checksum* — Displays the Fletcher checksum of an LSA's complete contents.
- *Link count* — Displays the number of interfaces for that router.

Example

```
OS10# show ip ospf 10 database
OSPF Router with ID (111.2.1.1) (Process ID 10)

          Router (Area 0.0.0.0)

Link ID      ADV Router      Age      Seq#      Checksum      Link
count
111.2.1.1    111.2.1.1        1281     0x8000000d  0x9bf2        3
111.111.111.1 111.111.111.1    1430     0x8000021a  0x515a        1
111.111.111.2 111.111.111.2    1430     0x8000021a  0x5552        1
112.2.1.1    112.2.1.1        1282     0x8000000b  0x0485        3
112.112.112.1 112.112.112.1    1305     0x80000250  0xbab2        1
112.112.112.2 112.112.112.2    1305     0x80000250  0xbeaa        1

          Network (Area 0.0.0.0)

Link ID      ADV Router      Age      Seq#      Checksum
110.1.1.2    112.2.1.1        1287     0x80000008  0xd2b1
111.1.1.1    111.2.1.1        1458     0x80000008  0x1b8f
111.2.1.1    111.2.1.1        1458     0x80000008  0x198f
112.1.1.1    112.2.1.1        1372     0x80000008  0x287c
112.2.1.1    112.2.1.1        1372     0x80000008  0x267c

          Summary Network (Area 0.0.0.0)
```

Supported Releases 10.2.0E or later

show ip ospf database asbr-summary

Displays information about AS boundary LSAs.

Syntax	<code>show ip ospf [<i>process-id</i>] database asbr-summary</code>
Parameters	<i>process-id</i> —(Optional) Displays the AS boundary LSA information for a specified OSPF process ID. If you do not enter a process ID, this applies only to the first OSPF process.
Default	Not configured
Command Mode	EXEC
Usage Information	<ul style="list-style-type: none">• <code>LS Age</code>—Displays the LS age.• <code>Options</code>—Displays optional capabilities.• <code>LS Type</code>—Displays the Link State type.• <code>Link State ID</code>—Identifies the router ID.• <code>Advertising Router</code>—Identifies the advertising router's ID.• <code>LS Seq Number</code>—Identifies the LS sequence number (identifies old or duplicate LSAs).• <code>Checksum</code>—Displays the Fletcher checksum of an LSA's complete contents.• <code>Length</code>—Displays the LSA length in bytes.• <code>Network Mask</code>—Identifies the network mask implemented on the area.• <code>TOS</code>—Displays the ToS options. The only option available is zero..• <code>Metric</code>—Displays the LSA metric.

Example

```
OS10# show ip ospf 10 database asbr-summary

  OSPF Router with ID (1.1.1.1) (Process ID 100)

  Summary Asbr (Area 0.0.0.1)

LS age: 32
Options: (No TOS-Capability, No DC)
LS type: Summary Asbr
Link State ID: 8.1.1.1
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0xB595
Length: 28
Network Mask: /0
      TOS: 0 Metric: 0
```

Supported Releases 10.2.0E or later

show ip ospf database external

Displays information about the AS external (Type 5) LSAs.

Syntax	<code>show ip ospf [<i>process-id</i>] database external</code>
Parameters	<i>process-id</i> —(Optional) Displays AS external (Type 5) LSA information for a specified OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.
Default	Not configured
Command Mode	EXEC
Usage Information	<ul style="list-style-type: none">• <code>LS Age</code> — Displays the LS age.• <code>Options</code> — Displays the optional capabilities available on the router.• <code>LS Type</code> — Displays the Link State type.

- **Link State ID** — Identifies the router ID.
- **Advertising Router** — Identifies the advertising router's ID.
- **LS Seq Number** — Identifies the LS sequence number (identifies old or duplicate LSAs).
- **Checksum** — Displays the Fletcher checksum of an LSA's complete contents.
- **Length** — Displays the LSA length in bytes.
- **Network Mask** — Identifies the network mask implemented on the area.
- **TOS** — Displays the ToS options. The only option available is zero..
- **Metric** — Displays the LSA metric.

Example

```
OS10# show ip ospf 10 database external

OSPF Router with ID (111.2.1.1) (Process ID 10)

                Type-5 AS External

LS age: 1424
Options: (No TOS-capability, No DC, E)
LS type: Type-5 AS External
Link State ID: 110.1.1.0
Advertising Router: 111.2.1.1
LS Seq Number: 0x80000009
Checksum: 0xc69a
Length: 36
Network Mask: /24
    Metric Type: 2
    TOS: 0
    Metric: 20
    Forward Address: 110.1.1.1
    External Route Tag: 0
```

Supported Releases

10.2.0E or later

show ip ospf database network

Displays information about network (Type 2) LSA information.

Syntax `show ip ospf [process-id] database network`

Parameters *process-id* — (Optional) Displays network (Type2) LSA information for a specified OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

Usage Information

- **LS Age**—Displays the LS age.
- **Options**—Displays optional capabilities.
- **LS Type**—Displays the Link State type.
- **Link State ID**—Identifies the router ID.
- **Advertising Router**—Identifies the advertising router's ID.
- **LS Seq Number**—Identifies the LS sequence number (identifies old or duplicate LSAs).
- **Checksum**—Displays the Fletcher checksum of an LSA's complete contents.
- **Length**—Displays the LSA length in bytes.
- **Network Mask**—Identifies the network mask implemented on the area.
- **TOS**—Displays the ToS options. The only option available is zero..
- **Metric**—Displays the LSA metric.

Example

```
OS10# show ip ospf 10 database network
OSPF Router with ID (111.2.1.1) (Process ID 10)

                Network (Area 0.0.0.0)
```

```

LS age: 1356
Options: (No TOS-capability, No DC, E)
LS type: Network
Link State ID: 110.1.1.2
Advertising Router: 112.2.1.1
LS Seq Number: 0x80000008
Checksum: 0xd2b1
Length: 32
Network Mask: /24
    Attached Router: 111.2.1.1
    Attached Router: 112.2.1.1

```

Supported Releases 10.2.0E or later

show ip ospf database nssa external

Displays information about the NSSA-External (Type 7) LSA.

Syntax `show ip ospf [process-id] database nssa external`

Parameters *process-id* — (Optional) Displays NSSA-External (Type7) LSA information for a specified OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

Usage Information

- **LS Age** — Displays the LS age.
- **Options** — Displays the optional capabilities available on the router.
- **LS Type** — Displays the Link State type.
- **Link State ID** — Identifies the router ID.
- **Advertising Router** — Identifies the advertising router's ID.
- **LS Seq Number** — Identifies the LS sequence number (identifies old or duplicate LSAs).
- **Checksum** — Displays the Fletcher checksum of an LSA's complete contents.
- **Length** — Displays the LSA length in bytes.
- **Network Mask**—Identifies the network mask implemented on the area.
- **TOS**—Displays the ToS options. The only option available is zero.
- **Metric**—Displays the LSA metric.

Example

```

OS10# show ip ospf database nssa external

      OSPF Router with ID (2.2.2.2) (Process ID 100)

      NSSA External (Area 0.0.0.1)

LS age: 98
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 0.0.0.0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000001
Checksum: 0x430C
Length: 36
Network Mask: /0
    Metric Type: 1
    TOS: 0
    Metric: 16777215
    Forward Address: 0.0.0.0
    External Route Tag: 0

LS age: 70
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 0.0.0.0

```

```

Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0x2526
Length: 36
Network Mask: /0
    Metric Type: 1
    TOS: 0
    Metric: 0
    Forward Address: 0.0.0.0
    External Route Tag: 0

LS age: 65
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 12.1.1.0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0xBDEA
Length: 36
Network Mask: /24
    Metric Type: 2
    TOS: 0
    Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 0

LS age: 65
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 13.1.1.0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0xB0F6
Length: 36
Network Mask: /24
    Metric Type: 2
    TOS: 0
    Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 0

LS age: 65
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 14.1.1.0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0xA303
Length: 36
Network Mask: /24
    Metric Type: 2
    TOS: 0
    Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 0

```

Supported Releases 10.2.0E or later

show ip ospf database opaque-area

Displays information about the opaque-area (Type 10) LSA.

Syntax `show ip ospf [process-id] database opaque-area`

Parameters *process-id* — (Optional) Displays the opaque-area (Type 10) information for an OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

- Usage Information**
- **LS Age** — Displays the LS age.
 - **Options** — Displays the optional capabilities available on the router.
 - **LS Type** — Displays the Link State type.
 - **Link State ID** — Identifies the router ID.
 - **Advertising Router** — Identifies the advertising router's ID.
 - **LS Seq Number** — Identifies the LS sequence number (identifies old or duplicate LSAs).
 - **Checksum** — Displays the Fletcher checksum of an LSA's complete contents.
 - **Length** — Displays the LSA length in bytes.
 - **Opaque Type** — Identifies the Opaque type field (the first 8 bits of the LS ID).
 - **Opaque ID** — Identifies the Opaque type-specific ID (the remaining 24 bits of the LS ID).

Example

```
OS10# show ip ospf database opaque-area
      OSPF Router with ID (1.1.1.1) (Process ID 100)

      Type-10 Area Local Opaque (Area 0.0.0.1)

LS age: 3600
Options: (No TOS-Capability, No DC)
LS type: Type-10 Area Local Opaque
Link State ID: 8.1.1.2
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000008
Checksum: 0x83B8
Length: 28
Opaque Type: 8
Opaque ID: 65794
!!
!
```

Supported Releases 10.2.0E or later

show ip ospf database opaque-as

Displays information about the opaque-as (Type 11) LSAs.

Syntax `show ip ospf [process-id] opaque-as`

Parameters *process-id* — (Optional) Displays opaque-as (Type 11) LSA information for a specified OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

- Usage Information**
- **LS Age** — Displays the LS age.
 - **Options** — Displays the optional capabilities available on the router.
 - **LS Type** — Displays the Link State type.
 - **Link State ID** — Identifies the router ID.
 - **Advertising Router** — Identifies the advertising router's ID.
 - **LS Seq Number** — Identifies the LS sequence number (identifies old or duplicate LSAs).
 - **Checksum** — Displays the Fletcher checksum of an LSA's complete contents.
 - **Length** — Displays the LSA length in bytes.
 - **Opaque Type** — Identifies the Opaque type field (the first 8 bits of the LS ID).
 - **Opaque ID** — Identifies the Opaque type-specific ID (the remaining 24 bits of the LS ID).

Example

```
OS10# show ip ospf 100 database opaque-as

      OSPF Router with ID (1.1.1.1) (Process ID 100)
```


Type-11 AS Opaque

```
LS age: 3600
Options: (No TOS-Capability, No DC)
LS type: Type-11 AS Opaque
Link State ID: 8.1.1.3
Advertising Router: 2.2.2.2
LS Seq Number: 0x8000000D
Checksum: 0x61D3
Length: 36
Opaque Type: 8
Opaque ID: 65795
```

Supported Releases 10.2.0E or later

show ip ospf database opaque-link

Displays information about the opaque-link (Type 9) LSA.

Syntax `show ip ospf [process-id] database opaque-link`

Parameters *process-id* — (Optional) Displays the opaque-link (Type 9) LSA information for an OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

Usage Information

- **LS Age** — Displays the LS age.
- **Options** — Displays the optional capabilities available on the router.
- **LS Type** — Displays the Link State type.
- **Link State ID** — Identifies the router ID.
- **Advertising Router** — Identifies the advertising router's ID.
- **LS Seq Number** — Identifies the LS sequence number (identifies old or duplicate LSAs).
- **Checksum** — Displays the Fletcher checksum of an LSA's complete contents.
- **Length** — Displays the LSA length in bytes.
- **Opaque Type** — Identifies the Opaque type field (the first 8 bits of the LS ID).
- **Opaque ID** — Identifies the Opaque type-specific ID (the remaining 24 bits of the LS ID).

Example

```
OS10# show ip ospf 100 database opaque-link
      OSPF Router with ID (1.1.1.1) (Process ID 100)

      Type-9 Link Local Opaque (Area 0.0.0.1)

LS age: 3600
Options: (No TOS-Capability, No DC)
LS type: Type-9 Link Local Opaque
Link State ID: 8.1.1.1
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000007
Checksum: 0x9DA1
Length: 28
Opaque Type: 8
Opaque ID: 65793
```

Supported Releases 10.2.0E or later

show ip ospf database router

Displays information about the router (Type 1) LSA.

Syntax `show ip ospf process-id database router`

Parameters *process-id* — (Optional) Displays the router (Type 1) LSA for an OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

Usage Output:

Information

- *LS age*—Displays the LS age.
- *Options*—Displays optional capabilities.
- *LS Type*—Displays the Link State type.
- *Link State ID*—Identifies the router ID.
- *Advertising Router*—Identifies the advertising router's ID.
- *LS Seq Number*—Identifies the LS sequence number (identifies old or duplicate LSAs).
- *Checksum*—Displays the Fletcher checksum of an LSA's complete contents.
- *Length*—Displays the LSA length in bytes.
- *TOS*—Displays the ToS options. The only option available is zero..
- *Metric*—Displays the LSA metric.

Example

```
OS10# show ip ospf 10 database router
      OSPF Router with ID (111.2.1.1) (Process ID 10)
          Router (Area 0.0.0.0)
      LS age: 1419
      Options: (No TOS-capability, No DC, E)
      LS type: Router
      Link State ID: 111.2.1.1
      Advertising Router: 111.2.1.1
      LS Seq Number: 0x8000000d
      Checksum: 0x9bf2
      Length: 60
      AS Boundary Router
      Number of Links: 3
      Link connected to: a Transit Network
      (Link ID) Designated Router address: 110.1.1.2
      (Link Data) Router Interface address: 110.1.1.1
      Number of TOS metric: 0
      TOS 0 Metric: 1
      Link connected to: a Transit Network
      (Link ID) Designated Router address: 111.1.1.1
      (Link Data) Router Interface address: 111.1.1.1
      Number of TOS metric: 0
      TOS 0 Metric: 1
      Link connected to: a Transit Network
      (Link ID) Designated Router address: 111.2.1.1
      (Link Data) Router Interface address: 111.2.1.1
      Number of TOS metric: 0
      TOS 0 Metric: 1
```

Supported Releases 10.2.0E or later

show ip ospf database summary

Displays the network summary (Type 3) LSA routing information.

Syntax `show ip ospf [process-id] database summary`

Parameters *process-id*—(Optional) Displays LSA information for a specific OSPF process ID. If you do not enter a process ID, this command applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

Usage Information

- **LS Age**—Displays the LS age.
- **Options**—Displays the optional capabilities available on the router.
- **LS Type**—Displays the Link State type.
- **Link State ID**—Identifies the router ID.
- **Advertising Router**—Identifies the advertising router's ID.
- **LS Seq Number**—Identifies the LS sequence number (identifies old or duplicate LSAs).
- **Checksum**—Displays the Fletcher checksum of an LSA's complete contents.
- **Length**—Displays the LSA length in bytes.
- **Network Mask**—Identifies the network mask implemented on the area.
- **TOS**—Displays the ToS options. The only option available is zero..
- **Metric**—Displays the LSA metric.

Example

```
OS10# show ip ospf 10 database summary
      OSPF Router with ID (111.2.1.1) (Process ID 10)

      Summary Network (Area 0.0.0.0)

      LS age: 623
      Options: (No TOS-capability, No DC)
      C: Summary Network
      Link State ID: 115.1.1.0
      Advertising Router: 111.111.111.1
      LS Seq Number: 0x800001e8
      Checksum: 0x4a67
      Length: 28
      Network Mask: /24
      TOS: 0 Metric: 0
```

Supported Releases 10.2.0E or later

show ip ospf interface

Displays the configured OSPF interfaces. You must enable OSPF to display output.

Syntax `show ip ospf interface [process-id] interface` or `show ip ospf [process-id] interface [interface]`

Parameters

- *process-id* — (Optional) Displays information for an OSPF Process ID. If you do not enter a Process ID, this command applies only to the first OSPF process.
- *interface* — (Optional) Enter the interface information:
 - *ethernet* — Enter the Ethernet interface information (1 to 48)
 - *port channel* — Enter the port-channel interface number (1 to 128).
 - *vlan* — Enter the VLAN interface number (1 to).

Default Not configured

Command Mode EXEC

Example

```
OS10# show ip ospf interface
ethernet1/1/1 is up, line protocol is up
  Internet Address 10.0.0.2/24, Area 0.0.0.0
  Process ID 200, Router ID 10.0.0.2, Network Type broadcast, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.2, Interface address 10.0.0.2 (local)
  Backup Designated router (ID) , Interface address 0.0.0.0
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Simple password authentication enabled
Neighbor Count is 0, Adjacent neighbor count is 0
```

Supported Releases 10.2.0E or later

show ip ospf routes

Displays OSPF routes received from neighbors along with parameters like cost, next-hop, area, interface, and type of route.

Syntax `show ip ospf [process-id] routes [prefix IP-prefix]`

Parameters

- *process-id* — (Optional) Enter OSPFv2 Process ID to view information specific to the ID.
- *IP-prefix* — (Optional) Specify an IP address to view information specific to the IP address.

Default None

Command Mode EXEC

Usage Information Displays the cost metric for each neighbor and interfaces.

Example

```
OS10# show ip ospf 10 routes
Prefix          Cost      Nexthop      Interface     Area
Type
110.1.1.0       1         0.0.0.0      vlan3050      0.0.0.0
  intra-area
111.1.1.0       1         0.0.0.0      vlan3051      0.0.0.0
  intra-area
111.2.1.0       1         0.0.0.0      vlan3053      0.0.0.0
  intra-area
```

Supported Releases 10.2.0E or later

show ip ospf statistics

Displays OSPF traffic statistics.

Syntax `show ip ospf [instance-number] statistics [interface interface]`

Parameters

- *instance-number* — (Optional) Enter an OSPF instance number (1 to 65535).
- *interface interface* — (Optional) Enter the interface information:
 - *ethernet node/slot/port[:subport]* — Enter an Ethernet port interface.
 - *port-channel number* — Enter the port-channel interface number (1 to 128).
 - *vlan vlan-id* — Enter the VLAN ID number (1 to 4093).

Default Not configured

Command Mode EXEC

Usage Information This command displays OSPFv2 traffic statistics for a specified instance or interface, or for all OSPFv2 instances and interfaces.

Example

```
OS10# show ip ospf 10 statistics
Interface vlan3050
Receive Statistics
  rx-invalid          0      rx-invalid-bytes      0
  rx-hello            0      rx-hello-bytes        0
  rx-db-des           0      rx-db-des-bytes       0
  rx-ls-req           0      rx-ls-req-bytes       0
  rx-ls-upd           0      rx-ls-upd-bytes       0
  rx-ls-ack           0      rx-ls-ack-bytes       0
Transmit Statistics
```

tx-failed	0	tx-failed-bytes	0
tx-hello	0	tx-hello-bytes	0
tx-db-des	0	tx-db-des-bytes	0
tx-ls-req	0	tx-ls-req-bytes	0
tx-ls-upd	0	tx-ls-upd-bytes	0
tx-ls-ack	0	tx-ls-ack-bytes	0
Error packets (Receive statistics)			
bad-src	0	dupe-id	0
0		hello-err	
mtu-mismatch	0	nbr-ignored	0
0		wrong-PROTO	
resource-err	0	bad-lsa-len	0
0		lsa-bad-type	
lsa-bad-len	0	lsa-bad-cksum	0
0		auth-fail	
netmask-mismatch	0	hello-tmr-mismatch	0
0		dead-ivl-mismatch	
options-mismatch	0	nbr-admin-down	0
0		own-hello-drop	
self-orig	0	wrong-length	0
0		checksum-error	
version-mismatch	0	area-mismatch	0

Supported Releases 10.2.0E or later

show ip ospf topology

Displays routers which are directly connected to OSPF areas.

Syntax `show ip ospf [process-id] topology`

Parameters *process-id* — (Optional) Displays OSPF process information. If you do not enter a process ID, this applies only to the first OSPF process.

Default Not configured

Command Mode EXEC

Usage Information The “E” flag output indicates the router listed is an ASBR. The “B” flag indicates that the router listed is an area border router (ABR). If the Flag field shows both E and B, it indicates that the listed router is both an ASBR and an ABR.

Example

```
OS10# show ip ospf 10 topology

Router ID      Flags      Cost  Nexthop      Interface  Area
111.111.111.1  -/B/-/    1     111.1.1.2    V1 3051    0
111.111.111.2  -/B/-/    1     111.2.1.2    V1 3053    0
112.2.1.1      E/-/-/    1     110.1.1.2    V1 3050    0
112.112.112.1 -/B/-/    2     110.1.1.2    V1 3050    0
112.112.112.2 -/B/-/    2     110.1.1.2    V1 3050    0
```

Supported Releases 10.2.0E or later

summary-address

Configures a summary address for an ASBR to advertise one external route as an aggregate, for all redistributed routes covered by specified address range.

Syntax `summary-address ip-address/mask [not-advertise | tag tag-value]`

Parameters

- *ip-address/mask*—Enter the IP address to be summarized along with the mask.
- *not-advertise*—(Optional) Suppresses IP addresses that do not match the network prefix/mask.
- *tag-value*—(Optional) Enter a value to match the routes redistributed through a route map (1 to 65535).

Default)	Not configured
Command Mode	ROUTER-OSPF
Usage Information	The <code>no</code> version of this command disables the summary address.

Example

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# summary-address 10.0.0.0/8 not-advertise
```

Supported Releases	10.3.0E or later
---------------------------	------------------

timers lsa arrival

Configures the LSA acceptance intervals.

Syntax	<code>timers lsa arrival arrival-time</code>
Parameters	<i>arrival-time</i> — Set the interval between receiving the LSA in milliseconds (0 to 600,000).
Default	1000 milliseconds
Command Mode	ROUTER-OSPF
Usage Information	Setting the LSA arrival time between receiving the LSA repeatedly ensures that the system gets enough time to accept the LSA. The <code>no</code> version of this command resets the value to the default.

Example

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# timers lsa arrival 2000
```

Supported Releases	10.2.0E or later
---------------------------	------------------

timers spf

Enables shortest path first (SPF) throttling to delay an SPF calculation when a topology change occurs.

Syntax	<code>timers spf [start-time [hold-time [max-wait]]]</code>
Parameters	<ul style="list-style-type: none"> • <i>start-time</i> — Sets the initial SPF delay in milliseconds (1 to 600000; default 1000). • <i>hold-time</i> — Sets the additional hold time between two SPF calculations in milliseconds (1 to 600000; default 10000). • <i>max-wait</i> — Sets the maximum wait time between two SPF calculations in milliseconds (1 to 600000; default 10000).
Default	<ul style="list-style-type: none"> • <i>start-time</i> — 1000 milliseconds • <i>hold-time</i> — 10000 milliseconds • <i>max-wait</i> — 10000 milliseconds
Command Mode	ROUTER-OSPF
Usage Information	<p>By default, SPF timers are disabled in an OSPF instance.</p> <p>Use SPF throttling to delay SPF calculations during periods of network instability. In an OSPF network, a topology change event triggers an SPF calculation after a start time. When the start timer finishes, a hold time may delay the next SPF calculation for an additional time. When the hold timer is running:</p> <ul style="list-style-type: none"> • Each time a topology change occurs, the SPF calculation is delayed for double the configured hold time up to maximum wait time. • If no topology change occurs, an SPF calculation is performed and the hold timer is reset to its configured value. <p>If you do not specify a start-time, hold-time or max-wait value, the default values are used. The <code>no</code> version of this command removes the configured SPF timers and disables SPF throttling in an OSPF instance.</p>

Example

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# timers spf 1200 2300 3400
OS10(config-router-ospf-100)# do show ip ospf

Routing Process ospf 100 with ID 12.1.1.1
Supports only single TOS (TOS0) routes
It is Flooding according to RFC 2328
SPF schedule delay 1200 msec, Hold time between two SPFs 2300 msec
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 1 times
```

Supported Releases 10.4.0E(R1) or later

timers throttle lsa all

Configures the LSA transmit intervals.

Syntax `timers lsa all [start-interval | hold-interval | max-interval]`

Parameters

- *start-interval* — Sets the minimum interval between initial sending and re-sending the same LSA in milliseconds (0 to 600,000).
- *hold-interval* — Sets the next interval to send the same LSA in milliseconds. This is the time between sending the same LSA after the start-interval has been attempted (1 to 600,000).
- *max-interval* — Sets the maximum amount of time the system waits before sending the LSA in milliseconds (1 to 600,000).

Default

- start-interval — 0 milliseconds
- hold-interval — 5000 milliseconds
- max-interval — 5000 milliseconds

Command Mode ROUTER-OSPF

Usage Information The `no` version of this command removes the LSA transmit timer.

Example

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# timers throttle lsa all 100 300 1000
```

Supported Releases 10.2.0E or later

OSPFv3

OSPFv3 is an IPv6 link-state routing protocol that supports IPv6 unicast address families (AFs). OSPFv3 is disabled by default. You must configure at least one interface, either physical or loopback. The OSPF process automatically starts when OSPFv3 is enabled for one or more interfaces. Any area besides *area 0* can have any number ID assigned to it.

Enable OSPFv3

1. Enable OSPFv3 globally and configure an OSPFv3 instance in CONFIGURATION mode.

```
router ospfv3 instance-number
```

2. Enter the interface information to configure the interface for OSPFv3 in INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
```

3. Enable (or bring up) the interface in INTERFACE mode.

```
no shutdown
```

4. Disable the default switchport configuration and remove it from an interface or a LAG port in INTERFACE mode.

```
no switchport
```

5. Enable the OSPFv3 on an interface in INTERFACE mode.

```
ipv6 ospfv3 process-id area area-id
```

- *process-id* — Enter the OSPFv3 process ID for a specific OSPFv3 process (1 to 65535).
- *area-id* — Enter the OSPF area ID as an IP address (A.B.C.D) or number (1 to 65535).

Enable OSPFv3

```
OS10(config)# router ospfv3 100
OS10(config-router-ospfv3-100)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ipv6 ospfv3 300 area 0.0.0.0
```

Assign Router ID

You can assign a router ID for the OSPFv3 process. Configure an arbitrary value in the IP address format for each router. Each router ID must be unique. Use the fixed router ID for the active OSPFv3 router process. Changing the router ID brings down the existing OSPFv3 adjacency. The new router ID becomes effective immediately.

- Assign the router ID for the OSPFv3 process in ROUTER-OSPFv3 mode.

```
router-id ip-address
```

Assign router ID

```
OS10(config)# router ospfv3 100
OS10(config-router-ospfv3-100)# router-id 10.10.1.5
```

View OSPFv3 Status

```
OS10# show ipv6 ospf
Routing Process ospfv3 100 with ID 10.10.1.5
It is an Area Border Router
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 2, normal 2 stub 0 nssa
Area (0.0.0.0)
  Number of interface in this area is 1
  SPF algorithm executed 42 times
Area (0.0.0.1)
  Number of interface in this area is 1
  SPF algorithm executed 42 times
```

Configure Stub Areas

The Type 5 LSAs are not flooded into stub areas. The ABR advertises a default route into the stub area to which it is attached. Stub area routers use the default route to reach external destinations.

1. Enable OSPFv3 routing and enter ROUTER-OSPFv3 mode (1 to 65535).

```
router ospfv3 instance number
```

2. Configure an area as a stub area in ROUTER-OSPFv3 mode.

```
area area-id stub [no-summary]
```

- *area-id* — Enter the OSPFv3 area ID as an IP address (A.B.C.D) or number (1 to 65535).
- *no-summary* — (Optional) Enter to prevent an ABR from sending summary LSAs into the stub area.

Configure Stub Area

```
OS10(config)# router ospfv3 10
OS10(conf-router-ospf-10)# area 10.10.5.1 stub no-summary
```

View Stub Area Configuration

```
OS10# show running-configuration ospfv3
!
interface ethernet1/1/3
ipv6 ospf 65 area 0.0.0.2
!
router ospfv3 65
area 0.0.0.2 stub no-summary

OS10# show ipv6 ospf database
      OSPF Router with ID (199.205.134.103) (Process ID 65)

Router Link States (Area 0.0.0.2)

ADV Router      Age      Seq#      Fragment ID Link count Bits
-----
199.205.134.103 32      0x80000002 0          1
202.254.156.15 33      0x80000002 0          1          B

Net Link States (Area 0.0.0.2)

ADV Router      Age      Seq#      Link ID  Rtr count
-----
202.254.156.15 38      0x80000001 12       2

Inter Area Prefix Link States (Area 0.0.0.2)

ADV Router      Age      Seq#      Prefix
-----
202.254.156.15 93      0x80000001  ::/0

Intra Area Prefix Link States (Area 0.0.0.2)

ADV Router      Age      Seq#      Link ID  Ref-lstype Ref-LSID
-----
202.254.156.15 34      0x80000003 65536    0x2002     12

Link (Type-8) Link States (Area 0.0.0.2)

ADV Router      Age      Seq#      Link ID  Interface
-----
199.205.134.103 42      0x80000001 12       ethernet1/1/3
202.254.156.15 54      0x80000001 12       ethernet1/1/3
```

Enable Passive Interfaces

A passive interface is one that does not send or receive routing information. Configuring an interface as a passive interface suppresses routing updates (both receiving and sending).

Although the passive interface does not send or receive routing updates, the network on that interface is still included in OSPF updates sent through other interfaces. You can remove an interface from passive interfaces using the `no ipv6 ospf passive` command.

1. Enter an interface type in INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
```

2. Configure the interface as a passive interface in INTERFACE mode.

```
ipv6 ospf passive
```

Configure Passive Interfaces

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ipv6 ospf passive
```

View Passive Interfaces

```
OS10# show running-configuraiton
!!!
!!
interface ethernet1/1/1
 ip address 10.10.10.1/24
 no switchport
 no shutdown
 ipv6 ospf 100 area 0
 ipv6 ospf passive
!!
!
```

Interface OSPFv3 Parameters

Interface parameter values must be consistent across all interfaces to avoid routing errors. For example, set the same time interval for the hello packets on all routers in the OSPF network to prevent misconfiguration of OSPF neighbors.

1. Enter the interface to change the OSPFv3 parameters in CONFIGURATION mode.

```
interface interface-name
```

2. Change the cost associated with OSPFv3 traffic on the interface in INTERFACE mode (1 to 65535, default depends on the interface speed).

```
ipv6 ospf cost
```

3. Change the time interval the router waits before declaring a neighbor dead in INTERFACE mode (1 to 65535, default 40). The dead interval must be four times the hello interval. The dead interval must be the same on all routers in the OSPFv3 network.

```
ipv6 ospf dead-interval seconds
```

4. Change the time interval (in seconds) between hello-packet transmission in INTERFACE mode (1 to 65535, default 10). The hello interval must be the same on all routers in the OSPFv3 network.

```
ipv6 ospf hello-interval seconds
```

5. Change the priority of the interface, which determines the DR for the OSPFv3 broadcast network in INTERFACE mode (0 to 255, default 1).

```
ipv6 ospf priority number
```

Change OSPFv3 Interface Parameters

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 ospf hello-interval 5
```

```
OS10(config-if-eth1/1/1)# ipv6 ospf dead-interval 20
OS10(config-if-eth1/1/1)# ipv6 ospf priority 4
```

View OSPFv3 Interface Parameters

```
OS10# show ipv6 ospf interface
fortyGigE 0/0 is up, line protocol is up
  Link Local Address fe80::92b1:1cff:fef4:a39d, Interface ID 1048581
  Area 0, Process ID 10, Instance ID 0, Router ID 60.60.60.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 0 sec, State BDR, Priority 4
  Designated router on this network is 70.70.70.1
  Backup designated router on this network is 60.60.60.1 (local)
  Timer intervals configured, Hello 5, Dead 20
```

Default route

You can generate an external default route and distribute the default information to the OSPFv3 routing domain.

- To generate the default route, use the `default-information originate [always]` command in ROUTER-OSPFv3 mode.

Configure default route

```
OS10(config)# router ospfv3 100
OS10(config-router-ospf-100)# default-information originate always
```

View default route configuration

```
OS10(config-router-ospf-100)# show configuration
!
router ospfv3 100
  default-information originate always
```

OSPFv3 IPsec authentication and encryption

Unlike OSPFv2, OSPFv3 does not have authentication fields in its protocol header to provide security. To provide authentication and confidentiality, OSPFv3 uses IP Security (IPsec) — a collection of security protocols for authenticating and encrypting data packets. OS10 OSPFv3 supports IPsec using the IPv6 authentication header (AH) or IPv6 encapsulating security payload (ESP).

- AH authentication verifies that data is not altered during transmission and ensures that users are communicating with the intended individual or organization. The authentication header is inserted after the IP header with a value of 51. MD5 and SHA1 authentication types are supported; encrypted and unencrypted keys are supported.
- ESP encryption encapsulates data, enabling the protection of data that follows in the datagram. The ESP extension header is inserted after the IP header and before the next layer protocol header. 3DES, DES, AES-CBC, and NULL encryption algorithms are supported; encrypted and unencrypted keys are supported.

Apply IPsec authentication or encryption on a physical, port-channel, or VLAN interface or in an OSPFv3 area. Each configuration consists of a security policy index (SPI) and the key used to validate OSPFv3 packets. After you configure an IPsec protocol for OSPFv3, IPsec operation is invisible to the user.

You can only enable one security protocol (authentication or encryption) at a time on an interface or for an area. Enable IPsec AH with the `ipv6 ospf authentication` command; enable IPsec ESP with the `ipv6 ospf encryption` command.

- A security policy configured for an area is inherited by default on all interfaces in the area.
- A security policy configured on an interface overrides any area-level configured security for the area to which the interface is assigned.
- The configured authentication or encryption policy is applied to all OSPFv3 packets transmitted on the interface or in the area. The IPsec security associations are the same on inbound and outbound traffic on an OSPFv3 interface.
- There is no maximum AH or ESP header length because the headers have fields with variable lengths.

Configure IPsec authentication on interfaces

Prerequisite: Before you enable IPsec authentication on an OSPFv3 interface, first enable IPv6 unicast routing globally, then enable OSPFv3 on the interface, and assign it to an area.

The SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. You cannot configure the same SPI value on another interface even if it uses the same authentication or encryption algorithm.

You cannot use an IPsec authentication type (MD5 or SHA-1) and the `null` setting at same time on an interface. These settings are mutually exclusive.

- Enable IPsec authentication for OSPFv3 packets in Interface mode.

```
ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1} key}
```

- `null` — Prevent an authentication policy configured for the area to be inherited on the interface. This parameter is only used if you configure IPsec area authentication.
- `ipsec spi number` — Enter a unique security policy index (SPI) value (256 to 4294967295).
- `md5` — Enable message digest 5 (MD5) authentication.
- `sha1` — Enable secure hash algorithm 1 (SHA-1) authentication.
- `key` — Enter the text string used in the authentication type. All neighboring OSPFv3 routers must share the key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.

To delete an IPsec authentication policy, use the `no ipv6 ospf authentication ipsec spi number` or `no ipv6 ospf authentication null` command.

Configure IPsec authentication on interface

```
OS10(conf-if-eth1/1/1)# ipv6 ospf authentication ipsec spi 400 md5
12345678123456781234567812345678
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
ipv6 ospf authentication ipsec spi 400 md5 12345678123456781234567812345678
no switchport
no shutdown
ipv6 address 1::1/64
```

IPsec encryption on interfaces

Prerequisite: Before you enable IPsec encryption on an OSPFv3 interface, enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign it to an area.

When you configure encryption on an interface, both IPsec encryption and authentication are enabled. You cannot configure encryption if you have already configured an interface for IPsec authentication (`ipv6 ospf authentication ipsec`). To configure encryption, you must first delete the authentication policy.

- Enable IPsec encryption for OSPFv3 packets in Interface mode.

```
ipv6 ospf encryption ipsec spi number esp encryption-type
key authentication-type key
```

- `ipsec spi number` — Enter a unique security policy index (SPI) value (256 to 4294967295).
- `esp encryption-type key` — Enter the encryption algorithm used with ESP (3DES, DES, AES-CBC, or NULL). For AES-CBC, only the AES-128 and AES-192 ciphers are supported.
- `key` — Enter the text string used in the encryption algorithm. All neighboring OSPFv3 routers must share the key to decrypt information. Only a non-encrypted key is supported. Required lengths of the non-encrypted key are: 3DES — 48 hex digits; DES — 16 hex digits; AES-CBC — 32 hex digits for AES-128 and 48 hex digits for AES-192.
- `authentication-type key` — Enter the encryption authentication algorithm to use (MD5 or SHA1).
- `key` — Enter the text string used in the authentication algorithm. All neighboring OSPFv3 routers must share the key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.

To delete an IPsec encryption policy, use the `no ipv6 ospf encryption ipsec spi number` or `no ipv6 ospf encryption null` command.

Configure IPsec encryption on interface

```
OS10(conf-if-eth1/1/1)# ipv6 ospf encryption ipsec spi 500 esp des 1234567812345678 md5
12345678123456781234567812345678
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
ipv6 ospf encryption ipsec spi 500 esp des 1234567812345678 md5
12345678123456781234567812345678
no switchport
no shutdown
ipv6 address 1::1/64
```

Configure IPsec authentication for OSPFv3 area

Prerequisite: Before you enable IPsec authentication for an OSPFv3 area, enable OSPFv3 globally on the router.

- Enable IPsec authentication for OSPFv3 packets in an area in Router-OSPFv3 mode.

```
area area-id authentication ipsec spi number {MD5 | SHA1} key
```

- `area area-id` — Enter an area ID as a number or IPv6 prefix.
- `ipsec spi number` — Enter a unique security policy index (SPI) value (256 to 4294967295).
- `md5` — Enable message digest 5 (MD5) authentication.
- `sha1` — Enable secure hash algorithm 1 (SHA-1) authentication.
- `key` — Enter the text string used in the authentication type. All OSPFv3 routers in the area share the key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.

To delete an IPsec area authentication policy, use the `no area area-id authentication ipsec spi number` command.

Configure IPsec authentication for an OSPfv3 area

```
OS10(config-router-ospfv3-100)# area 1 authentication ipsec spi 400 md5
12345678123456781234567812345678
OS10(config-router-ospfv3-100)# show configuration
!
router ospfv3 100
area 0.0.0.1 authentication ipsec spi 400 md5 12345678123456781234567812345678
```

IPsec encryption for OSPV3 area

Prerequisite: Before you enable IPsec encryption for an OSPFv3 area, first enable OSPFv3 globally on the router.

When you configure encryption at the area level, both IPsec encryption and authentication are enabled. You cannot configure encryption if you have already configured an IPsec area authentication (`area ospf authentication ipsec`). To configure encryption, you must first delete the authentication policy.

- Enable IPsec encryption for OSPFv3 packets in an area in Router-OSPFv3 mode.

```
area area-id encryption ipsec spi number esp encryption-type key
authentication-type key
```

- `area area-id` — Enter an area ID as a number or IPv6 prefix.
- `ipsec spi number` — Enter a unique security policy index (SPI) value (256 to 4294967295).
- `esp encryption-type` — Enter the encryption algorithm used with ESP (3DES, DES, AES-CBC, or NULL). For AES-CBC, only the AES-128 and AES-192 ciphers are supported.
- `key` — Enter the text string used in the encryption algorithm. All neighboring OSPFv3 routers must share the key to decrypt information. Only a non-encrypted key is supported. Required lengths of the non-encrypted key are: 3DES — 48 hex digits; DES — 16 hex digits; AES-CBC — 32 hex digits for AES-128 and 48 hex digits for AES-192.
- `authentication-type` — Enter the encryption authentication algorithm to use (MD5 or SHA1).
- `key` — Enter the text string used in the authentication algorithm. All neighboring OSPFv3 routers must share the key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must

be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.

To delete an IPsec encryption policy, use the `no area area-id encryption ipsec spi number` command.

Configure IPsec encryption for OSPFv3 area

```
OS10(config-router-ospfv3-100)# area 1 encryption ipsec spi 401 esp des 1234567812345678
md5
12345678123456781234567812345678
OS10(config-router-ospfv3-100)# show configuration
!
router ospfv3 100
area 0.0.0.1 encryption ipsec spi 401 esp des 1234567812345678 md5
12345678123456781234567812345678
```

Troubleshoot OSPFv3

You can troubleshoot OSPFv3 operations, as well as check questions for any typical issues that interrupt a process.

- Is OSPFv3 enabled globally?
- Is OSPFv3 enabled on the interface?
- Are adjacencies established correctly?
- Are the interfaces configured for L3 correctly?
- Is the router in the correct area type?
- Are the OSPF routes included in the OSPF database?
- Are the OSPF routes included in the routing table in addition to the OSPF database?
- Are you able to ping the link-local IPv6 address of adjacent router interface?

Troubleshooting OSPFv3 with show Commands

- View a summary of all OSPF process IDs enabled in EXEC mode.

```
show running-configuration ospfv3
```

- View summary information of IP routes in EXEC mode.

```
show ipv6 route summary
```

- View summary information for the OSPF database in EXEC mode.

```
show ipv6 ospf database
```

- View the configuration of OSPF neighbors connected to the local router in EXEC mode.

```
show ipv6 ospf neighbor
```

View OSPF Configuration

```
OS10# show running-configuration ospfv3
!
interface ethernet1/1/1
ip ospf 100 area 0.0.0.0
!
router ospf 100
log-adjacency-changes
```

OSPFv3 Commands

area authentication

Configures authentication for an OSPFv3 area.

Syntax `area area-id authentication ipsec spi number {MD5 | SHA1} key`

Parameters	<ul style="list-style-type: none"> • <code>area area-id</code> — Enter an area ID as a number or IPv6 prefix. • <code>ipsec spi number</code> — Enter a unique security policy index (SPI) value (256 to 4294967295). • <code>md5</code> — Enable MD5 authentication. • <code>sha1</code> — Enable SHA-1 authentication. • <code>key</code> — Enter the text string used in the authentication type.
Default	OSPFv3 area authentication is not configured.
Command Mode	ROUTER-OSPFv3
Usage Information	<ul style="list-style-type: none"> • Before you enable IPsec authentication for an OSPFv3 area, you must enable OSPFv3 globally on each router. • All OSPFv3 routers in the area must share the same authentication key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.
Example	<pre>OS10(config-router-ospfv3-100)# area 1 authentication ipsec spi 400 md5 12345678123456781234567812345678</pre>
Supported Releases	10.4.0E(R1) or later

area encryption

Configures encryption for an OSPFv3 area.

Syntax	<code>area area-id encryption ipsec spi number esp encryption-type key authentication-type key</code>
Parameters	<ul style="list-style-type: none"> • <code>area area-id</code> — Enter an area ID as a number or IPv6 prefix. • <code>ipsec spi number</code> — Enter a unique security policy index number (256 to 4294967295). • <code>esp encryption-type</code> — Enter the encryption algorithm used with ESP (3DES, DES, AES-CBC, or NULL). For AES-CBC, only the AES-128 and AES-192 ciphers are supported. • <code>key</code> — Enter the text string used in the encryption algorithm. • <code>authentication-type</code> — Enter the encryption authentication algorithm to use (MD5 or SHA1). • <code>key</code> — Enter the text string used in the authentication algorithm.
Default	OSPFv3 area encryption is not configured.
Command Mode	ROUTER-OSPFv3
Usage Information	<ul style="list-style-type: none"> • Before you enable IPsec encryption for an OSPFv3 area, you must enable OSPFv3 globally on each router. • When you configure encryption at the area level, both IPsec encryption and authentication are enabled. You cannot configure encryption if you have already configured an IPsec area authentication (<code>area ospf authentication ipsec</code>). To configure encryption, you must first delete the authentication policy. • All OSPFv3 routers in the area must share the same encryption key to decrypt information. Only a non-encrypted key is supported. Required lengths of the non-encrypted key are: 3DES — 48 hex digits; DES — 16 hex digits; AES-CBC — 32 hex digits for AES-128 and 48 hex digits for AES-192. • All OSPFv3 routers in the area must share the same authentication key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.
Example	<pre>OS10(config-router-ospfv3-100)# area 1 encryption ipsec spi 401 esp des 1234567812345678 md5 12345678123456781234567812345678</pre>
Supported Releases	10.4.0E(R1) or later

area stub

Defines an area as the OSPF stub area.

Syntax	<code>area <i>area-id</i> stub [no-summary]</code>
Parameters	<ul style="list-style-type: none">• <i>area-id</i>—Set the OSPFv3 area ID as an IP address (A.B.C.D) or number (1 to 65535).• <i>no-summary</i>—(Optional) Prevents an area border router from sending summary link advertisements into the stub area.
Default	Not configured
Command Mode	ROUTER-OSPFv3
Usage Information	The <i>no</i> version of this command deletes a stub area.
Example	<pre>OS10(config)# router ospfv3 10 OS10(config-router-ospfv3-10)# area 10.10.1.5 stub</pre>
Supported Releases	10.3.0E or later

auto-cost reference-bandwidth

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

Syntax	<code>auto-cost reference-bandwidth <i>value</i></code>
Parameters	<i>value</i> — Enter the reference bandwidth value to calculate the OSPFv3 interface cost in megabits per second (1 to 4294967).
Default	100000
Command Mode	ROUTER-OSPFv3
Usage Information	The value set by the <code>ipv6 ospf cost</code> command in INTERFACE mode overrides the cost resulting from the <code>auto-cost</code> command. The <i>no</i> version of this command resets the value to the default.
Example	<pre>OS10(config)# router ospfv3 100 OS10(config-router-ospfv3-100)# auto-cost reference-bandwidth 150</pre>
Supported Releases	10.3.0E or later

clear ipv6 ospf process

Clears all OSPFv3 routing tables.

Syntax	<code>clear ipv6 ospf {<i>instance-number</i>} process</code>
Parameters	<i>instance-number</i> — Enter an OSPFv3 instance number (1 to 65535).
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	<pre>OS10# clear ipv6 ospf 3 process</pre>
Supported Releases	10.3.0E or later

clear ipv6 ospf statistics

Clears OSPFv3 traffic statistics.

Syntax	<code>clear ipv6 ospf [<i>instance-number</i>] statistics</code>
Parameters	<i>instance-number</i> — (Optional) Enter an OSPFv3 instance number (1 to 65535).
Default	Not configured
Command Mode	EXEC
Usage Information	This command clears the OSPFv3 traffic statistics in a specified instance or in all the configured OSPFv3 instances, and resets them to zero.
Example	<pre>OS10# clear ipv6 ospf 100 statistics</pre>
Supported Releases	10.4.0E(R1) or later

default-information originate

Generates and distributes a default external route information to the OSPFv3 routing domain.

Syntax	<code>default-information originate [always]</code>
Parameters	<i>always</i> — (Optional) Always advertise the default route.
Defaults	Disabled
Command Mode	ROUTER-OSPFv3
Usage Information	The <code>no</code> version of this command disables the distribution of default route.
Example	<pre>OS10(config)# router ospfv3 100 OS10(config-router-ospfv3-100)# default-information originate always</pre>
Supported Releases	10.3.0E or later

ipv6 ospf area

Attaches an interface to an OSPF area.

Syntax	<code>ipv6 ospf <i>process-id</i> area <i>area-id</i></code>
Parameters	<ul style="list-style-type: none">• <i>process-id</i>—Enter an OSPFv3 process ID for a specific OSPFv3 process (1 to 65535).• <i>area-id</i>—Enter the OSPFv3 area ID in dotted decimal format (A.B.C.D) or enter an area ID number (1 to 65535).
Default	Not configured
Command Mode	INTERFACE
Usage Information	The <code>no</code> version of this command removes an interface from an OSPFv3 area.
Example	<pre>OS10(config)# interface vlan 10 OS10(config-if-vl-10)# ipv6 ospf 10 area 1</pre>
Supported Releases	10.3.0E or later

ipv6 ospf authentication

Configures OSPFv3 authentication on an IPv6 interface.

Syntax `ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1} key}`

- Parameters**
- `null` — Prevents area authentication from being inherited on the interface.
 - `ipsec spi number` — Enter a unique security policy index number (256 to 4294967295).
 - `md5` — Enable MD5 authentication.
 - `sha1` — Enable SHA-1 authentication.
 - `key` — Enter the text string used by the authentication type.

Default IPv6 OSPF authentication is not configured on an interface.

Command Mode INTERFACE

- Usage Information**
- Before you enable IPsec authentication on an OSPFv3 interface, you must enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign it to an area.
 - The SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. You cannot configure the same SPI value on another interface even if it uses the same authentication or encryption algorithm.
 - You cannot use an IPsec authentication type (MD5 or SHA-1) and the `null` setting at same time on an interface. These settings are mutually exclusive.
 - All neighboring OSPFv3 routers must share the key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.

Example

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ipv6 ospf authentication ipsec spi 400 md5
12345678123456781234567812345678
```

Supported Releases 10.4.0E(R1) or later

ipv6 ospf cost

Changes the cost associated with the OSPFv3 traffic on an interface

Syntax `ipv6 ospf cost cost`

Parameters `cost` — Enter a value as the OSPFv3 cost for the interface (1 to 65335).

Default Based on bandwidth reference

Command Mode INTERFACE

Usage Information If not configured, the interface cost is based on the `auto-cost` command. This command configures OSPFv3 over multiple vendors to ensure that all routers use the same cost value. The `no` version of this command removes the IPv6 OSPF cost configuration.

Example

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# ipv6 ospf cost 10
```

Supported Releases 10.3.0E or later

ipv6 ospf dead-interval

Sets the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

Syntax `ipv6 ospf dead-interval seconds`

Parameters	<i>seconds</i> — Enter the dead interval value in seconds (1 to 65535).
Default	40 seconds
Command Mode	INTERFACE
Usage Information	The dead interval is four times the default hello-interval by default. The <i>no</i> version of this command removes the IPv6 OSPF dead-interval configuration.
Example	<pre>OS10(config)# interface vlan 10 OS10(conf-if-vl-10)# ipv6 ospf dead-interval 10</pre>
Supported Releases	10.3.0E or later

ipv6 ospf encryption

Configures OSPFv3 encryption on an IPv6 interface.

Syntax	<code>ipv6 ospf encryption {ipsec spi number esp encryption-type key authentication-type key null}</code>
Parameters	<ul style="list-style-type: none"> • <i>ipsec spi number</i> — Enter a unique security policy index number (256 to 4294967295). • <i>esp encryption-type</i> — Enter the encryption algorithm used with ESP (3DES, DES, AES-CBC, or NULL). For AES-CBC, only the AES-128 and AES-192 ciphers are supported. • <i>key</i> — Enter the text string used in the encryption algorithm. • <i>authentication-type</i> — Enter the encryption authentication algorithm to use (MD5 or SHA1). • <i>key</i> — Enter the text string used in the authentication algorithm. • <i>null</i> — Enter the keyword to not use the IPsec encryption.
Default	IPv6 OSPF encryption is not configured on an interface.
Command Mode	INTERFACE
Usage Information	<ul style="list-style-type: none"> • Before you enable IPsec authentication on an OSPFv3 interface, you must enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign it to an area. • When you configure encryption on an interface, both IPsec encryption and authentication are enabled. You cannot configure encryption if you have already configured an interface for IPsec authentication (<code>ipv6 ospf authentication ipsec</code>). To configure encryption, you must first delete the authentication policy. • All neighboring OSPFv3 routers must share the same encryption key to decrypt information. Only a non-encrypted key is supported. Required lengths of the non-encrypted key are: 3DES — 48 hex digits; DES — 16 hex digits; AES-CBC — 32 hex digits for AES-128 and 48 hex digits for AES-192. • All neighboring OSPFv3 routers must share the same authentication key to exchange information. Only a non-encrypted key is supported. For MD5 authentication, the non-encrypted key must be 32 plain hex digits. For SHA-1 authentication, the non-encrypted key must be 40 hex digits. An encrypted key is not supported.
Example	<pre>OS10(config)# interface ethernet 1/1/6 OS10(conf-if-eth1/1/6)# ipv6 ospf encryption ipsec spi 500 esp des 1234567812345678 md5 1234567812345678123456781234567812345678</pre> <pre>OS10(config)# interface ethernet 1/1/5 OS10(conf-if-eth1/1/5)# ipv6 ospf encryption null</pre>
Supported Releases	10.4.0E(R1) or later

ipv6 ospf hello-interval

Sets the time interval between hello packets sent on an interface.

Syntax	<code>ipv6 ospf hello-interval <i>seconds</i></code>
Parameters	<i>seconds</i> — Enter the hello-interval value in seconds (1 to 65535).
Default	10 seconds
Command Mode	INTERFACE
Usage Information	All routers in a network must have the same hello time interval between the hello packets. The <code>no</code> version of the this command resets the value to the default.
Example	<pre>OS10(config)# interface vlan 10 OS10(conf-if-vl-10)# ipv6 ospf hello-interval 30</pre>
Supported Releases	10.3.0E or later

ipv6 ospf network

Sets the network type for the interface.

Syntax	<code>ipv6 ospf network {point-to-point broadcast}</code>
Parameters	<ul style="list-style-type: none">• <code>point-to-point</code> — Sets the interface as part of a point-to-point network.• <code>broadcast</code> — Sets the interface as part of a broadcast network.
Default	Broadcast
Command Mode	INTERFACE
Usage Information	The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# ipv6 ospf network broadcast</pre>
Supported Releases	10.3.0E or later

ipv6 ospf passive

Configures an interface as a passive interface and suppresses routing updates (both receiving and sending) to the passive interface.

Syntax	<code>ipv6 ospf passive</code>
Parameters	None
Default	Not configured
Command Mode	INTERFACE
Usage Information	You must configure the interface before setting the interface to passive mode. The <code>no</code> version of the this command disables the Passive interface configuration.
Example	<pre>OS10(config)# interface ethernet 1/1/6 OS10(conf-if-eth1/1/6)# ipv6 ospf passive</pre>
Supported Releases	10.3.0E or later

ipv6 ospf priority

Sets the priority of the interface to determine the designated router for the OSPFv3 network.

Syntax	<code>ipv6 ospf priority number</code>
Parameters	<i>number</i> — Enter a router priority number (0 to 255).
Default	1
Command Mode	INTERFACE
Usage Information	When two routers attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# interface ethernet 1/1/6 OS10(config-if-eth1/1/6)# ipv6 ospf priority 4</pre>
Supported Releases	10.3.0E or later

log-adjacency-changes

Enables logging of syslog messages about changes in the OSPFv3 adjacency state.

Syntax	<code>log-adjacency-changes</code>
Parameters	None
Default	Disabled
Command Mode	ROUTER-OSPFv3
Usage Information	The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# router ospfv3 100 OS10(config-router-ospfv3-100)# log-adjacency-changes</pre>
Supported Releases	10.3.0E or later

maximum-paths

Enables forwarding of packets over multiple paths.

Syntax	<code>maximum-paths number</code>
Parameters	<i>number</i> — Enter the number of paths for OSPFv3 (1 to 128).
Default	Disabled
Command Mode	ROUTER-OSPFv3
Usage Information	The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# router ospfv3 OS10(config-router-ospfv3-100)# maximum-paths 1</pre>
Supported Releases	10.3.0E or later

redistribute

Redistributes information from another routing protocol or routing instance to the OSPFv3 process.

Syntax	<code>redistribute {bgp <i>as-number</i> connected static} [route-map <i>route-map name</i>]</code>
Parameters	<ul style="list-style-type: none">• <i>as-number</i> — Enter an autonomous number to redistribute BGP routing information throughout the OSPFv3 instance (1 to 4294967295).• <i>route-map name</i> — Enter the name of a configured route-map.• <i>connected</i> — Enter the information from connected (active) routes on interfaces to redistribute.• <i>static</i> — Enter the information from static routes on interfaces redistribute.
Defaults	Not configured
Command Mode	ROUTER-OSPFv3
Usage Information	When an OSPFv3 redistributes, the process is not completely removed from the BGP configuration. The <code>no</code> version of this command disables the redistribute configuration.
Example	<pre>OS10(config)# router ospfv3 100 OS10(config-router-ospfv3-100)# redistribute bgp 4 route-map dell1</pre>
Example (Connected)	<pre>OS10((config-router-ospfv3-100)# redistribute connected route-map dell2</pre>
Supported Releases	10.3.0E or later

router-id

Configures a fixed router ID for the OSPFv3 process.

Syntax	<code>router-id <i>ip-address</i></code>
Parameters	<i>ip-address</i> — Enter the IP address of the router as the router ID.
Default	Not configured
Command Mode	ROUTER-OSPFv3
Usage Information	Configure an arbitrary value in the IP address format for each router. Each router ID must be unique. Use the fixed router ID for the active OSPFv3 router process. Changing the router ID brings down the existing OSPFv3 adjacency. The new router ID becomes effective immediately. The <code>no</code> version of this command disables the router ID configuration.
Example	<pre>OS10(config)# router ospfv3 10 OS10(config-router-ospfv3-100)# router-id 10.10.1.5</pre>
Supported Releases	10.3.0E or later

router ospfv3

Enters Router OSPFv3 mode and configures an OSPFv3 instance.

Syntax	<code>router ospfv3 <i>instance-number</i></code>
Parameters	<i>instance-number</i> —Enter a router OSPFv3 instance number, from 1 to 65535.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes an OSPFv3 instance.

Example

```
OS10(config)# router ospfv3 10
```

Supported Releases

10.3.0E or later

show ipv6 ospf

Displays OSPFv3 instance configuration information.

Syntax

```
show ipv6 ospf [instance-number]
```

Parameters

instance-number — (Optional) View OSPFv3 information for a specified instance number (1 to 65535)

Default

None

Command Mode

EXEC

Usage

None

Information**Example**

```
OS10# show ipv6 ospf
Routing Process ospfv3 200 with ID 1.1.1.1
It is an Area Border Router
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 2, normal 2 stub 0 nssa
  Area (0.0.0.0)
    Number of interface in this area is 1
    SPF algorithm executed 42 times
  Area (0.0.0.1)
    Number of interface in this area is 1
    SPF algorithm executed 42 times
OS10# show ipv6 ospf 200
Routing Process ospfv3 200 with ID 10.0.0.2
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 1, normal 1 stub 0 nssa
  Area (0.0.0.0)
    Number of interface in this area is 1
    SPF algorithm executed 3 times
```

Supported Releases

10.3.0E or later

show ipv6 ospf database

Displays all LSA information. You must enable OSPFv3 to generate output.

Syntax

```
show ipv6 ospf process-id database
```

Parameters

process-id — Enter the OSPFv3 process ID to view a specific process. If you do not enter a process ID, the command applies to all the configured OSPFv3 processes.

Default

Not configured

Command Mode

EXEC

Usage**Information**

- **Link ID**—Identifies the router ID.
- **ADV Router**—Identifies the advertising router's ID.
- **Age**—Displays the link state age.
- **Seq#**—Identifies the link state sequence number (identifies old or duplicate LSAs).
- **Checksum**—Displays the Fletcher checksum of an LSA's complete contents.
- **Link count**—Displays the number of interfaces for that router.
- **Rtr Count**—Displays the router count.

- **Dest RtrID**—Displays the destination router ID.
- **Interface**—Displays the interface type.
- **Prefix**—Displays the prefix details.

Example

```
OS10# show ipv6 ospf database
      OSPF Router with ID (10.0.0.2) (Process ID 200)
Router Link States (Area 0.0.0.0)
ADV Router      Age      Seq#          Fragment ID Link count Bits
-----
1.1.1.1         1610    0x80000144   0           1           B
2.2.2.2         1040    0x8000013A   0           1
10.0.0.2        1039    0x80000002   0           1
Net Link States (Area 0.0.0.0)
ADV Router      Age      Seq#          Link ID    Rtr count
-----
2.2.2.2         1045    0x80000001   5           2
Inter Area Router States (Area 0.0.0.0)
ADV Router      Age      Seq#          Link ID    Dest RtrID
-----
1.1.1.1         1605    0x80000027   1           3.3.3.3
Link (Type-8) Link States (Area 0.0.0.0)
ADV Router      Age      Seq#          Link ID    Interface
-----
1.1.1.1         1615    0x80000125   5           ethernet1/1/1
2.2.2.2         1369    0x8000011B   5           ethernet1/1/1
10.0.0.2        1044    0x80000001   5           ethernet1/1/1
Type-5 AS External Link States
ADV Router      Age      Seq#          Prefix
-----
3.3.3.3         3116    0x80000126   400::/64
3.3.3.3         3116    0x80000124   34::/64
```

Supported Releases

10.3.0E or later

show ipv6 ospf interface

Displays the configured OSPFv3 interfaces. You must enable OSPFv3 to display the output.

Syntax `show ipv6 ospf interface interface`

Parameters *interface* — (Optional) Enter the interface information:

- **ethernet** — Physical interface (1 to 48)
- **port-channel** — Port-channel interface (1 to 128).
- **vlan** — VLAN interface 1 to 4093).

Default Not configured

Command Mode EXEC

Example

```
OS10# show ipv6 ospf interface
ethernet1/1/1 is up, line protocol is up
  Link Local Address fe80::20c:29ff:fe0a:d59/64, Interface ID 5
  Area 0.0.0.0, Process ID 200, Instance ID 0, Router ID 10.0.0.2
  Network Type broadcast, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router on this network is 2.2.2.2
  Backup Designated router on this network is 10.0.0.2 (local)
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2(Designated Router)
```

Supported Releases

10.3.0E or later

show ipv6 ospf neighbor

Displays a list of OSPFv3 neighbors connected to the local router.

Syntax show ipv6 ospf neighbor

Parameters None

Default Not configured

Command Mode EXEC

Usage Information

- Neighbor ID—Displays the neighbor router ID.
- Pri—Displays the priority assigned neighbor.
- State—Displays the OSPF state of the neighbor.
- Dead Time—Displays the expected time until the system declares the neighbor dead.
- Interface ID—Displays the neighbor interface ID
- Interface—Displays the interface type, node/slot/port or number information.

Example

```
OS10(conf-if-eth1/1/1)# show ipv6 ospf neighbor
Neighbor ID   Pri   State   Dead Time   Interface ID   Interface
-----
2.2.2.2       1     Full/DR  00:00:30    5              ethernet1/1/1
```

Supported Releases 10.3.0E or later

show ipv6 ospf statistics

Displays OSPFv3 traffic statistics.

Syntax show ipv6 ospf [*instance-number*] statistics [*interface interface*]

Parameters

- *instance-number* — (Optional) Enter an OSPFv3 instance number (1 to 65535).
- *interface interface* — (Optional) Enter the interface information:
 - ethernet *node/slot/port[:subport]* — Enter an Ethernet port interface.
 - port-channel *number* — Enter the port-channel interface number (1 to 128).
 - vlan *vlan-id* — Enter the VLAN ID number (1 to 4093).

Default Not configured

Command Mode EXEC

Usage Information This command displays OSPFv3 traffic statistics for a specified instance or interface, or for all OSPFv3 instances and interfaces.

Example

```
OS10# show ipv6 ospf interface ethernet 1/1/1

Interface ethernet1/1/1
Receive Statistics
  rx-invalid 0 rx-invalid-bytes 0
  rx-hello 0 rx-hello-bytes 0
  rx-db-des 0 rx-db-des-bytes 0
  rx-ls-req 0 rx-ls-req-bytes 0
  rx-ls-upd 0 rx-ls-upd-bytes 0
  rx-ls-ack 0 rx-ls-ack-bytes 0
Transmit Statistics
  tx-hello 1054 tx-hello-bytes 37944
  tx-db-des 0 tx-db-des-bytes 0
  tx-ls-req 0 tx-ls-req-bytes 0
  tx-ls-upd 0 tx-ls-upd-bytes 0
  tx-ls-ack 0 tx-ls-ack-bytes 0
Error packets (Receive statistics)
  bad-src 0 dupe-id 0 hello-err 0
  mtu-mismatch 0 nbr-ignored 0
  resource-err 0 bad-lsa-len 0 lsa-bad-type 0
```

```
lsa-bad-len 0 lsa-bad-cksum 0
hello-tmr-mismatch 0 dead-ivl-mismatch 0
options-mismatch 0 nbr-admin-down 0 own-hello-drop 0
self-orig 0 wrong-length 0
version-mismatch 0 area-mismatch 0
```

Supported Releases 10.4.0E(R1) or later

timers spf (OSPFv3)

Enables shortest path first (SPF) throttling to delay an SPF calculation when a topology change occurs.

Syntax `timers spf [start-time [hold-time [max-wait]]]`

Parameters

- *start-time* — Sets the initial SPF delay in milliseconds (1 to 600000; default 1000).
- *hold-time* — Sets the additional hold time between two SPF calculations in milliseconds (1 to 600000; default 10000).
- *max-wait* — Sets the maximum wait time between two SPF calculations in milliseconds (1 to 600000; default 10000).

Default

- *start-time* — 1000 milliseconds
- *hold-time* — 10000 milliseconds
- *max-wait* — 10000 milliseconds

Command Mode ROUTER-OSPFv3

Usage Information OSPFv2 and OSPFv3 support SPF throttling. By default, SPF timers are disabled in an OSPF instance.

Use SPF throttling to delay SPF calculations during periods of network instability. In an OSPF network, a topology change event triggers an SPF calculation after a specified start time. When the start timer finishes, a hold time may delay the next SPF calculation for an additional time. When the hold timer is running:

- Each time a topology change occurs, the SPF calculation is delayed for double the configured hold time up to maximum wait time.
- If no topology change occurs, an SPF calculation is performed and the hold timer is reset to its configured value.

If you do not specify a start-time, hold-time or max-wait value, the default values are used. The `no` version of this command removes the configured SPF timers and disables SPF throttling in an OSPF instance.

Example

```
OS10(config)# router ospfv3 100
OS10(config-router-ospfv3-100)# timers spf 1345 2324 9234

OS10(config-router-ospfv3-100)# do show ipv6 ospf
Routing Process ospfv3 100 with ID 129.240.244.107
SPF schedule delay 1345 msecs, Hold time between two SPFs 2324 msecs
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 1, normal 1 stub 0 nssa
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 2 times
```

Supported Releases 10.4.0E(R1) or later

Object tracking manager

Object tracking manager (OTM) allows you to track the link status of Layer 2 interfaces, and the reachability of IP and IPv6 hosts. You can increase the availability of the network and shorten recovery time if an object state goes Down.

Object tracking monitors the status of tracked objects and communicates any changes made to interested client applications. OTM client applications are VRRP and PBR. Each tracked object has a unique identifying number that clients use to configure the action to take when a tracked object changes state. You can also optionally specify a time delay before changes in a tracked object's state are reported to a client application.

VRRP can subscribe to a track object which tracks the interface line protocol state. It can use the tracked object status to determine the priority of the VRRP router in a VRRP group. If a tracked state, or interface goes down, VRRP updates the priority based on what you configure the new priority to be for the tracked state. When the tracked state comes up, VRRP restores the original priority for the virtual router group.

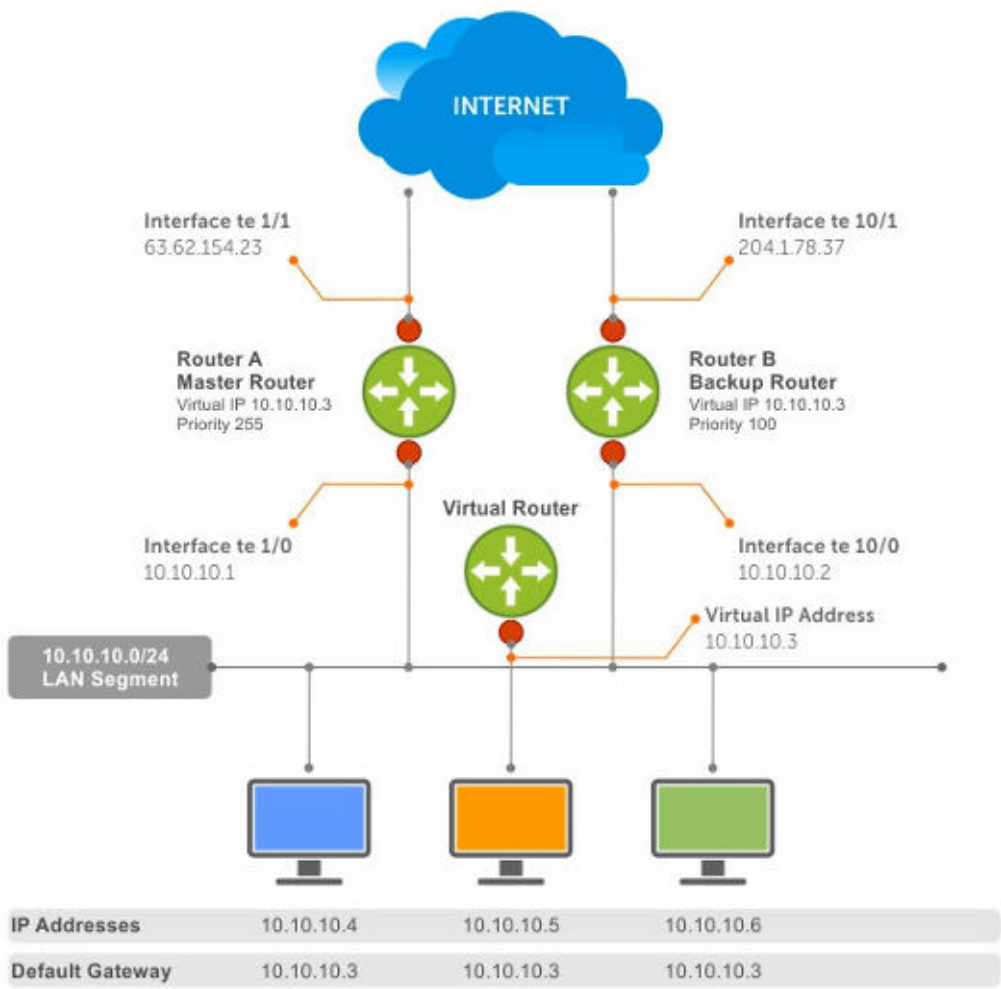


Figure 4. Object tracking

Interface tracking

You can create an object that tracks the line-protocol state of a Layer 2 interface, and monitors its operational status (Up or Down). You can configure up to 500 objects. Each object is assigned a unique ID. The `no` version of this command deletes the tracked object from an interface.

When the link-level status goes down, the tracked resource status is also considered Down. If the link-level status goes up, the tracked resource status is also considered Up. For logical interfaces (port-channels or VLANs), the link-protocol status is considered to be Up if any physical interface under the logical interface is Up.

The list of available interfaces include:

- `ethernet` — Physical interface
- `port-channel` — Port-channel identifier

- VLAN — VLAN identifier
- Loopback — Loopback interface identifier
- mgmt — Management interface

1. Configure object tracking in CONFIGURATION mode from 1 to 500.

```
track object-id
```

2. (Optional) Enter the interface object tracking on the line-protocol state of a Layer 2 interface in OBJECT TRACKING mode.

```
interface interface line-protocol
```

3. (Optional) Configure the time delay used before communicating a change to the status of a tracked interface in OBJECT TRACKING mode from 0 to 80 seconds; default 0.

```
delay [up seconds] [down seconds]
```

4. (Optional) View the tracked object information in EXEC mode.

```
show track object-id
```

5. (Optional) View all interface object information in EXEC mode.

```
show track interface
```

6. (Optional) View all IPv4 or IPv6 next-hop object information in EXEC mode.

```
show track [ip | ipv6]
```

7. (Optional) View brief status of object information in EXEC mode.

```
show track brief
```

Configure object tracking

```
OS10(config)# track 1
OS10(conf-track-1)# interface ethernet 1/1/1 line-protocol
OS10(conf-track-1)# delay up 20
OS10(conf-track-1)# delay down 10
OS10(conf-track-1)# do show track 1
Interface ethernet1/1/1 line-protocol
Line protocol is UP
1 changes, Last change 2017-04-26T06:41:36Z
```

Host tracking

If you configure an IP host as a tracked object, the entry or the next-hop address in the ARP cache determines the Up or Down state of the route.

A tracked host is reachable if there is an ARP cache entry for the router's next-hop address. An attempt to regenerate the ARP cache entry occurs if the next-hop address appears before considering the route Down.

1. Configure object tracking in CONFIGURATION mode.

```
track object-id
```

2. Enter the host IP address for reachability of an IPv4 or IPv6 route in OBJECT TRACKING mode.

```
[ip | ipv6] host-ip-address reachability
```

3. Configure the time delay used before communicating a change in the status of a tracked route in OBJECT TRACKING mode.

```
delay [up seconds] [down seconds]
```

4. Track the host by checking the reachability periodically in OBJECT TRACKING mode.

```
reachability-refresh interval
```

5. View the tracking configuration and the tracked object status in EXEC mode.

```
show track object-id
```

Configure IPv4 host tracking

```
OS10 (conf-track-1)# track 2
OS10 (conf-track-2)# ip 1.1.1.1 reachability
OS10 (conf-track-2)# do show track 2
IP Host 1.1.1.1 reachability
Reachability is DOWN
1 changes, Last change 2017-04-26T06:45:31Z
OS10 (conf-track-2)#
```

Configure IPv6 host tracking

```
OS10 (conf-track-2)# track 3
OS10 (conf-track-3)# ipv6 20::20 reachability
OS10 (conf-track-3)# delay up 20
OS10 (conf-track-3)# do show track 3
IP Host 20::20 reachability
Reachability is DOWN
1 changes, Last change 2017-04-26T06:47:04Z
OS10 (conf-track-3)#
```

Set tracking delays

You can configure an optional Up and/or Down timer for each tracked object. The timer allows you to set the time delay before a change in the state of a tracked object is communicated to clients. The time delay starts when the state changes from Up to Down or from Down to Up.

If the state of an object changes back to its former Up or Down state before the timer expires, the timer is canceled without notifying the client. If the timer expires and an object's state has changed, a notification is sent to the client. For example, if the Down timer is running and an interface goes down then comes back up, the Down timer is canceled. The client is not notified of the event.

If you do not configure a delay, a notification is sent when a change in the state of a tracked object is detected. The time delay in communicating a state change is specified in seconds.

Object tracking

As a client, VRRP can track up to 20 interface objects plus 12 tracked interfaces supported for each VRRP group. You can assign a unique priority-cost value from 1 to 254 to each tracked VRRP object or group interface.

The priority cost is subtracted from the VRRP group priority if a tracked VRRP object is in a Down state. If a VRRP group router acts as owner-master, the run-time VRRP group priority remains fixed at 255. Changes in the state of a tracked object have no effect.

In VRRP object tracking, the sum of the priority costs for all tracked objects and interfaces cannot equal or exceed the priority of the VRRP group.

View tracked objects

You can view the status of currently tracked Layer 2 or Layer 3 interfaces, or the IPv4 or IPv6 hosts.

View brief object tracking information

```
OS10# show track brief
TrackID  Resource                Parameter                Status    LastChange
-----
1        line-protocol            ethernet1/1/1           DOWN
2017-02-03T08:41:25Z
2        ipv4-reachablity        1.1.1.1                 DOWN
```

```
2017-02-03T08:41:43Z1
3          ipv6-reachablity      10::10          DOWN          2017-02-03T08:41:55Z1
```

View all object tracking information

```
OS10# show track
```

View interface object tracking information

```
OS10# show track interface
TrackID  Resource                Parameter          Status    LastChange
-----
1        line-protocol            ethernet1/1/1     DOWN
2017-02-03T08:41:25Z1
OS10# show track ip
TrackID  Resource                Parameter          Status    LastChange
-----
2        ipv4-reachablity        1.1.1.1          DOWN
2017-02-03T08:41:43Z1
OS10# show track ipv6
TrackID  Resource                Parameter          Status    LastChange
-----
3        ipv6-reachablity        10::10          DOWN
2017-02-03T08:41:55Z1
```

View IPv4 next-hop object tracking

```
OS10# show track ip
```

View IPv6 next-hop object tracking

```
OS10# show track ipv6
```

View running configuration

```
OS10# show running-configuration
```

OTM commands

delay

Configures the delay timers.

Syntax	<code>delay {up down} seconds</code>
Parameters	<code>seconds</code> — Enter the delay time in seconds (up to 180).
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(conf-track-100)# delay up 200 down 100</pre>
Supported Releases	10.3.0E or later

interface line-protocol

Configures an object to track a specific interface's line-protocol status.

Syntax	<code>interface <i>interface</i> line-protocol</code>
Parameters	<i>interface</i> — Enter the interface information: <ul style="list-style-type: none">• <code>ethernet</code> — Physical interface.• <code>port-channel</code> — Enter the port-channel identifier.• <code>vlan</code> — Enter the VLAN identifier.• <code>loopback</code> — Enter the Loopback interface identifier.• <code>mgmt</code> — Enter the Management interface.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(conf-track-100)# interface ethernet line-protocol</pre>
Supported Releases	10.3.0E or later

ip reachability

Configures an object to track a specific next-hop host's reachability.

Syntax	<code>ip <i>host-ip-address</i> reachability</code>
Parameters	<i>host-ip-address</i> — Enter the IPv4 host address.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(config)# track 100 OS10(conf-track-100)# ip 10.10.10.1 reachability</pre>
Supported Releases	10.3.0E or later

ipv6 reachability

Configures an object to track a specific next-hop host's reachability.

Syntax	<code>ipv6 <i>host-ip-address</i> reachability</code>
Parameters	<i>host-ip-address</i> — Enter the IPv6 host address.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(config)# track 200 OS10(conf-track-200)# ipv6 10::1 reachability</pre>

Supported Releases 10.3.0E or later

reachability-refresh

Configures a polling interval for reachability tracking.

Syntax `reachability-refresh interval`

Parameters `interval` — Enter the polling interval value (up to 3600 seconds).

Defaults 0 seconds

Command Mode CONFIGURATION

Usage Information Set the interval to 0 to disable the refresh.

Example

```
OS10(conf-track-100)# reachability-refresh 600
```

Supported Releases 10.3.0E or later

show track

Displays tracked object information.

Syntax `show track [brief] [object-id] [interface] [ip | ipv6]`

Parameters

- `brief` — (Optional) Displays brief tracked object information.
- `object-id` — (Optional) Displays the tracked object information for a specific object ID.
- `interface` — (Optional) Displays all interface object information.
- `ip` — (Optional) Displays all IPv4 next-hop object information.
- `ipv6` — (Optional) Displays all IPv6 next-hop object information.

Defaults None

Command Mode CONFIGURATION

Usage Information None

Example (Brief)

```
OS10# show track brief
TrackID Resource Parameter Status LastChange
-----
1 line-protocol ethernet1/1/1 DOWN
2017-02-03T08:41:25Z1
2 ipv4-reachablity 1.1.1.1 DOWN
2017-02-03T08:41:43Z1
3 ipv6-reachablity 10::10 DOWN 2017-02-03T08:41:55Z1
```

Supported Releases 10.3.0E or later

track

Configures and manages tracked objects.

Syntax `track object-id`

Parameters `object-id` — Enter the object ID to track (up to 500).

Defaults Not configured

Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command deletes the tracked object from an interface.
Example	<pre>OS10# track 100</pre>
Supported Releases	10.3.0E or later

Policy-based routing

Policy-based routing (PBR) provides a mechanism to redirect IPv4 and IPv6 data packets based on the policies defined to override the switch's forwarding decisions based on the routing table.

Policy-based route-maps

A route-map is an ordered set of rules that control the redistribution of IP routes into a protocol domain. When you enable PBR on an interface, all IPv4 or IPv6 data packets received are processed based on the policies that you define in the route-maps. The rules defined in the route-maps are based on access control lists (ACLs) and next-hop addresses, and only apply to ACLs used in policy-based routing.

You can create a route-map that specifies the match criteria and the resulting action if all the match clauses are met. After you create the route-map, you can enable PBR for that route-map on a specific interface. Route-maps contain `match` and `set` statements that you can mark as *permit*.

Access-list to match route-map

You can assign an IPv4 or IPv6 access-list to match a route-map.

The IP access list contains the criteria to match the traffic content based on the header field, such as destination IP or source IP.

When `permit` or `deny` is present in the `access-list`, it is omitted and the action present in the `route-map` command is used for policy-based routing. `permit` in the route-map statement indicates policy-based routing, as where `deny` in the route-map statement indicates a switch-based forwarding decision—PBR exception. Access-list is used only for the packet match criteria in policy-based routing.

1. Assign an access-list to match the route-map in CONFIGURATION mode.

```
ip access-list access-list-name
```

2. Set the IP address to match the access-list in IP-ACL mode.

```
permit ip ip-address
```

Configure IPv4 access-list to match route-map

```
OS10(config)# ip access-list acl5
OS10(conf-ipv4-acl)# permit ip 10.10.10.0/24 any
```

Configure IPv6 access-list to match route-map

```
OS10(config)# ipv6 access-list acl8
OS10(conf-ipv6-acl)# permit ipv6 10::10 any
```

Set address to match route-map

You can set an IPv4 or IPv6 address to match a route-map.

1. Enter the IPv4 or IPv6 address to match and specify the access-list name in Route-Map mode.

```
match {ip | ipv6} address access-list-name
```

2. Set the next-hop IP address in Route-Map mode.

```
set {ip | ipv6} next-hop ip-address
```

Apply match parameters to IPv4 route-map

```
OS10(conf-route-map)# route-map map1  
OS10(conf-route-map)# match ip address acl5
```

Apply match and set parameters to IPv6 route-map

```
OS10(conf-route-map)# route-map map1  
OS10(conf-route-map)# match ipv6 address acl8  
OS10(conf-route-map)# set ipv6 next-hop 20::20
```

Assign route-map to interface

You can assign a route-map to an interface for IPv4 or IPv6 policy-based routing to an interface.

- Assign the IPv4 or IPv6 policy-based route-map to an interface in INTERFACE mode.

```
{ip | ipv6} policy route-map map-name
```

Assign route-map to an IPv4 interface

```
OS10(config)# interface ethernet 1/1/5  
OS10(conf-if-eth1/1/5)# ip policy route-map map1
```

Assign route-map to an IPv6 interface

```
OS10(conf-if-eth1/1/5)# ipv6 policy route-map map2
```

View PBR information

Display PBR information to verify IPv4 or IPv6 configuration and view statistics.

1. View IPv4 or IPv6 PBR policy information in EXEC mode.

```
show {ip | ipv6} policy name
```

2. View the current PBR statistics in EXEC mode.

```
show route-map map-name pbr-statistics
```

3. Clear all policy statistics information in EXEC mode.

```
clear route-map map-name pbr-statistics
```

Verify IPv4 PBR configuration

```
OS10# show ip policy abc  
Interface      Route-map  
-----  
ethernet1/1/1  abc  
ethernet1/1/3  abc  
vlan100        abc
```

Verify IPv6 PBR configuration

```
OS10# show ipv6 policy abc
Interface      Route-map
-----
ethernet1/1/1  abc
ethernet1/1/3  abc
vlan100        abc

show route-map pbr-sample pbr-statistics
route-map pbr-sample, permit, sequence 10

Policy routing matches: 84 packets
```

PBR commands

clear route-map pbr-statistics

Clears all PBR counters.

Syntax	<code>clear route-map [map-name] pbr-statistics</code>
Parameters	<i>map-name</i> —Enter the name of a configured route-map (up to 140 characters).
Defaults	None
Command Mode	EXEC
Usage Information	Use the <code>clear route-map pbr-statistics</code> command to clear all PBR counters.
Example	<pre>OS10# clear route-map map1 pbr-statistics</pre>
Supported Releases	10.3.0E or later

match address

Matches the access-list to the route-map.

Syntax	<code>match {ip ipv6} address [name]</code>
Parameters	<i>name</i> —Enter the name of an access-list (up to 140 characters).
Defaults	Not configured
Command Mode	ROUTE-MAP
Usage Information	None
Example	<pre>OS10(conf-route-map)# match ip address acl1</pre>
Supported Releases	10.3.0E or later

policy route-map

Assigns a route-map for IPv4 or IPv6 policy-based routing to the interface.

Syntax	<code>{ip ipv6} policy route-map [map-name]</code>
Parameters	<i>map-name</i> —Enter the name of a configured route-map (up to 140 characters).

Defaults Not configured

Command Mode INTERFACE

Usage Information None

Example

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip policy route-map map1
```

Supported Releases 10.3.0E or later

route-map pbr-statistics

Enables counters for PBR statistics.

Syntax `route-map [map-name] pbr-statistics`

Parameters `map-name`—Enter the name of a configured route-map (up to 140 characters).

Defaults Not configured

Command Mode CONFIGURATION

Usage Information None

Example

```
OS10(config)# route-map map1 pbr-statistics
```

Supported Releases 10.3.0E or later

set next-hop

Sets an IPv4 or IPv6 next-hop address for policy-based routing.

Syntax `set {ip | ipv6} next-hop address`

Parameters `address` — Enter the next-hop IPv4 or IPv6 address.

Defaults Not configured

Command Mode ROUTE-MAP

Usage Information None

Example

```
OS10(conf-route-map)# set ip next-hop 10.10.10.10
```

Supported Releases 10.3.0E or later

set next-hop track

Sets the next-hop IPv4 or IPv6 address to track the PBR object.

Syntax `set {ip | ipv6} next-hop address track track-id`

Parameters

- `address`—Enter an IPv4 or IPv6 address.
- `track-id`—(Optional) Enter the track ID of the PBR object.

Defaults Not configured

Command Mode ROUTE-MAP

Usage Information None

Example

```
OS10(conf-route-map)# set ip next-hop 10.10.10.10 track-id 12
```

Supported Releases 10.3.0E or later

show policy

Displays policy information.

Syntax show {ip | ipv6} policy [map-name]

Parameters map-name — (Optional) Enter the name of a configured route map (up to 140 characters).

Defaults None

Command Mode EXEC

Usage Information None

Example

```
OS10# show ip policy map-name
```

Supported Releases 10.3.0E or later

show route-map pbr-statistics

Displays the current PBR statistics.

Syntax show route-map [map-name] pbr-statistics

Parameters map-name — (Optional) Enter the name of a configured route map (up to 140 characters).

Defaults None

Command Mode EXEC

Usage Information None

Example

```
OS10# show route-map map1 pbr-statistics
```

Supported Releases 10.3.0E or later

Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) allows you to form virtual routers from groups of physical routers on your LAN. These virtual routing platforms — master and backup pairs — provide redundancy in case of hardware failure. VRRP also allows you to easily configure a virtual router as the default gateway to all your hosts and avoids the single point of failure of a physical router.

VRRP advantages in ease of administration and network throughput and reliability:

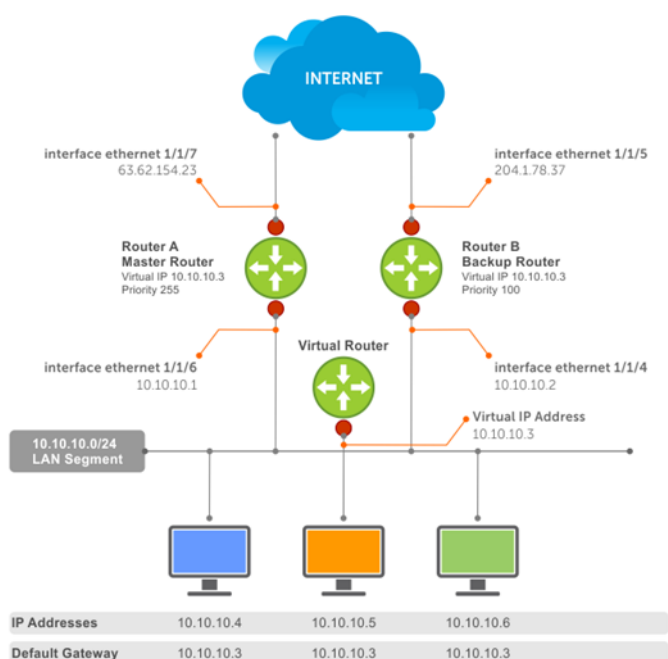
- Provides a virtual default routing platform
- Provides load balancing
- Supports multiple logical IP subnets on a single LAN segment
- Enables simple traffic routing without the single point of failure of a static default route

- Avoids issues with dynamic routing and discovery protocols
- Takes over a failed default router:
 - Within a few seconds
 - With a minimum of VRRP traffic
 - Without any interaction from hosts

Configuration

VRRP specifies a master (active) router that owns the next hop IP and MAC address for end stations on a LAN. The master router is chosen from the virtual routers by an election process and forwards packets sent to the next hop IP address. If the master router fails, VRRP begins the election process to choose a new master router which continues routing traffic.

VRRP packets are transmitted with the virtual router MAC address as the source MAC address. The virtual router MAC address associated with a virtual router is in format: 00:00:5E:00:01:{VRID} for IPv4 and 00:00:5E:00:02:{VRID} for IPv6. The VRID is the virtual router identifier that allows up to 255 IPv4 VRRP routers and 255 IPv6 VRRP routers on a network. The first four octets are unquenchable, the last two octets are 01:{VRID} for IPv4 and 02:{VRID} for IPv6. The final octet changes depending on the VRRP virtual router identifier and allows for up to 255 VRRP routers on a network.



The example shows a typical network configuration using VRRP. Instead of configuring the hosts on network 10.10.10.0 with the IP address of either Router A or Router B as the default router, the default router of all hosts is set to the IP address of the virtual router. When any host on the LAN segment requests Internet access, it sends packets to the IP address of the virtual router.

Router A is configured as the master router with the virtual router IP address and sends any packets addressed to the virtual router to the Internet. Router B is the backup router and is also configured with the virtual router IP address.

If the master router (Router A) becomes unavailable, Router B (backup router) automatically becomes the master router and responds to packets sent to the virtual IP address. All workstations continue to use the IP address of the virtual router to transmit packets destined to the Internet. Router B receives and forwards packets on interface ethernet 1/1/5. Until Router A resumes operation, VRRP allows Router B to provide uninterrupted service to the users on the LAN segment accessing the Internet.

Create virtual router

VRRP uses the VRID to identify each virtual router configured. Before using VRRP, you must configure the interface with the primary IP address and enable it.

- Create a virtual router for the interface with the VRRP identifier in INTERFACE mode (1 to 255).

```
vrrp-group vrrp-id
```

- Delete a VRRP group in INTERFACE mode.

```
no vrrp-group vrrp-id
```

Configure VRRP

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# vrrp-group 254
```

Verify VRRP

```
OS10(conf-eth1/1/5-vrid-254)# do show running-configuration
...
!
interface ethernet 1/1/5
ip address 10.10.10.1/24
!
vrrp-group 254
no shutdown
...
```

Group version

Configure a VRRP version for the system. Define either VRRPv2 — `vrrp version 2` or VRRPv3 — `vrrp version 3`.

- Configure the VRRP version for IPv4 in INTERFACE mode.

```
vrrp version
```

Configure VRRP version 3

```
OS10(config)# vrrp version 3
```

1. Set the switch with the lowest priority to `vrrp version 2`.
2. Set the switch with the highest priority to `vrrp version 3`.
3. Set all switches from `vrrp version 2` to `vrrp version 3`.

Migrate IPv4 group from VRRPv2 to VRRPv3

```
OS10_backup_switch1(config)# vrrp version 2
OS10_backup_switch2(config)# vrrp version 2
```

Set master switch to VRRPv3

```
OS10_master_switch(config)# vrrp version 3
```

Set backup switches to VRRPv3

```
OS10_backup_switch1(config)# vrrp version 3
OS10_backup_switch2(config)# vrrp version 3
```

Virtual IP addresses

Virtual routers contain virtual IP addresses configured for that VRRP group (VRID). A VRRP group does not transmit VRRP packets until you assign the virtual IP address to the VRRP group.

To activate a VRRP group on an interface, configure at least one virtual IP address for a VRRP group. The virtual IP address is the IP address of the virtual router and does not require an IP address mask. You can configure up to 10 virtual IP addresses on a single VRRP group (VRID).

These rules apply to virtual IP addresses:

- The virtual IP addresses must be in the same subnet as the primary or secondary IP addresses configured on the interface. Though a single VRRP group can contain virtual IP addresses belonging to multiple IP subnets configured on the interface, Dell EMC recommends configuring virtual IP addresses belonging to the same IP subnet for any one VRRP group. An interface on which you enable VRRP contains a primary IP address of 50.1.1.1/24 and a secondary IP address of 60.1.1.1/24. The VRRP group (VRID 1) must contain virtual addresses belonging to subnet 50.1.1.0/24 or subnet 60.1.1.0/24.
- If the virtual IP address and the interface's primary/secondary IP address are the same, the priority of the VRRP group is set to 255 by default. The interface then becomes the owner router of the VRRP group and the interface's physical MAC address changes to that of the owner VRRP group's MAC address.
- If you configure multiple VRRP groups on an interface, only one of the VRRP groups can contain the interface primary or secondary IP address.

Configure virtual IP address

Configure the virtual IP address — the primary IP address and the virtual IP addresses must be on the same subnet.

1. Configure a VRRP group in INTERFACE mode (1 to 255).

```
vrrp-group vrrp-id
```

2. Configure virtual IP addresses for this VRRP ID in INTERFACE-VRRP mode (up to 10 IP addresses).

```
virtual-address ip-address1 [...ip-address12]
```

Configure virtual IP address

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip address 10.1.1.1/24
OS10(conf-if-eth1/1/1)# vrrp-group 10
OS10(conf-eth1/1/1-vrid-10)# virtual-address 10.1.1.8
```

Verify virtual IP address

```
OS10# show running-configuration
! Version 10.1.9999P.2281
! Last configuration change at Jul 26 12:01:58 2016
!
aaa authentication system:local
!
interface ethernet1/1/1
 ip address 10.1.1.1/24
 no switchport
 no shutdown
!
 vrrp-group 10
  virtual-address 10.1.1.8
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/3
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/4
 switchport access vlan 1
--more--
```

View VRRP information

When the VRRP process completes initialization, the State field contains either master or backup.

```
OS10# show vrrp brief
Interface      Group    Priority  Preemption  State  Master-addr  Virtual addr(s)
```



```
-----  
ethernet1/1/1 IPv4 10 100 true master 10.1.1.8 10.1.1.8
```

View VRRP group 1

```
OS10# show vrrp 1  
Interface : ethernet1/1/1 IPv4 VRID : 1  
Primary IP Address : 10.1.1.1 State : master-state  
Virtual MAC Address : 00:00:5e:00:01:01  
Version : version-3 Priority : 100  
Preempt : Hold-time :  
Authentication : no-authentication  
Virtual IP address :  
10.1.1.1  
master-transitions : 1 advertise-rcvd : 0  
advertise-interval-errors : 0 ip-ttl-errors : 0  
priority-zero-pkts-rcvd : 0 priority-zero-pkts-sent : 0  
invalid-type-pkts-rcvd : 0 address-list-errors : 0  
pkt-length-errors : 0
```

Set group priority

Set a virtual router priority to 255 to ensure that router is the *owner* virtual router for the VRRP group. The router which has the highest primary IP address of the interface becomes the *master*. The default priority for a virtual router is 100. If the master router fails, VRRP begins the election process to choose a new master router based on the next-highest priority.

1. Create a virtual router for the interface with the VRRP identifier in INTERFACE mode (1 to 255).

```
vrrp-group vrrp-id
```

2. Configure the priority number for the VRRP group in INTERFACE-VRRP mode (1 to 255, default 100).

```
priority number
```

Set VRRP group priority

```
OS10(config)# interface ethernet 1/1/5  
OS10(conf-if-eth1/1/5)# vrrp-group 254  
OS10(conf-eth1/1/5-vrid-254)# priority 200
```

Verify VRRP group priority

```
OS10(conf-eth1/1/5-vrid-254)# do show vrrp 254  
  
Interface : ethernet1/1/5 IPv4 VRID : 254  
Primary IP Address : 10.1.1.1 State : master-state  
Virtual MAC Address : 00:00:5e:00:01:01  
Version : version-3 Priority : 200  
Preempt : Hold-time :  
Authentication : no-authentication  
Virtual IP address :  
10.1.1.1  
master-transitions : 1 advertise-rcvd : 0  
advertise-interval-errors : 0 ip-ttl-errors : 0  
priority-zero-pkts-rcvd : 0 priority-zero-pkts-sent : 0  
invalid-type-pkts-rcvd : 0 address-list-errors : 0  
pkt-length-errors : 0
```

Authentication

Simple authentication of VRRP packets ensures that only trusted routers participate in VRRP processes. When you enable authentication, OS10 includes the password in its VRRP transmission. The receiving router uses that password to verify the transmission.

You must configure all virtual routers in the VRRP group with the same password. You must enable authentication with the same password or authentication is disabled. Authentication for VRRPv3 is not supported.

1. Create a virtual router for the interface with the VRRP identifier in INTERFACE mode (1 to 255).

```
vrrp-group vrrp-id
```

2. Configure a simple text password in INTERFACE-VRRP mode.

```
authentication-type simple-text text [auth-text]
```

- `simple-text text` — Enter the keyword and a simple text password.
- `auth-text` — (Optional) Enter a character string up to eight characters long as a password.

Configure VRRP authentication

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# vrrp-group 250
OS10(conf-eth1/1/5-vrid-250)# authentication simple-text eureka
```

Verify VRRP authentication configuration

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# vrrp-group 1
OS10(conf-eth1/1/1-vrid-1)# authentication simple-text dell
```

Disable preempt

Prevent the Backup router with the higher priority from becoming the master router by disabling the preemption process. The `preempt` command is enabled by default. The command forces the system to change the master router if another router with a higher priority comes online.

You must configure all virtual routers in the VRRP group with the same settings. Configure all routers with `preempt` enabled or configure all with `preempt` disabled.

1. Create a virtual router for the interface with the VRRP identifier in INTERFACE mode (1 to 255).

```
vrrp-group vrrp-id
```

2. Prevent any backup router with a higher priority from becoming the Master router in INTERFACE-VRRP mode.

```
no preempt
```

Disable preempt

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# vrrp-group 254
OS10(conf-eth1/1/5-vrid-254)# no preempt
```

View running configuration

```
OS10(conf-eth1/1/5-vrid-254)# do show running-configuration
! Version 10.2.0E
! Last configuration change at Sep  24
07:17:45 2016
!
debug radius false
snmp-server contact http://www.dell.com/support/softwarecontacts
snmp-server location "United States"
username admin password $6$q9QBeYjZ$jfzxVqGhxxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH.
aaa authentication system:local
!
interface ethernet1/1/5
 ip address 1.1.1.1/16
 no switchport
 no shutdown
!
vrrp-group 254
 priority 125
 virtual-address 1.1.1.3
```

```
no preempt
!
```

Advertisement interval

By default, the Master router transmits a VRRP advertisement to all members of the VRRP group every one second, indicating it is operational and is the Master router.

If the VRRP group misses three consecutive advertisements, the election process begins and the Backup virtual router with the highest priority transitions to Master. To avoid throttling VRRP advertisement packets, Dell EMC recommends increasing the VRRP advertisement interval to a value higher than the default value of one second. If you do change the time interval between VRRP advertisements on one router, change it on all participating routers.

If you are configuring VRRP version 2, you must configure the timer values in multiple of whole seconds. For example, a timer value of 3 seconds or 300 centiseconds are valid and equivalent. A time value of 50 centiseconds is invalid because it not a multiple of 1 second. If you are using VRRP version 3, you must configure the timer values in multiples of 25 centiseconds. A centiseconds is 1/100 of a second.

- Create a virtual router for the interface with the VRRP identifier in INTERFACE mode (1 to 255).

```
vrrp-group vrrp-id
```

- For VRRPv2, change the advertisement interval setting in seconds in INTERFACE-VRRP mode (1 to 255, default 1).

```
advertise-interval seconds
```

- For VRRPv3, change the advertisement centiseconds interval setting INTERFACE-VRRP mode (25 to 4075, default 100).

```
advertise-interval centiseconds centiseconds
```

Change advertisement interval

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# vrrp-group 1
OS10(config-eth1/1/1-vrid-1)# advertise-interval centiseconds 200
```

View running configuration

```
OS10(config-eth1/1/1-vrid-1)# do show running-configuration

! Version 10.1.9999P.2281
! Last configuration change at Jul 26 12:22:33 2016
!
aaa authentication system:local
!
interface ethernet1/1/1
 ip address 10.1.1.1/16
 no switchport
 no shutdown
!
 vrrp-group 1
  advertisement-interval centiseconds 200
  priority 200
  virtual-address 10.1.1.1
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
```

Interface/object tracking

You can monitor the state of any interface according to the virtual group. OS10 supports a maximum of 10 track groups and each track group can track a maximum of five interfaces.

If the tracked interface goes down, the VRRP group's priority decreases by a default value of **10** — also known as *cost*. If the tracked interface's state goes up, the VRRP group's priority increases by *priority-cost*.

The lowered priority of the VRRP group may trigger an election. As the Master/Backup VRRP routers are selected based on the VRRP group's priority, tracking features ensure that the best VRRP router is the Master for that group. The priority cost of tracking group must be less than the configured priority on the VRRP group. If the VRRP group is configured as Owner router (priority 255), tracking for that group is disabled, regardless of the state of the tracked interfaces. The priority of the Owner group always remains at 255.

For a virtual group, track the line-protocol state or the routing status of any interface with the `interface` command. Enter an interface type and `node/slot/port[:subport]` information, or VLAN number:

- `ethernet` — Physical interface (1 to 48)
- `vlan` — VLAN interface (1 to 4093)

For a virtual group, track the status of a configured object with the `track` command and use the object number. You can also configure a tracked object for a VRRP group with this command before you create the tracked object. No changes in the VRRP group's priority occur until the tracked object is defined and determined to be down.

Configure tracking

To track the objects in a VRRP group or on interfaces, use the following commands. The sum of all the costs for all tracked interfaces must be less than the configured priority of the VRRP group.

1. Assign an object tracking unique ID number in CONFIGURATION mode (1 to 500).

```
track track-id
```

2. Monitor an interface and set a value to subtract from the interface's VRRP group priority in Track CONFIGURATION mode.

```
interface ethernet node/slot/port[:subport]
```

3. (Optional) View the configuration of tracked objects in VRRP groups on a specified interface in Track CONFIGURATION mode.

```
do show running-config interface interface
```

Configure interface tracking

```
OS10(config)# track 10
OS10(conf-track-10)# interface ethernet 1/1/5
```

View running configuration

```
OS10(conf-track-10)# do show running-configuration

! Version 10.1.9999P.2281
! Last configuration change at Jul 27 03:24:01 2016
!
aaa authentication system:local
!
interface ethernet1/1/1
 ip address 10.1.1.1/16
 no switchport
 no shutdown
!
 vrrp-group 1
  priority 200
  virtual-address 10.1.1.1
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/3
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/4
 switchport access vlan 1
 no shutdown
!
```

```

interface ethernet1/1/5
  switchport access vlan 1
  no shutdown
!
interface ethernet1/1/6
  switchport access vlan 1
  no shutdown
!
.....
.....
interface vlan1
  no shutdown
!
interface mgmt1/1/1
  no shutdown
!
support-assist
!
track 10
  track-interface ethernet1/1/1

```

VRRP commands

advertise-interval

Sets the time interval between VRRP advertisements.

Syntax `advertise-interval [seconds | centiseconds centiseconds]`

Parameters

- `seconds` — Set the advertise interval in seconds (1 to 255).
- `centiseconds centiseconds` — (Optional) Enter a value in multiples of 25 (25 to 4075).

Default 1 second or 100 centiseconds

Command Mode INTERFACE-VRRP

Usage Information Dell EMC recommends keeping the default setting for this command. If you do change the time interval between VRRP advertisements on one router, change it on all routers. The `no` version of this command sets the VRRP advertisements timer interval back to its default value (1 second or 100 centiseconds).

Example

```
OS10(conf-eth1/1/6-vrid-250)# advertise-interval 120 centiseconds 100
```

Supported Releases 10.2.0E or later

authentication-type

Enables authentication of VRRP data exchanges.

Syntax `authentication-type simple-text password [auth-text]`

Parameters

- `simple-text password` — Enter a simple text password.
- `auth-text` — (Optional) Enter a character string up to eight characters long as a password.

Default Disabled

Command Mode INTERFACE-VRRP

Usage Information With authentication enabled, OS10 ensures that only trusted routers participate in routing in an autonomous network. The `no` version of this command disables authentication of VRRP data exchanges.

Example

```
OS10(conf-ethernet1/1/6-vrid-250)# authentication simple-text eureka
```

Supported Releases 10.2.0E or later

preempt

Permits (preempts) a backup router with a higher priority value to become the master router.

Syntax `preempt`

Parameters None

Default Enabled

Command Mode INTERFACE-VRRP

Usage Information VRRP uses preempt to determine what happens after a VRRP backup router becomes the Master. With preempt enabled by default, VRRP switches to a backup if that backup router comes online with a priority higher than the new Master router. If you disable preempt, VRRP switches only if the original Master recovers or the new Master fails. The `no` version of this command disables preemption.

Example

```
OS10(conf-eth1/1/5-vrid-254)# preempt
```

Supported Releases 10.2.0E or later

priority

Assigns a VRRP priority value for the VRRP group. The VRRP uses this value during the master election process.

Syntax `priority number`

Parameters `number` — Enter a priority value (1 to 254).

Default 100

Command Mode INTERFACE-VRRP

Usage Information To guarantee that a VRRP group becomes master, configure the VRRP group's virtual address with same IP address as the interface's primary IP address, and change the priority of the VRRP group to 255. If you set this command to 255 and the `virtual-address` is not equal to the interface's primary IP address, the system displays an error message. The `no` version of this command resets the value to the default (100).

Example

```
OS10(conf-eth1/1/5-vrid-254)# priority 200
```

Supported Releases 10.2.0E or later

show vrrp

Displays VRRP group information.

Syntax `show vrrp {brief | vrrp-id | ipv6 group-id}`

Parameters

- `brief` — Displays the configuration information for all VRRP instances in the system.
- `vrrp-id` — Enter a VRRP group ID number to view the VRRP IPv4 group operational status information (1 to 255).
- `ipv6 group-id` — (Optional) Enter a VRRP group ID number to view the specific IPv6 group operational status information (1 to 255).

Default All IPv4 VRRP group configuration

Command Mode EXEC

Usage Information Displays all active VRRP groups. If no VRRP groups are active, the system displays “No Active VRRP group.”.

Example (Brief)

```
OS10 # show vrrp brief
Interface      Group Priority Preemption State      Master-addr Virtual
addr(s)
-----
ethernet1/1/1 1      200      true      master-state 10.1.1.1 10.1.1.1
```

Example (IPv6)

```
OS10 # show vrrp ipv6 1
Interface : ethernet1/1/1      IPv6 VRID : 1
Primary IP Address : 10::1      State : master-state
Virtual MAC Address : 00:00:5e:00:02:01
Version : version-3      Priority : 200
Preempt :      Hold-time :
Authentication : no-authentication
Virtual IP address :
10::1
master-transitions : 1      advertise-rcvd : 0
advertise-interval-errors : 0      ip-ttl-errors : 0
priority-zero-pkts-rcvd : 0      priority-zero-pkts-sent : 0
invalid-type-pkts-rcvd : 0      address-list-errors : 0
pkt-length-errors : 0
```

Supported Releases 10.2.0E or later

track

Assigns a unique identifier to track an object.

Syntax track *track-id* [priority cost [value]]

- Parameters**
- *track-id* — Enter the object tracking resource ID number (1 to 500).
 - *priority cost value* — (Optional) Enter a cost value to subtract from the priority value (1 to 254)

Default 10

Command Mode INTERFACE-VRRP

Usage Information If the interface is disabled, the cost value subtracts from the priority value and forces a new Master election. This election process is applicable when the priority value is lower than the priority value in the Backup virtual router. The no version of this command resets the value to the default.

Example

```
OS10(conf-eth1/1/5-vrid-254)# track 400
```

Example (Priority Cost)

```
OS10(conf-eth1/1/5-vrid-254)# track 400 priority-cost 20
```

Supported Releases 10.2.0E or later

track interface

Monitors an interface and lowers the priority value of the VRRP group on that interface, if disabled.

Syntax interface {ethernet *node/slot/port[:subport]*} [*line-protocol*]

- Parameters**
- *ethernet node/slot/port[:subport]* — (Optional) Enter the keyword and the interface information to track.
 - *line-protocol* — (Optional) Tracks the interface line-protocol operational status.

Default Disabled

Command Mode	EXEC
Usage Information	Assign an object tracking unique ID number before tracking the interface. Use the <code>line-protocol</code> parameter to track for interface operational status information. The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# track 10 OS10(conf-track-10)# interface ethernet 1/1/5</pre>
Supported Releases	10.2.0E or later

virtual-address

Configures up to 10 virtual router IP addresses in the VRRP group. Set at least one virtual IP address for the VRRP group to start sending VRRP packets.

Syntax	<code>virtual-address ip-address1 [ip-address2...ip-address10]</code>
Parameters	<ul style="list-style-type: none"> <code>ip-address1</code> — Enter the IP address of a virtual router in A.B.C.D format. The IP address must be on the same subnet as the interface's primary IP address. <code>ip-address2...ip-address10</code> — (Optional) Enter up to nine additional IP addresses of virtual routers, separated by a space. The IP addresses must be on the same subnet as the interface's primary IP address.
Default	Enabled
Command Mode	INTERFACE-VRRP
Usage Information	The VRRP group only becomes active and sends VRRP packets when you configure a virtual IP address. When you delete the virtual address, the VRRP group stops sending VRRP packets. A system message appears after you enter or delete the <code>virtual-address</code> command. To guarantee that a VRRP group becomes Master, configure the VRRP group's virtual address with the same IP address as the interface's primary IP address and change the priority of the VRRP group to 255. You can ping the virtual addresses configured in all VRRP groups. The <code>no</code> version of this command deletes one or more virtual-addresses configured in the system.
Example	<pre>OS10(conf-eth1/1/5-vrid-254)# virtual address 10.1.1.15</pre>
Supported Releases	10.2.0E or later

vrrp delay reload

Sets the delay time for VRRP initialization after a system reboot.

Syntax	<code>vrrp delay reload seconds</code>
Parameters	<code>seconds</code> — Enter the number of seconds for the VRRP reload time (0 to 900).
Default	0
Command Mode	CONFIGURATION
Usage Information	VRRP delay reload time of zero seconds indicates no delays. This command configuration applies to all the VRRP configured interfaces. The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# vrrp delay reload 5</pre>
Supported Releases	10.4.0E(R1) or later

vrrp-group

Assigns a VRRP group identification number to an IPv4 interface or VLAN

Syntax	<code>vrrp-group vrrp-id</code>
Parameters	<i>vrrp-id</i> — Enter a VRRP group identification number (1 to 255).
Default	Not configured
Command Mode	INTERFACE-VRRP
Usage Information	The VRRP group only becomes active and sends VRRP packets when you configure a virtual IP address. When you delete the virtual address, the VRRP group stops sending VRRP packets. The <code>no</code> version of this command removes the <code>vrrp-group</code> configuration.

Example

```
OS10(conf-if-eth1/1/5)# vrrp-group 254
```

Example (VLAN)

```
OS10(conf-if-vl-10)# vrrp-group 5
```

Supported Releases 10.2.0E or later

vrrp-ipv6-group

Assigns a VRRP group identification number to an IPv6 interface.

Syntax	<code>vrrp-ipv6-group vrrp-id</code>
Parameters	<i>vrrp-id</i> — Enter a VRRP group identification number (1 to 255).
Default	Not configured
Command Mode	INTERFACE-VRRP
Usage Information	The VRRP group only becomes active and sends VRRP packets when you configure a virtual IP address. When you delete the virtual address, the VRRP group stops sending VRRP packets. The <code>no</code> version of this command removes the <code>vrrp-ipv6-group</code> configuration.

Example

```
OS10(conf-if-eth1/1/7)# vrrp-ipv6-group 250
```

Supported Releases 10.2.0E or later

vrrp version

Sets the VRRP version for the IPv4 group.

Syntax	<code>vrrp version {2 3}</code>
Parameters	<ul style="list-style-type: none">• 2 — Set to VRRP version 2.• 3 — Set to VRRP version 3.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command disables the VRRP version for the IPv4 group.

Example

```
OS10(config)# vrrp version 2
```

Supported Releases 10.2.0E or later

UFT modes

Unified Forwarding Table (UFT) gives the flexibility to configure the sizes of internal L2/L3 forwarding tables of a switch to match the needs of particular network environment. A switch in a Layer 2 network may require a larger MAC address table size, while a switch in a Layer 3 network may require a larger routing table size.

OS10 supports several UFT modes for the forwarding tables. By default, OS10 selects a UFT mode which provides a reasonable size for all tables. The supported UFT modes are: default, scaled-l2-switch, scaled-l3-hosts, and scaled-l3-routes.

Table 5. UFT Modes — Table Size for S4000, S6010, S4048

UFT Mode	L2 MAC Table Size	L3 Host Table Size	L3 Routes Table Size
Scaled-l2-switch	294912	16384	16384
Scaled-l3-hosts	98304	212992	98304
Scaled-l3-routes	32768	16384	131072
Default	163840	147456	16384

Table 6. UFT Modes — Table Size for S3000

UFT Mode	L2 MAC Table Size	L3 Host Table Size	L3 Routes Table Size
Scaled-l2-switch	40960	2048	8192
Scaled-l3-hosts	8192	18432	8192
Default	28672	8192	8192

Table 7. UFT Modes — Table Size for S41XX

UFT Mode	L2 MAC Table Size	L3 Host Table Size	L3 Routes Table Size
Scaled-l2-switch	278528	4096	16384
Scaled-l3-hosts	16384	266240	16384
Scaled-l3-routes	16384	4096	262144
Default	81920	69632	131072

Configure UFT modes

Available UFT modes include L2 MAC table, L3 host table, or L3 route table sizes.

- Select a mode to initialize the maximum table size in CONFIGURATION mode.

```
hardware forwarding-table mode [scaled-l2 | scaled-l3-routes | scaled-l3-hosts]
```

- Disable UFT mode in CONFIGURATION mode.

```
no hardware forwarding-table
```

Configure UFT mode

```
OS10(config)# hardware forwarding-table mode scaled-l3-hosts
```

View UFT mode information

```
OS10# show hardware forwarding-table mode
Mode                               Current Settings           Next-boot Settings
L2 MAC Entries :                   163840                     98304
L3 Host Entries :                   147456                     212992
L3 Route Entries :                  16384                      98304
```

View UFT information for all modes

```
OS10# show hardware forwarding-table mode all
Mode           default      scaled-l2    scaled-l3-routes    scaled-l3-hosts
L2 MAC Entries 163840      294912      32768              98304
L3 Host Entries 147456      16384       16384              212992
L3 Route Entries 16384       16384       131072             98304
```

IPv6 extended prefix routes

IPv6 addresses that contain prefix routes with mask between /64 to /128 are called as IPv6 extended prefix routes. These routes require double the key size in the Longest prefix match (LPM) table.

You can configure the number of route entries for extended prefix using the `hardware l3 ipv6-extended-prefix prefix-number` command.

Save and Reload the switch for the settings to become effective.

Configure IPv6 extended prefix route

```
OS10# configure terminal
OS10(config)# hardware l3 ipv6-extended-prefix 2048
% Warning: IPv6 Extended Prefix Installation will be applied only after a save and reload.
OS10(config)# do write memory
OS10(config)# reload
```

View IPv6 extended prefix route configuration

```
OS10# show running-configuration | grep hardware
hardware l3 ipv6-extended-prefix 2048
```

Configuration before reload:

```
OS10# show hardware l3
IPv6 Extended Prefix Entries: 0
Current Settings           Next-boot Settings
                           2048
```

Configuration after reload:

```
OS10# show hardware l3
IPv6 Extended Prefix Entries: 2048
Current Settings           Next-boot Settings
                           2048
```

The `no` version of the command removes the IPv6 extended prefix route configuration. Save and Reload the switch to remove the configuration.

```
OS10(config)# no hardware l3 ipv6-extended-prefix
% Warning: Un-configuring IPv6 Extended Prefix will be applied only after a save and reload.
```

UFT commands

hardware forwarding-table mode

Select a mode to initialize the maximum scalability size. The available options are: scaled L2 MAC address table, scaled L3 routes table, or scaled L3 hosts table.

Syntax `hardware forwarding-table mode {scaled-l2 | scaled-l3-routes | scaled-l3-hosts}`

Use the `no hardware forwarding-table mode` command to set the UFT mode to default.

- Parameters**
- `scaled-l2` — Maximize the MAC address table size.
 - `scaled-l3-routes` — Maximize the L3 routes table size.
 - `scaled-l3-hosts` — Maximize the L3 hosts table size

Defaults The default parameters vary according to the platform. See [UFT modes](#) on page 458.

Command Mode CONFIGURATION

Usage Information Configure the sizes of internal L2 and L3 forwarding tables of the switch as per the requirements of the network environment. You need to reload the switch to apply the changes.

Example

```
OS10(config)# hardware forwarding-table mode scaled-l3-hosts
```

Supported Releases 10.3.0E or later

hardware l3 ipv6-extended-prefix

Configures the maximum number of route entries for IPv6 extended prefix route.

Syntax `hardware l3 ipv6-extended-prefix prefix-number`

Parameters *prefix-number* — Enter the maximum number of route entries for IPv6 extended prefix route. The options available are: 1024, 2048, or 3072.

Defaults None

Command Mode CONFIGURATION

Usage Information Save and Reload the switch for the settings to become effective. The `no` version of the command removes the IPv6 extended prefix route configuration.

Example

```
OS10# configure terminal
OS10(config)# hardware l3 ipv6-extended-prefix 2048
% Warning: IPv6 Extended Prefix Installation will be applied only after
a save and reload.
OS10(config)# do write memory
OS10(config)# reload
```

Supported Releases 10.4.1.0 or later

show hardware forwarding-table mode

Displays the current hardware forwarding table mode, and the mode after the next boot.

Syntax `show hardware forwarding-table mode`

Parameters None

Defaults None

Command Mode	EXEC
Usage Information	Use this command to view the current hardware forwarding table mode and the mode after the next boot.
Example	<pre>OS10# show hardware forwarding-table mode Mode Current Settings Next-boot Settings L2 MAC Entries : 163840 scaled-l3-hosts L3 Host Entries : 147456 98304 L3 Route Entries : 16384 212992 L3 Route Entries : 16384 98304</pre>
Supported Releases	10.3.0E or later

show hardware forwarding-table mode all

Displays table sizes for the available hardware forwarding table modes.

Syntax	show hardware forwarding-table mode all
Parameters	None
Defaults	None
Command Mode	EXEC
Usage Information	Use this command to view details of all the forwarding-table modes.

Example

```
OS10# show hardware forwarding-table mode all
Mode                               default      scaled-l2    scaled-l3-routes
scaled-l3-hosts
L2 MAC Entries      163840      294912      32768        98304
L3 Host Entries     147456      16384       16384        212992
L3 Route Entries    16384       16384       131072       98304
```

Supported Releases	10.3.0E or later
---------------------------	------------------

show hardware l3

Displays the IPv6 extended prefix route configuration.

Syntax	show hardware l3
Parameters	None
Defaults	None
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show hardware l3
IPv6 Extended Prefix Entries: 2048
Current Settings           Next-boot Settings
2048
```

Supported Releases	10.4.1.0 or later
---------------------------	-------------------

System management

Dynamic Host Configuration Protocol	Provides information to dynamically assign IP addresses and other configuration parameters to network hosts based on policies, see DHCP commands .
Network Time Protocol	Provides information to synchronize timekeeping between time servers and clients, see NTP commands .
RESTCONF API	Enables you to configure and monitor an OS10 switch using JSON-structured messages to access YANG-modeled data in configuration data stores, see CLI commands for RESTCONF API .
Security	Provides information about role-based access control, RADIUS server, user roles, and user names, see Security commands .
Simple Network Management Protocol	Provides a message format for communication between Simple Network Management Protocol (SNMP) managers and agents. SNMP provides a standardized framework and common language for network monitoring and device management, see SNMP commands .
OS10 image upgrade	Provides information to upgrade the OS10 software image, see Upgrade commands .

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is an application layer protocol that dynamically assigns IP addresses and other configuration parameters to network end-stations, also known as hosts, based on configuration policies network administrators determine.

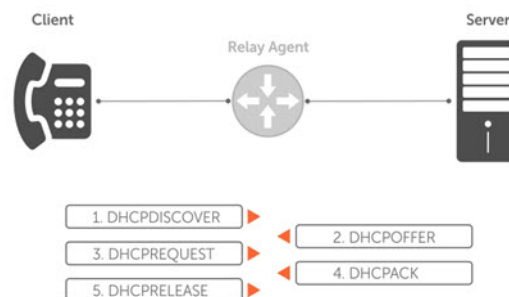


Figure 5. Client and Server Messaging

DHCP server	Network device offering configuration parameters to the client.
DHCP client	Network device requesting configuration parameters from the server.
Relay agent	Intermediary network device that passes DHCP messages between the client and the server when the server is not on the same subnet as the host.

Packet format and options

The DHCP server listens on port 67 and transmits to port 68. The DHCP client listens on port 68 and transmits to port 67.

Configuration parameters are options in the DHCP packet in type, length, value (TLV) format. To limit the number of parameters that servers must provide, hosts enter the parameters that they require and the server sends only those parameters. DHCP uses the User Datagram Protocol (UDP) as its transport protocol.

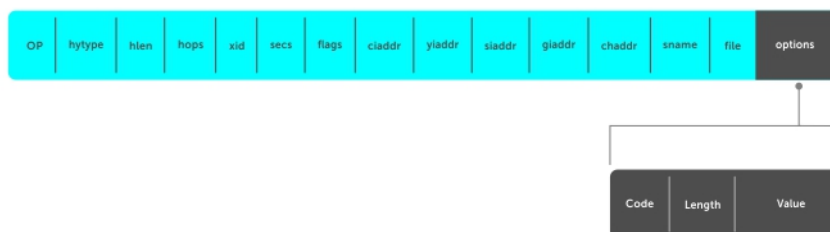


Figure 6. DHCP Packet Format

The table shows common options using DHCP packet formats.

DHCP Option Description

Subnet mask	1 — Subnet mask of the client
Router	3 — Router IP addresses that serve as the default gateway for the client
Domain name server	6 — Domain name servers (DNS) that are available to the client
Domain name	15 — Domain name that clients use to resolve hostnames via DNS
IP address lease time	51 — Amount of time that the client uses an assigned IP address
DHCP message type	53: <ul style="list-style-type: none"> • 1 — DHCPDISCOVER • 2 — DHCPOFFER • 3 — DHCPREQUEST • 4 — DHCPDECLINE • 5 — DHCPACK • 6 — DHCPNACK • 7 — DHCPRELEASE • 8 — DHCPINFORM
Parameter request list	55 — Parameters the server requires for DHCP clients. This is a series of octets where each octet is a DHCP option code
Renewal time	58 — Amount of time, after the IP address is granted, that the client attempts to renew its lease with the <i>original</i> server
Rebinding time	59 — Amount of time, after the IP address is granted, that the client attempts to renew its lease with <i>any</i> server, if the original server does not respond
Vendor class identifier	60 — User-defined string the Relay Agent uses to forward DHCP client packets to a specific DHCP server
User port stacking	230 — Stacking option variable that provides the DHCP server stack-port details when the DHCP offer is set
End	255 — Signal of the last option in the DHCP packet

DHCP server

The Dynamic Host Configuration Protocol (DHCP) server provides network configuration parameters to DHCP clients on request. A DHCP server dynamically allocates four required IP parameters to each computer on the virtual local area network (VLAN) — the IP address, network mask, default gateway, and name server address. DHCP IP address allocation works on a client/server model where the server assigns the client reusable IP information from an address pool.

DHCP automates network-parameter assignment to network devices. Even in small networks, DHCP makes it easier to add new devices to the network. The DHCP access service provides a centralized, server-based setup to add clients to the network. This setup means you do not have to manually create and maintain IP address assignments for clients.

When you use DHCP to manage a pool of IP addresses among hosts, you reduce the number of IP addresses you need. DHCP manages the IP address pool by leasing an IP address to a host for a limited period, allowing the DHCP server to share a limited number of IP addresses. DHCP also provides a central database of devices that connects to the network and eliminates duplicate resource assignments.

Automatic address allocation

Automatic address allocation is an address assignment method that the DHCP server uses to lease an IP address to a client from a pool of available addresses. You cannot configure an empty DHCP pool, under a DHCP pool configuration. For a successful commit, you must have either a network statement or host/hardware-address (manual binding) configuration. An IP address pool is a range of addresses that the DHCP server assigns. The subnet number indexes the address pools.

1. Enable DHCP server-assigned dynamic addresses on an interface in DHCP <POOL> mode.

```
ip dhcp server
```

2. Create an IP address pool and provide a name in DHCP mode.

```
pool name
```

3. Enter the subnet from which the DHCP server may assign addresses in DHCP <POOL> mode. The `network` option specifies the subnet address. The `prefix-length` option specifies the number of bits used for the network portion of the address (18 to 31).

```
network network/prefix-length
```

4. Enter a range of IP addresses from the subnet specified above, which the DHCP server uses to assign addresses in DHCP <POOL> mode.

```
range {ip-address1 [ip-address2]}
```

NOTE: NOTE: Configure at least one interface to match one of the configured network pools. An interface matches a network pool when its IP address is included in the subnet defined for that network pool. For example, an interface with IP address 10.1.1.1/24 matches a pool configured with network 10.1.1.0/24.

DHCP server automatic address allocation

```
OS10(config)# ip dhcp server
OS10(config-dhcp)# pool Dell
OS10(config-dhcp-Dell)# default-router 20.1.1.1
OS10(config-dhcp-Dell)# network 20.1.1.0/24
OS10(config-dhcp-Dell)# range 20.1.1.2 20.1.1.8
```

Show running configuration

```
OS10(conf-dhcp-Dell)# do show running-configuration
...
!
ip dhcp server
!
pool Dell
network 20.1.1.0/24
default-router 20.1.1.1
range 20.1.1.2 20.1.1.8
```

Address lease time

Use the `lease {days [hours] [minutes] | infinite}` command to configure an address lease time (default 24 hours).

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool Dell
OS10(conf-dhcp-Dell)# lease 36
```


Default gateway

Ensure the IP address of the default router is on the same subnet as the client.

1. Enable DHCP server-assigned dynamic addresses on an interface in CONFIGURATION mode.

```
ip dhcp server
```

2. Create an IP address pool and provide a name in DHCP mode.

```
pool name
```

3. Enter the default gateway(s) for the clients on the subnet in order of preference in DHCP<POOL> mode.

```
default-router address
```

Change default gateway name

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool Dell
OS10(conf-dhcp-Dell)# default-router 20.1.1.1
```

Enable DHCP server

Use the `ip dhcp server` command to enable DHCP server-assigned dynamic addresses on an interface in CONFIGURATION mode. The DHCP server is disabled by default.

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# no disable
```

Hostname resolution

You have two choices for hostname resolution — domain name server (DNS) or NetBIOS Windows internet naming service (WINS). Both DHCP and WINS clients query IP servers to compare host names to IP addresses.

1. Enable DHCP server-assigned dynamic addresses on an interface in DHCP <POOL> mode.

```
ip dhcp server
```

2. Create in IP address pool and enter the name in DHCP mode.

```
pool name
```

3. Create a domain and enter the domain name in DHCP <POOL> mode.

```
domain-name name
```

4. Enter the DNS servers in order of preference that are available to a DHCP client in DHCP <POOL> mode.

```
dns-server address
```

DNS address resolution

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool Dell
OS10(conf-dhcp-Dell)# domain-name dell.com
OS10(conf-dhcp-Dell)# dns-server 192.168.1.1
```

NetBIOS WINS address resolution

DHCP clients can be one of four types of NetBIOS nodes — broadcast, peer-to-peer, mixed, or hybrid. Dell EMC recommends using hybrid as the NetBIOS node type.

1. Enable DHCP server-assigned dynamic addresses on an interface in DHCP *<POOL>* mode.

```
ip dhcp server
```

2. Create an IP address pool and enter the pool name in DHCP mode.

```
pool name
```

3. Enter the NetBIOS WINS name servers in order of preference that are available to DHCP clients in DHCP *<POOL>* mode.

```
netbios-name-server ip-address
```

4. Enter the keyword `Hybrid` as the NetBIOS node type in DHCP *<POOL>* mode.

```
netbios-node-type type
```

Configure NetBIOS WINS address resolution

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool Dell
OS10(conf-dhcp-Dell)# netbios-name-server 192.168.10.5
OS10(conf-dhcp-Dell)# netbios-node-type Hybrid
```

Manual binding entries

Address binding is mapping between the IP address and the media access control (MAC) address of a client. The DHCP server assigns the client an available IP address automatically and then creates an entry in the binding table. You can also manually create an entry for a client. Manual bindings help to guarantee that a particular network device receives a particular IP address.

Consider manual bindings as single-host address pools. There is no limit to the number of manual bindings, but you can only configure one manual binding per host. Manual binding entries do not display in the `show ip dhcp binding` output.

1. Create an address pool in DHCP mode.

```
pool name
```

2. Enter the client IP address in DHCP *<POOL>* mode.

```
host address
```

3. Enter the client hardware address in DHCP *<POOL>* mode.

```
hardware-address hardware-address
```

Configure manual binding

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool static
OS10(conf-dhcp-static)# host 20.1.1.2
OS10(conf-dhcp-static)# hardware-address 00:01:e8:8c:4d:0a
```

View DHCP binding table

```
OS10# show ip dhcp binding
  IP Address           Hardware address           Lease expiration           Hostname
+-----+-----+-----+-----+
11.1.1.254           00:00:12:12:12:12 Jan 27 2016 06:23:45

Total Number of Entries in the Table = 1
```

With fixed host configuration (manual binding), you must configure a network pool with a matching subnet. The static host-to-MAC address mapping pool inherits the network mask from the network pool with subnet configuration, which includes the host's address range.

Consider the following example:

```
OS10# show running-configuration interface ethernet 1/1/2
!
interface ethernet1/1/2
no shutdown
no switchport
ip address 100.1.1.1/24
flowcontrol receive off

OS10# show running-configuration ip dhcp
!
ip dhcp server
no disable
!
pool host1
host 100.1.1.34
hardware-address 00:0c:29:ee:4c:f4
!
pool hostnetwork
lease infinite
network 100.1.1.0/24
!
pool host2
host 20.1.1.34
hardware-address 00:0c:29:aa:22:f4
```

In this example, the pool 'host1,' which is the fixed host mapping pool, inherits the subnet and other attributes from the pool, 'hostnetwork,' which is the DHCP client IP address pool. There is no matching network pool for "host2." Hence, the DHCP client with the MAC address 00:0c:29:aa:22:f4 will not obtain the correct parameters.

DHCP relay agent

A DHCP relay agent relays DHCP messages to and from a remote DHCP server, even if the client and server are on different IP networks. You can configure the IP address of the remote DHCP server.

You can configure a device either as a DHCP server or a DHCP relay agent — but not both.

The DHCP relay agent supports multi-virtual routing and forwarding (VRF) instances. The client-facing and server-facing interfaces must be in the same VRF.

The DHCPv6 relay agent performs the same role as that of a DHCP relay agent, but in an IPv6 network. The DHCP relay agent forwards the DHCPv4/DHCPv6 messages from the configured interface to the DHCPv6 server as a unicast message. The DHCP relay agent then forwards the server's response to the client.

When you configure DHCPv6 relay on an interface, you must:

- Configure an IPv6 address on the interface.
- Ensure that the DHCPv6 server is reachable.

Option 82 for security

DHCP, as defined by RFC 2131, provides no authentication or security mechanisms. To provide security, the DHCP relay agent supports Option-82 with Circuit ID sub option, which is the printable name of the interface where the client request was received.

This option secures all DHCP traffic that goes through a DHCP relay agent, and ensures that communication between the DHCP relay agent and the DHCP server is not compromised.

The DHCP relay agent inserts Option 82 before forwarding DHCP packets to the DHCP server. The DHCP server includes Option 82 back in its response to the relay agent. The relay agent uses this information to forward a reply out the interface on which the request was received rather than flooding it on the entire VLAN. However, the relay agent removes Option 82 from its DHCP responses before forwarding the responses to the client.

 **NOTE:** Option 82 is supported, but not configurable.

View DHCP Information

Use the `show ip dhcp binding` command to view the DHCP binding table entries.

View DHCP Binding Table

```
OS10# show ip dhcp binding
  IP Address           Hardware address      Lease expiration      Hostname
+-----+-----+-----+-----+
11.1.1.254           00:00:12:12:12:12  Jan 27 2016 06:23:45
Total Number of Entries in the Table = 1
```

System domain name and list

If you enter a partial domain, the system searches different domains to finish or fully qualify that partial domain. A fully qualified domain name (FQDN) is any name that terminates with a period or dot.

OS10 searches the host table first to resolve the partial domain. The host table contains both statically configured and dynamically learned host and IP addresses. If OS10 cannot resolve the domain, it tries the domain name assigned to the local system. If that does not resolve the partial domain, the system searches the list of domains configured.

You can configure the `ip domain-list` command up to five times to enter a list of possible domain names. The system searches the domain names in the order they were configured until a match is found or the list is exhausted.

1. Enter a domain name in CONFIGURATION mode (up to 64 alphanumeric characters).

```
ip domain-name name
```

2. Add names to complete unqualified host names in CONFIGURATION mode.

```
ip domain-list name
```

Configure local system domain name and list

```
OS10(config)# ip domain-name ntengg.com
OS10(config)# ip domain-list dns1
OS10(config)# ip domain-list dns2
OS10(config)# ip domain-list dns3
OS10(config)# ip domain-list dns4
OS10(config)# ip domain-list dns5
```

View local system domain name information

```
OS10# show running-configuration

! Version 10.2.9999E
! Last configuration change at Feb 20 04:50:33 2017
!
username admin password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH.
aaa authentication system:local
ip domain-name dell.com
ip domain-list f10.com
ip name-server 1.1.1.1 2::2
ip host dell-f10.com 10.10.10.10
snmp-server community public read-only
snmp-server contact http://www.dell.com/support/
snmp-server location United States
debug radius false
```

DHCP commands

default-router address

Assigns a default gateway to clients based on the IP address pool.

Syntax	<code>default-router address [address2...address8]</code>
Parameters	<ul style="list-style-type: none">• <i>address</i> — Enter an IPv4 or IPv6 address to use as the default gateway for clients on the subnet in A.B.C.D or A::B format.• <i>address2...address8</i> — (Optional) Enter up to eight IP addresses, in order of preference.
Default	Not configured
Command Mode	DHCP-POOL
Usage Information	Configure up to eight IP addresses, in order of preference. Use the <code>no</code> version of this command to remove the configuration.
Example	<pre>OS10(conf-dhcp-20.1.1.1)# default-router 20.1.1.100</pre>
Supported Releases	10.2.0E or later

disable

Disables the DHCP server.

Syntax	<code>disable</code>
Parameters	None
Default	Disabled
Command Mode	DHCP
Usage Information	The <code>no</code> version of this command enables the DHCP server.
Example	<pre>OS10(conf-dhcp)# no disable</pre>
Supported Releases	10.2.0E or later

dns-server address

Assigns a DNS server to clients based on the address pool.

Syntax	<code>dns-server address [address2...address8]</code>
Parameters	<ul style="list-style-type: none">• <i>address</i> — Enter the DNS server IP address that services clients on the subnet in A.B.C.D or A::B format.• <i>address2...address8</i> — (Optional) Enter up to eight DNS server addresses, in order of preference.
Default	Not configured
Command Mode	DHCP-POOL
Usage Information	None
Example	<pre>OS10(conf-dhcp-Dell)# dns-server 192.168.1.1</pre>

Supported Releases 10.2.0E or later

domain-name

Configures the name of the domain where the device is located.

Syntax `domain-name domain-name`

Parameters `domain-name` — Enter the name of the domain (up to 32 characters).

Default Not configured

Command Mode DHCP-POOL

Usage Information This is the default domain name that appends to hostnames that are not fully qualified. The `no` version of this command removes the configuration.

Example

```
OS10(conf-dhcp-Dell)# domain-name dell.com
```

Supported Releases 10.2.0E or later

hardware-address

Configures the client hardware address for manual configurations.

Syntax `hardware-address nn:nn:nn:nn:nn:nn`

Parameters `nn:nn:nn:nn:nn:nn` — Enter the 48-bit hardware address.

Default Not configured

Command Mode DHCP-POOL

Usage Information The client hardware address is the MAC address of the client machine to which to lease a static IP address from.

Example

```
OS10(conf-dhcp-static)# hardware-address 00:01:e8:8c:4d:0a
```

Supported Releases 10.2.0E or later

host

Assigns a host to a single IPv4 or IPv6 address pool for manual configurations.

Syntax `host A.B.C.D/A::B`

Parameters `A.B.C.D/A::B` — Enter the host IP address in A.B.C.D or A::B format.

Default Not configured

Command Mode DHCP-POOL

Usage Information The host address is the IP address used by the client machine for DHCP.

Example

```
OS10(conf-dhcp-Dell)# host 20.1.1.100
```

Supported Releases 10.2.0E or later

ip dhcp server

Enters DHCP mode.

Syntax	<code>ip dhcp server</code>
Parameters	None
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	This command is used to enter DHCP mode.

Example

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)#
```

Supported Releases	10.2.0E or later
---------------------------	------------------

ip helper-address

Configure the DHCP server address. Forwards UDP broadcasts received on an interface to the DHCP server. You can configure multiple helper addresses per interface by repeating the same command for each DHCP server address.

Syntax	<code>ip helper-address address [vrf vrf-name]</code>
Parameters	<ul style="list-style-type: none">• <code>address</code> — Enter the IPv4 address to forward UDP broadcasts to the DHCP server in the A.B.C.D format.• <code>vrf vrf-name</code> — (Optional) Enter the keyword <code>vrf</code> and then the name of the VRF through which the host address can be reached.
Default	Disabled
Command Mode	INTERFACE
Usage Information	The DHCP server is available on L3 interfaces only. The <code>no</code> version of this command returns the value to the default. The client-facing and server-facing interfaces must be in the same VRF.

Example (IPv4)

```
OS10(config)# interface eth 1/1/22
OS10(conf-if-eth1/1/22)# ip helper-address 20.1.1.1 vrf blue
```

Supported Releases	10.2.0E or later
---------------------------	------------------

ipv6 helper-address

Configure the DHCPv6 server address. Forwards UDP broadcasts received from IPv6 clients to the DHCPv6 server. You can configure multiple helper addresses per interface by repeating the same command for each DHCPv6 server address.

Syntax	<code>ipv6 helper-address ipv6-address [vrf vrf-name]</code>
Parameters	<ul style="list-style-type: none">• <code>vrf vrf-name</code> — (Optional) Enter the keyword <code>vrf</code> and then the name of the VRF through which the host address can be reached.• <code>ipv6-address</code> — Specify the DHCPv6 server address in the A::B format.
Defaults	Disabled
Command Mode	INTERFACE
Usage Information	The <code>no</code> version of this command deletes the IPv6 helper address. Use this command on the interfaces where the DHCPv6 clients connect to forward the packets from clients to DHCPv6 server and vice-versa.

Example

```
OS10(config)# interface ethernet 1/1/22
OS10(conf-if-eth1/1/22)# ipv6 helper-address 2001:db8:0:1:1:1:1:1 vrf
blue
```

Supported Releases 10.4.1.0 or later

lease

Configures a lease time for the IP addresses in a pool.

Syntax `lease {infinite | days [hours] [minutes]}`

Parameters

- `infinite` — Enter the keyword to configure a lease which never expires.
- `days` — Enter the number of lease days (0 to 31).
- `hours` — Enter the number of lease hours (0 to 23).
- `minutes` — Enter the number of lease minutes (0 to 59).

Default 24 hours

Command Mode DHCP-POOL

Usage Information The `no` version of this command removes the lease configuration.

Example

```
OS10(conf-dhcp-Dell)# lease 2 5 10
```

Example (Infinite)

```
OS10(conf-dhcp-Dell)# lease infinite
```

Supported Releases 10.2.0E or later

netbios-name-server address

Configures a NetBIOS WINS server which is available to DHCP clients.

Syntax `netbios-name-server ip-address [address2...address8]`

Parameters

- `ip-address` — Enter the address of the NetBIOS WINS server.
- `address2...address8` — (Optional) Enter additional server addresses.

Default Not configured

Command Mode DHCP-POOL

Usage Information Configure up to eight NetBIOS WINS servers available to a Microsoft DHCP client, in order of preference. The `no` version of this command returns the value to the default.

Example

```
OS10(conf-dhcp-Dell)# netbios-name-server 192.168.10.5
```

Supported Releases 10.2.0E or later

netbios-node-type

Configures the NetBIOS node type for the DHCP client.

Syntax `netbios-node-type type`

Parameters `type` — Enter the NetBIOS node type:

- Broadcast — Enter b-node.
- Hybrid — Enter h-node.
- Mixed — Enter m-node.
- Peer-to-peer — Enter p-node.

Default	Hybrid
Command Mode	DHCP-POOL
Usage Information	The no version of this command resets the value to the default.
Example	<pre>OS10(conf-dhcp-Dell)# netbios-node-type h-node</pre>
Supported Releases	10.2.0E or later

network

Configures a range of IPv4 or IPv6 addresses in the address pool.

Syntax	<code>network address/mask</code>
Parameters	<code>address/mask</code> — Enter a range of IP addresses and subnet mask in A.B.C.D/x or A::B/x format.
Default	Not configured
Command Mode	DHCP-POOL
Usage Information	Use this command to configure a range of IPv4 or IPv6 addresses.
Example	<pre>OS10(config-dhcp-Dell)# network 20.1.1.1/24</pre>
Supported Releases	10.2.0E or later

pool

Creates an IP address pool name.

Syntax	<code>pool pool-name</code>
Parameters	<code>pool-name</code> — Enter the DHCP server pool name.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	Use this command to create an IP address pool name.
Example	<pre>OS10(conf-dhcp)# pool Dell OS10(conf-dhcp-Dell)#</pre>
Supported Releases	10.2.0E or later

range

Configures a range of IP addresses.

Syntax	<code>range {ip-address1 [ip-address2]}</code>
---------------	--

Parameters	<ul style="list-style-type: none"> • <i>ip-address1</i>—First IP address of the IP address range. • <i>ip-address2</i>—Last IP address of the IP address range.
Default	Not configured
Command Mode	DHCP-POOL
Usage Information	This command is used to configure a range of IP addresses that the OS10 switch, acting as the DHCP server, can assign to DHCP clients. The no version of this command requires only the first IP address to remove the range configuration.
Example	<pre>OS10(config)# ip dhcp server OS10(config-dhcp)# pool pool1 OS10(config-dhcp-pool1)# network 192.168.10.0/24 OS10(config-dhcp-pool1)# range 192.168.10.2 192.168.10.8</pre>
Supported Releases	10.4.1 or later

show ip dhcp binding

Displays the DHCP binding table with IPv4 addresses.

Syntax	<code>show ip dhcp binding</code>
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to view the DHCP binding table.
Example	<pre>OS10# show ip dhcp binding IP Address Hardware address Lease expiration Hostname +-----+-----+-----+-----+ 11.1.1.254 00:00:12:12:12:12 Jan 27 2016 06:23:45 -----+-----+-----+-----+ Total Number of Entries in the Table = 1</pre>
Supported Releases	10.2.0E or later

DNS commands

OS10 supports the configuration of a DNS host and domain parameters.

ip domain-list

Adds a domain name to the DNS list. This domain name appends to incomplete hostnames in DNS requests.

Syntax	<code>ip domain-list [<i>vrf vrf-name</i>] [<i>server-name</i>] <i>name</i></code>
Parameters	<ul style="list-style-type: none"> • <i>vrf vrf-name</i> — (Optional) Enter the key word <code>vrf</code> and then the name of the VRF to add a domain name to the DNS list corresponding to that VRF. • <i>server-name</i> — (Optional) Enter the server name to add a domain name to the DNS list. • <i>name</i> — Enter the name of the domain to append to the DNS list.
Default	Not configured
Command Mode	CONFIGURATION

Usage Information There is a maximum of six domain names to the DNS list. Use this domain name to complete unqualified host names. The `no` version of this command removes a domain name from the DNS list.

Example

```
OS10(config)# ip domain-list jay dell.com
```

Supported Releases 10.2.0E or later

ip domain-name

Configures the default domain and appends to incomplete DNS requests.

Syntax `ip domain-name [vrf vrf-name] server-name`

Parameters

- `vrf vrf-name` — (Optional) Enter the key word `vrf` and then the name of the VRF to configure the domain corresponding to that VRF.
- `server-name` — (Optional) Enter the server name the default domain uses.

Default Not configured

Command Mode CONFIGURATION

Usage Information This domain appends to incomplete DNS requests. The `no` version of this command returns the value to the default.

Example

```
OS10(config)# ip domain-name jay dell.com
```

Supported Releases 10.2.0E or later

ip host

Configures mapping between the host name server and the IP address.

Syntax `ip host [vrf vrf-name] [host-name] address`

Parameters

- `vrf vrf-name` — (Optional) Enter the key word `vrf` and then the name of the VRF to configure the name server to IP address mapping for that VRF.
- `host-name` — (Optional) Enter the name of the host.
- `address` — Enter an IPv4 or IPv6 address of the name server in A.B.C.D or A::B format.

Default Not configured

Command Mode CONFIGURATION

Usage Information The name-to-IP address table uses this mapping information to resolve host names. The `no` version of this command disables the mapping.

Example

```
OS10(config)# ip host dell 1.1.1.1
```

Supported Releases 10.2.0E or later

ip name-server

Configures up to a three IPv4 or IPv6 addresses used for network name servers.

Syntax `ip name-server ip-address [ip-address2 ip-address3]`

Parameters

- `ip-address` — Enter the IPv4 or IPv6 address of a domain name server to use for completing unqualified names (incomplete domain names that cannot be resolved).

- *ip-address2 ip-address3* — (Optional) Enter up to two additional IPv4 or IPv6 name servers, separated with a space.

Default Not configured

Command Mode CONFIGURATION

Usage Information OS10 does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port. You can separately configure both IPv4 and IPv6 domain name servers. In a dual stack setup, the system sends both A (request for IPv4) and AAAA (request for IPv6) record requests to a DNS server even if you only configure this command. The `no` version of this command removes the IP name-server configuration.

Example

```
OS10(config)# ip name-server 10.1.1.5
```

Supported Releases 10.2.0E or later

show hosts

Displays the host table and DNS configuration.

Syntax `show hosts [vrf vrf-name]`

Parameters `vrf vrf-name` — Enter the keyword `vrf` followed by the name of the VRF to display DNS host information corresponding to that VRF.

Default Not configured

Command Mode EXEC

Usage Information This command displays domain and host information.

Example

```
OS10# show hosts
Default Domain Name : dell.com
Domain List : abc.com
Name Servers : 1.1.1.1 20::2
=====
          Static Host to IP mapping Table
=====
Host                               IP-Address
-----
dell-pc1                            20.1.1.1
```

Supported Releases 10.2.0E or later

DHCP Limitations

This section lists the limitations in DHCP functionality.

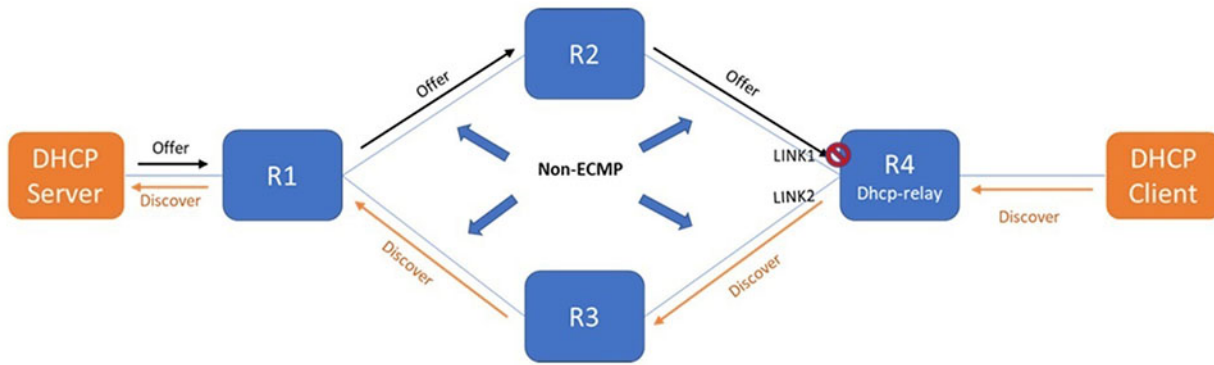
IPv4 DHCP asymmetric routing

OS10 does not support DHCP relay with IPv4 asymmetric routing. OS10 supports DHCP relay with IPv6 asymmetric routing.

The DHCP relay agent listens on the best DHCP server path. If the `DHCP OFFER` packet is sent through a path that the DHCP relay agent is not listening on, the `DHCP OFFER` packet drops. In this case, the DHCP client-enabled interface does not receive the IPv4 address.

For example, in the following topology, the `DHCP DISCOVER` packet is sent by the relay agent (R4) on link 2. The relay agent routing table points only to link 2 to reach the DHCP server. However, the DHCP server sends the `DHCP OFFER` packet to relay agent (R4) on a different path and the `DHCP OFFER` packet drops.

This issue occurs because the relay agent listens only on the *best path* uplink interfaces where the DHCP server is reachable.

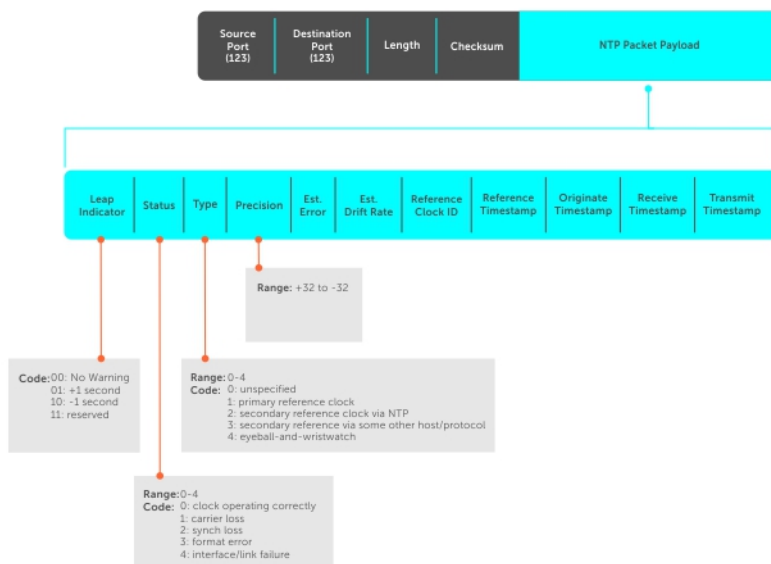


Network Time Protocol

Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients. The protocol coordinates time distribution in a large, diverse network. NTP clients synchronize with NTP servers that provide accurate time measurement. NTP clients choose from several NTP servers to determine which offers the best available source of time and the most reliable transmission of information.

To get the correct time, OS10 synchronizes with a time-serving host. For the current time, you can set the system to poll specific NTP time-serving hosts. From those time-serving hosts, the system chooses one NTP host to synchronize with and acts as a client to the NTP host. After the host-client relationship establishes, the networking device propagates the time information throughout its local network.

The NTP client sends messages to one or more servers and processes the replies as received. Information included in the NTP message allows each client/server peer to determine the timekeeping characteristics of its other peers, including the expected accuracies of their clocks. Using this information, each peer selects the best time from several other clocks, updates the local clock, and estimates its accuracy.



NOTE: OS10 supports both NTP server and client roles.

Enable NTP

NTP is disabled by default. To enable NTP, configure an NTP server to which the system synchronizes. To configure multiple servers, enter the command multiple times. Multiple servers may impact CPU resources.

- Enter the IP address of the NTP server to which the system synchronizes in CONFIGURATION mode.

```
ntp server ip-address
```

View system clock state

```
OS10(config)# do show ntp status
system peer:          0.0.0.0
system peer mode:    unspec
leap indicator:      11
stratum:             16
precision:           -22
root distance:       0.00000 s
root dispersion:     1.28647 s
reference ID:        [73.78.73.84]
reference time:      00000000.00000000 Mon, Jan  1 1900  0:00:00.000
system flags:        monitor ntp kernel stats
jitter:              0.000000 s
stability:           0.000 ppm
broadcastdelay:      0.000000 s
authdelay:           0.000000 s
```

View calculated NTP synchronization variables

```
OS10(config)# do show ntp associations
=====
remote          local      st poll reach  delay  offset  disp
=====
10.16.150.185   10.16.151.123 16 1024   0 0.00000 0.000000 3.99217
OS10# show ntp associations
remote          local      st poll reach  delay  offset  disp
=====
10.16.150.185   10.16.151.123 16 1024   0 0.00000 0.000000 3.99217
```

Broadcasts

Receive broadcasts of time information and set interfaces within the system to receive NTP information through broadcast. NTP is enabled on all active interfaces by default. If you disable NTP on an interface, the system drops any NTP packets sent to that interface.

1. Set the interface to receive NTP packets in INTERFACE mode.

```
ntp broadcast client
```

2. Disable NTP on the interface in INTERFACE mode.

```
ntp disable
```

Configure NTP broadcasts

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# ntp broadcast client
```

Disable NTP broadcasts

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# ntp disable
```

Source IP address

Configure one interface IP address to include in all NTP packets. The source address of NTP packets is the interface IP address the system uses to reach the network by default.

- Configure a source IP address for NTP packets in CONFIGURATION mode.

```
ntp source interface
```

- *ethernet* — Enter the keyword and node/slot/port information.
- *port-channel* — Enter the keyword and number.
- *vlan* — Enter the keyword and VLAN number (1 to 4093).
- *loopback* — Enter the keyword and number (0 to 16383).
- *mgmt* — Enter the keyword and node/slot/port information (default 1/1/1).

Configure source IP address

```
OS10(config)# ntp source ethernet 1/1/10
```

View source IP configuration

```
OS10(config)# do show running-configuration | grep source  
ntp source ethernet1/1/1
```

Authentication

NTP authentication and the corresponding trusted key provide a reliable exchange of NTP packets with trusted time sources. NTP authentication begins with the creation of the first NTP packet after key configuration. NTP authentication uses the message digest 5 (MD5) algorithm. The key is embedded in the synchronization packet that is sent to an NTP time source.

1. Enable NTP authentication in CONFIGURATION mode.

```
ntp authenticate
```

2. Set an authentication key number and key in CONFIGURATION mode (1 to 4294967295).

```
ntp authentication-key number md5 key
```

- The *number* must match in the `ntp trusted-key` command.
 - The *key* is an encrypted string.
3. Define a trusted key in CONFIGURATION mode (1 to 4294967295). The *number* must match in the `ntp trusted-key` command.

```
ntp trusted-key number
```

4. Configure an NTP server in CONFIGURATION mode.

```
ntp server {hostname | ipv4-address | ipv6-address} [key keyid] [prefer]
```

- *hostname* — Enter the keyword to see the IP address or host name of the remote device.
 - *ipv4-address* — Enter an IPv4 address in A.B.C.D format.
 - *ipv6-address* — Enter an IPv6 address in nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn format (elision of zeros is supported).
 - *key keyid* — Enter a text string as the key exchanged between the NTP server and the client.
 - *prefer* — Enter the keyword to set this NTP server as the preferred server.
5. Configure the NTP master and enter the stratum number that identifies the NTP server hierarchy in CONFIGURATION mode (2 to 10, default 8).

```
ntp master <2-10>
```

Configure NTP

```
OS10(config)# ntp authenticate
OS10(config)# ntp trusted-key 345
OS10(config)# ntp authentication-key 345 md5 0 5A60910FED211F02
OS10(config)# ntp server 1.1.1.1 key 345
OS10(config)# ntp master 7
```

View NTP configuration

```
OS10(config)# do show running-configuration
!
ntp authenticate
ntp authentication-key 345 md5 0 5A60910FED211F02
ntp server 1.1.1.1 key 345
ntp trusted-key 345
ntp master 7
...
```

NTP commands

ntp authenticate

Enables authentication of NTP traffic between the device and the NTP time serving hosts.

Syntax	<code>ntp authenticate</code>
Parameters	None
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	You must also configure an authentication key for NTP traffic using the <code>ntp authentication-key</code> command. The <code>no</code> version of this command disables NTP authentication.
Example	<pre>OS10(config)# ntp authenticate</pre>
Supported Releases	10.2.0E or later

ntp authenticate-key

Configures the authentication key for trusted time sources.

Syntax	<code>ntp authenticate-key <i>number</i> md5 [<i>0</i> <i>7</i>] <i>key</i></code>
Parameters	<ul style="list-style-type: none">• <i>number</i> — Enter the authentication key number (1 to 4294967295).• <code>md5</code> — Set to MD5 encryption.• <code>0</code> — Set to unencrypted format (default).• <code>7</code> — Set to hidden encryption.• <i>key</i> — Enter the authentication key.
Default	0
Command Mode	CONFIGURATION
Usage Information	The authentication number must be the same as the <code>number</code> parameter configured in the <code>ntp trusted-key</code> command. Use the <code>ntp authenticate</code> command to enable NTP authentication.
Example	<pre>OS10(config)# ntp authentication-key 1200 md5 0 dell</pre>

Supported Releases 10.2.0E or later

ntp broadcast client

Configures the interface to receive NTP broadcasts from an NTP server.

Syntax `ntp broadcast client`

Parameters None

Default Not configured

Command Mode INTERFACE

Usage Information The `no` version of this command disables broadcast.

Example

```
OS10(conf-if-eth1/1/1)# ntp broadcast client
```

Supported Releases 10.2.0E or later

ntp disable

By default, NTP is enabled on all interfaces. Prevents an interface from receiving NTP packets.

Syntax `ntp disable`

Parameters None

Default Enabled

Command Mode INTERFACE

Usage Information This command is used to configure OS10 to not listen to a particular server and prevents the interface from receiving NTP packets. The `no` version of this command re-enables NTP on an interface.

Example

```
OS10(conf-if-eth1/1/7)# ntp disable
```

Supported Releases 10.2.0E or later

ntp enable vrf management

Enables NTP for the management VRF instance.

Syntax `ntp enable vrf management`

Parameters None

Defaults Disabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables NTP for the management VRF instance.

Example

```
OS10(config)# ntp enable vrf management
```

Supported Releases 10.4.0E(R1) or later

ntp master

Configures an NTP master server.

Syntax `ntp master stratum`

Parameters `stratum` — Enter the stratum number to identify the NTP server hierarchy (2 to 10).

Default 8

Command Mode CONFIGURATION

Usage Information The `no` version of this command resets the value to the default.

Example

```
OS10(config)# ntp master 6
```

Supported Releases 10.2.0E or later

ntp server

Configures an NTP time-serving host.

Syntax `ntp server {hostname | ipv4-address | ipv6-address} [key keyid] [prefer]`

Parameters

- `hostname` — Enter the host name of the server.
- `ipv4-address | ipv6-address` — Enter the IPv4 address (A.B.C.D) or IPv6 address (A::B) of the NTP server.
- `key keyid` — (Optional) Enter the NTP peer key ID (1 to 4294967295).
- `prefer` — (Optional) Configures this peer to have priority over other servers.

Default Not configured

Command Mode CONFIGURATION

Usage Information You can configure multiple time-serving hosts. From these time-serving hosts, the system chooses one NTP host to synchronize with. To determine which server to select, use the `show ntp associations` command. Dell EMC recommends limiting the number of hosts you configure, as many polls to the NTP hosts can impact network performance.

Example

```
OS10(config)# ntp server eureka.com
```

Supported Releases 10.2.0E or later

ntp source

Configures an interface IP address to include in NTP packets.

Syntax `ntp source interface`

Parameters `interface` — Set the interface type:

- `ethernet node/slot/port[:subport]` — Enter the Ethernet interface information.
- `port-channel id-number` — Enter the port-channel number (1 to 128).
- `vlan vlan-id` — Enter the VLAN number (1 to 4093).
- `loopback loopback-id` — Enter the Loopback interface number (0 to 16383).
- `mgmt node/slot/port` — Enter the Management port interface information.

Default Not configured

Command Mode CONFIGURATION

Usage Information The no version of this command removes the configuration.

Example

```
OS10(config)# ntp source ethernet 1/1/24
```

Supported Releases 10.2.0E or later

ntp trusted-key

Sets a key to authenticate the system to which NTP synchronizes with.

Syntax ntp trusted-key *number*

Parameters *number* — Enter the trusted key ID (1 to 4294967295).

Default Not configured

Command Mode CONFIGURATION

Usage Information The *number* parameter must be the same number as the *number* parameter in the `ntp authentication-key` command. If you change the `ntp authentication-key` command, you must also change this command. The no version of this command removes the key.

Example

```
OS10(config)# ntp trusted-key 234567
```

Supported Releases 10.2.0E or later

show ntp associations

Displays the NTP master and peers.

Syntax show ntp associations [*vrf management*]

Parameters None

Default Not configured

Command Mode EXEC

Usage Information

- (none) — One or more of the following symbols displays:
 - * — Synchronized to this peer.
 - # — Almost synchronized to this peer.
 - + — Peer was selected for possible synchronization.
 - - — Peer is a candidate for selection.
 - ~ — Peer is statically configured.
- remote — Remote IP address of the NTP peer.
- ref clock — IP address of the remote peer's reference clock.
- st — Peer stratum (number of hops away from the external time source). 16 means that the NTP peer cannot reach the time source.
- when — Last time the device received an NTP packet.
- poll — Polling interval (in seconds).
- reach — Reachability to the peer (in octal bitstream).
- delay — Time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
- offset — Relative time of the NTP peer's clock to the network device clock (in milliseconds).
- disp — Dispersion.

Example

```
OS10# show ntp associations
remote      ref clock  st when poll reach delay  offset disp
```

```
=====
10.10.120.5 0.0.0.0      16 - 256      0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16      377 -0.08 -1499.9 104.16
172.31.1.33 0.0.0.0      16 - 256      0 0.00 0.000 16000.0
192.200.0.2 0.0.0.0      16 - 256      0 0.00 0.000 16000.0
=====
```

```
OS10# show ntp associations vrf management
remote      local      st      poll reach  delay      offset      disp
=====
*1.1.1.2    1.1.1.1    3      64      1      0.00027    0.000056    0.43309
=====
```

Supported Releases 10.2.0E or later

show ntp status

Displays NTP configuration information.

Syntax `show ntp status [vrf management]`

Parameters `status` — (Optional) View the NTP status.

Default Not configured

Command Mode EXEC

Usage Information Use this command to view NTP status information.

Example (Status)

```
OS10# show ntp status
system peer:      0.0.0.0
system peer mode: unspec
leap indicator:   11
stratum:          16
precision:        -22
root distance:    0.00000 s
root dispersion:  1.28647 s
reference ID:     [73.78.73.84]
reference time:   00000000.00000000 Mon, Jan 1 1900 0:00:00.000
system flags:    monitor ntp kernel stats
jitter:          0.000000 s
stability:        0.000 ppm
broadcastdelay:  0.000000 s
authdelay:       0.000000 s
```

```
OS10# show ntp status vrf management
system peer:      1.1.1.2
system peer mode: client
leap indicator:   00
stratum:          4
precision:        -23
root distance:    0.00027 s
root dispersion:  0.94948 s
reference ID:     [1.1.1.2]
reference time:   ddc78084.f17ea38b Tue, Nov 28 2017 6:28:20.943
system flags:    ntp kernel stats
jitter:          0.000000 s
stability:        0.000 ppm
broadcastdelay:  0.000000 s
authdelay:       0.000000 s
OS10#
```

Supported Releases 10.2.0E or later

System clock

OS10 uses NTP to synchronize the system clock with a time-serving host. If you do not use NTP, set the system time in EXEC mode. The hardware-based real-clock time (RTC) is reset to the new system time.

You can set the current time and date after you disable NTP. When NTP is enabled, it overwrites the system time.

- Enter the time and date in EXEC mode.

```
clock set time year-month-day
```

Enter *time* in the format *hour:minute:second*, where *hour* is 1 to 24; *minute* is 1 to 60; *second* is 1 to 60 (enter 5:15 PM as 17:15:00).

Enter *year-month-day* in the format YYYY-MM-DD, where YYYY is a four-digit year, such as 2016; MM is a month from 1 to 12; DD is a day from 1 to 31.

Set time and date

```
OS10# clock set 18:30:10 2017-01-25
```

View system time and date

```
OS10# show clock
2017-01-25T18:30:17.92+00:00
```

System Clock commands

clock set

Sets the system time.

Syntax	<code>clock set time year-month-day</code>
Parameters	<p>time Enter <i>time</i> in the format <i>hour:minute:second</i>, where <i>hour</i> is 1 to 24; <i>minute</i> is 1 to 60; <i>second</i> is 1 to 60. For example, enter 5:15 PM as 17:15:00.</p> <p>year-month-day Enter <i>year-month-day</i> in the format YYYY-MM-DD, where YYYY is a four-digit year, such as 2016; MM is a month from 1 to 12; DD is a day from 1 to 31.</p>
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to reset the system time if the system clock is out of synch with the NTP time. The hardware-based real-clock time (RTC) resets to the new time. The new system clock setting is applied immediately.
Example	<pre>OS10# clock set 18:30:10 2017-01-25</pre>
Supported Releases	10.2.1E or later

clock timezone

Sets the time zone used for the system clock.

Syntax	<code>clock timezone timezone-string Hours Minutes</code>
Parameters	<ul style="list-style-type: none">• Enter <i>timezone-string</i> which is the name of the time zone.• Enter <i>Hours</i> offset from UTC, ranging from -23 to 23.

- Enter *Minutes* offset from UTC, ranging from **0** to **59**.

Default Not configured

Command Mode CONFIGURATION

Usage Information Universal time coordinated (UTC) is the time standard based on Greenwich Mean time. To set the time zone for the system clock, enter the difference of hours between UTC and your time zone.

Example

```
OS10(config)# clock timezone IST 5 30
```

Supported Releases 10.3.0E or later

show clock

Displays the current system clock settings.

Syntax show clock

Parameters None

Default Not configured

Command Mode EXEC

Usage Information The universal time coordinated (UTC) value is the number of hours that your time zone is later than or earlier than UTC/Greenwich mean time.

Example

```
OS10# show clock
2017-01-25T11:00:31.68-08:00
```

Supported Releases 10.2.1E or later

System banners

You can configure a system login and message of the day (MOTD) text banners. The system login banner displays before you log in. The MOTD banner displays immediately after a successful login.

You can reset the banner text to the Dell EMC default banner or disable the banner display.

Login banner

Configure a system login banner that displays before you log in using interactive mode. Starting and ending double-quotes are not necessary. Enter a single delimiter character or the key combination `^C` to specify the start and end of the text banner.

1. Enter the `banner login delimiter` command with a single delimiter character and press **Enter**.
2. Enter each line of text and press **Enter**. Enter a maximum of 4096 characters. There is no limit to the number of lines.
3. Complete the banner configuration by entering a line that contains only the delimiter character.

- Enable a login banner in CONFIGURATION mode. Enclose the delimiters and banner text in double-quotes.

```
banner login delimiter <Enter>
banner-text <Enter>
banner-text <Enter>
... <Enter>
delimiter
```

Configure login banner

```
OS10(config)# banner login %
DellEMC S4148U-ON login
```

```
Enter your username and password
%
```

To delete a login banner and reset it to the Dell EMC default banner, enter the `no banner login` command. To disable banner display before login, enter the `banner login disable` command.

MOTD banner

Configure a message of the day banner that displays after you log in. Enter up to 4096 characters. To start and end the MOTD banner, enter a single delimiter character or the key combination `^C`. You can enter any character as the delimiter.

To enter a MOTD banner text, use the interactive mode. Enter the command with the delimiter character and press **Enter**. Then enter each line and press **Enter**. Complete the banner configuration by entering a line that contains only the delimiter character. Starting and ending double-quotes are not necessary.

Configure MOTD banner

```
OS10(config)# banner motd %
DellEMC S4148U-ON
Today's tip: Press tab or spacebar for command completion.
Have a nice day!
%
```

To delete a MOTD banner and reset it to the Dell EMC default MOTD banner, enter the `no banner motd` command. To disable MOTD banner display after login, enter the `banner motd disable` command.

System banner commands

banner login

Configures a login banner that displays before you log in to the system.

Syntax

```
banner login delimiter <Enter>
banner-text <Enter>
banner-text <Enter>
... <Enter>
delimiter
```

Parameters

- *delimiter* — Enter a single delimiter character or the key combination `^C` to specify the start and end of the text banner.
- *banner-text* — Enter a maximum of 4096 characters. There is no limit to the number of lines.

Default

The Dell EMC default banner is displayed before you log in.

Command Mode

CONFIGURATION

Usage Information

- To enter multiline banner text, use the interactive mode. Enter the command with the delimiter character and press **Enter**. Then enter each line and press **Enter**. Complete the banner configuration by entering a line that contains only the delimiter character. Starting and ending double-quotes are not necessary.
- To delete a login banner and reset it to the Dell EMC default banner, enter the `no banner login` command. To disable banner display before login, enter the `banner login disable` command.

Example

```
OS10(config)# banner login %
Welcome to DellEMC Z9100-ON
Enter your username and password
%
```

Supported Releases

10.4.1.0 or later

banner motd

Configures a multi-line message of the day banner that displays after you log in.

Syntax

```
banner motd delimiter <Enter>
banner-text <Enter>
banner-text <Enter>
... <Enter>
delimiter
```

Parameters

- *delimiter* — Enter a single delimiter character or the key combination ^C to specify the start and end of the text banner.
- *banner-text* — Enter a maximum of 4096 characters. There is no limit on the number of lines.

Default

The Dell EMC default MOTD banner is displayed after you log in.

Command Mode

CONFIGURATION

Usage Information

- To enter a MOTD banner text, use the interactive mode. Enter the command with the delimiter character and press **Enter**. Then enter each line and press **Enter**. Complete the banner configuration by entering a line that contains only the delimiter character. Starting and ending double-quotes are not necessary.
- To delete a login banner and reset it to the Dell EMC default banner, enter the `no banner motd` command. To disable banner display before login, enter the `banner motd disable` command.

Example

```
OS10(config)# banner motd %
DellEMC S4148U-ON
Today's tip: Press tab or spacebar for command completion.
Have a nice day!
%
```

Supported releases

10.4.1.0 or later

User session management

You can manage the active user sessions using the following commands:

- Configure the timeout for all the active user sessions using `exec-timeout timeout-value` in the CONFIGURATION mode.
- Clear any user session using `kill-session session-ID` in the EXEC mode.
- View the active user sessions using `show sessions` in the EXEC mode.

Configure timeout for user sessions

```
OS10(config)# exec-timeout 300
OS10(config)#
```

Clear user session

```
OS10# kill-session 3
```

View active user sessions

```
OS10# show sessions

Current session's operation mode: Non-transaction

Session-ID User      In-rpcs In-bad-rpcs Out-rpc-err Out-notify Login-time
Lock
-----
--
3          snmp_user 114      0           0           0           2017-07-10T23:58:39Z
4          snmp_user 57       0           0           0           2017-07-10T23:58:40Z
```


6	admin	17	0	0	4	2017-07-12T03:55:18Z
*7	admin	10	0	0	0	2017-07-12T04:42:55Z
OS10#						

User session management commands

exec-timeout

Configure timeout in seconds for all the user sessions.

Syntax	<code>exec-timeout <i>timeout-value</i></code>
Parameters	<i>timeout-value</i> — Enter the timeout value in seconds (0 to 3600).
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The no version of this command disables the timeout.
Example	

```
OS10(config)# exec-timeout 300
OS10(config)#
```

Supported Releases 10.3.1E or later

kill-session

Terminate a user session.

Syntax	<code>kill-session <i>session-ID</i></code>
Parameters	<i>session-ID</i> — Enter the user session ID.
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	

```
OS10# kill-session 3
```

Supported Releases 10.3.1E or later

show sessions

Displays the active management sessions.

Syntax	<code>show sessions</code>
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	Use this command to view information about the active user management sessions.

Example

```
OS10# show sessions

Current session's operation mode: Non-transaction

Session-ID User          In-rpcs In-bad-rpcs Out-rpc-err Out-notify Login-time          Lock
-----
3          snmp_user 114      0           0           0           2017-07-10T23:58:39Z
4          snmp_user 57       0           0           0           2017-07-10T23:58:40Z
6          admin    17       0           0           4           2017-07-12T03:55:18Z
*7         admin    10       0           0           0           2017-07-12T04:42:55Z
OS10#
```

Supported Releases 10.3.1E or later

Telnet server

To allow Telnet TCP/IP connections to an OS10 switch, enable the Telnet server. The OS10 Telnet server uses the Debian `telnetd` package. By default, the Telnet server is disabled.

When the Telnet server is enabled, connect to the switch using the IP address configured on the management or any front-panel port. The Telnet server configuration is persistent and is maintained after you reload the switch. To verify the Telnet server configuration, enter the `show running-configuration` command.

Enable Telnet server

```
OS10(config)# ip telnet server enable
```

Disable Telnet server

```
OS10(config)# no ip telnet server enable
```

By default, the Telnet server is disabled on the default VRF. To configure the Telnet server to be reachable on the management VRF, use the `ip telnet server vrf management` command.

Configure Telnet server on management VRF

```
OS10(config)# ip telnet server vrf management
```

Telnet commands

ip telnet server enable

Enables Telnet TCP/IP connections to an OS10 switch.

Syntax `ip telnet server enable`

Parameters None

Default Disabled

Command Mode CONFIGURATION

Usage Information By default, the Telnet server is disabled. When you enable the Telnet server, use the IP address configured on the management or any front-panel port to connect to an OS10 switch. After you reload the switch, the Telnet server configuration is maintained. To verify the Telnet server configuration, enter the `show running-configuration` command.

Example

```
OS10(config)# ip telnet server enable
```

Example (disable)

```
OS10(config)# no ip telnet server enable
```

Supported Releases 10.4.0E(R1) or later

ip telnet server vrf

Configures the Telnet server for the management VRF instance.

Syntax `ip telnet server vrf management`

Parameters

- `management` — Configures the management VRF to be used to reach the Telnet server.

Default The Telnet server is reachable on the default VRF.

Command Mode CONFIGURATION

Usage Information By default, the Telnet server is disabled. To enable the Telnet server, enter the `telnet enable` command. To configure the Telnet server to be reachable on the management VRF instance, use the `ip telnet server vrf management` command.

Example

```
OS10(config)# ip telnet server vrf management
```

Supported Releases 10.4.0E(R1) or later

Security

Authentication, authorization, and accounting (AAA) services secure networks against unauthorized access. In addition to local authentication, OS10 supports remote authentication dial-in user service (RADIUS) and terminal access controller access control system (TACACS+) client/server authentication systems. For RADIUS and TACACS+, an OS10 switch acts as a client and sends authentication requests to a server that contains all user authentication and network service access information.

A RADIUS or TACACS+ server provides authentication (user credentials verification), authorization (role-based permissions), and accounting services. You can configure the security protocol used for different login methods and users. RADIUS provides very limited authorization and accounting services compared to TACACS+.

An OS10 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 configured.

The authentication methods in the method list are executed in the order in which they are configured. You can re-enter the methods to change the order. The `local` authentication method remains enabled even if you remove all configured methods in the list (`no aaa authentication login {console | default}` command).

- Configure the AAA authentication method in CONFIGURATION mode.

```
aaa authentication login {console | default} {local | group radius | group tacacs+}
```

- `console` — Configure authentication methods for console logins.
- `default` — Configure authentication methods for non-console (SSH and Telnet) logins.
- `local` — Use the local username, password, and role entries configured with the `username password role` command.
- `group radius` — Use the RADIUS servers configured with the `radius-server host` command.
- `group tacacs+` — Use the TACACS+ servers configured with the `tacacs-server host` command.

Configure user role on server

If a console user logs in with RADIUS or TACACS+ authentication, the role you configured for the user on the RADIUS or TACACS+ server is applied. User authentication fails if no role is configured on the authentication server.

In addition, you must configure the user role on the RADIUS or TACACS+ server using the vendor-specific attribute (VSA) or the authentication fails. Dell's vendor ID is 674. You create a VSA with `Name = Dell-group-name`, `OID = 2`, `Type = string`. Valid values for `Dell-group-name` are `sysadmin`, `secadmin`, `netadmin`, and `netoperator`. Use the VSA `Dell-group-name` values when you create users on a Radius or TACACS+ server.

For detailed information about how to configure vendor-specific attributes on a RADIUS or TACACS+ server, refer to the respective RADIUS or TACACS+ server documentation.

Configure AAA authentication

```
OS10(config)# aaa authentication login default group radius local
OS10(config)# do show running-configuration aaa
aaa authentication login default group radius local
aaa authentication login console local
```

Remove AAA authentication methods

```
OS10(config)# no aaa authentication login default
OS10(config)# do show running-configuration aaa
aaa authentication login default local
aaa authentication login console local
```

User re-authentication

To prevent users from accessing resources and performing tasks for which they are not authorized, OS10 allows you to require users to re-authenticate by logging in again when an authentication method or server changes, such as:

- Adding or removing a RADIUS server (`radius-server host` command)
- Adding or removing an authentication method (`aaa authentication login {console | default} {local | group radius | group tacacs+}` command)

You can enable this feature so that user re-authentication is required when any of these actions are performed. In these cases, logged-in users are logged out of the switch and all OS10 sessions are terminated. By default, user re-authentication is disabled.

Enable user re-authentication

- Enable user re-authentication in CONFIGURATION mode.

```
aaa re-authenticate enable
```

Enter the `no` form of the command to disable user re-authentication.

Password strength

By default, the password you configure with the `username password` command must be at least nine alphanumeric characters.

To increase password strength, you can create password rules using the `password-attributes` command. When you enter the command, at least one parameter is required. When you enter the `character-restriction` parameter, at least one option is required.

- Create rules for stronger passwords in CONFIGURATION mode.

```
password-attributes {[min-length number] [character-restriction {[upper number]
[lower number][numeric number] [special-char number]}}
```

- `min-length number` — Enter the minimum number of required alphanumeric characters (6 to 32; default 9).
- `character-restriction` — Enter a requirement for the alphanumeric characters in a password:
 - `upper number` — Minimum number of uppercase characters required (0 to 31; default 0).
 - `lower number` — Minimum number of lowercase characters required (0 to 31; default 0).
 - `numeric number` — Minimum number of numeric characters required (0 to 31; default 0).
 - `special-char number` — Minimum number of special characters required (0 to 31; default 0).

Create password rules

```
OS10(config)# password-attributes min-length 7 character-restriction upper 4 numeric 2
```

Display password rules

```
OS10(config)# do show running-configuration password-attributes
password-attributes min-length 7 character-restriction upper 4 numeric 2
```

Role-based access control

RBAC provides control for access and authorization. Users are granted permissions based on defined roles — not on their individual system user ID. Create user roles based on job functions to help users perform their associated job function. You can assign each user only a single role, and many users can have the same role. A user role authenticates and authorizes a user at login, and places you in EXEC mode (see [CLI basics](#)).

OS10 supports four pre-defined roles: `sysadmin`, `secadmin`, `netadmin`, and `netoperator`. Each user role assigns permissions that determine the commands a user can enter, and the actions a user can perform. RBAC provides an easy and efficient way to administer user rights. If a user's role matches one of the allowed user roles for a command, command authorization is granted.

The OS10 RBAC model provides separation of duty as well as greater security. It places some limitations on each role's permissions to allow you to partition tasks. For greater security, only some user roles can view events, audits, and security system logs.

Assign user role

To limit OS10 system access, assign a role when you configure each user.

- Enter a user name, password, and role in CONFIGURATION mode.

```
username username password password role role
```

- `username username` — Enter a text string (up to 32 alphanumeric characters; 1 character minimum).
- `password password` — Enter a text string (up to 32 alphanumeric characters; 9 characters minimum).
- `role role` — Enter a user role:
 - `sysadmin` — Full access to all commands in the system, exclusive access to commands that manipulate the file system, and access to the system shell. A system administrator can create user IDs and user roles.
 - `secadmin` — Full access to configuration commands that set security policy and system access, such as password strength, AAA authorization, and cryptographic keys. A security administrator can display security information, such as cryptographic keys, login statistics, and log information.
 - `netadmin` — Full access to configuration commands that manage traffic flowing through the switch, such as routes, interfaces, and ACLs. A network administrator cannot access configuration commands for security features or view security information.
 - `netoperator` — Access to EXEC mode to view the current configuration. A network operator cannot modify any configuration setting on a switch.

Create user and assign role

```
OS10(config)# username smith password silver403! newuser role sysadmin
```

View users

```
OS10# show users
```

Index	Line	User	Role	Application	Idle	Login-Time	Location
1	ttyS	root	root	-bash	>24h	2018-05-23 T23:05:03Z	console
2	pts/0	admin	sysadmin	bash	1.1s	2018-05-30 T20:04:27Z	10.14.1.214[ssh]

RADIUS authentication

To configure a RADIUS server for authentication, enter the server's IP address or host name, and the key used to authenticate the OS10 switch on a RADIUS host. You can enter the authentication key in plain text or encrypted format. You can change the UDP port number on the server.

- Configure a RADIUS authentication server in CONFIGURATION mode. By default, a RADIUS server uses UDP port 1812.

```
radius-server host {hostname | ip-address} key {0 authentication-key | 9  
authentication-key | authentication-key} [auth-port port-number]
```

Re-enter the `radius-server host` command multiple times to configure more than one RADIUS server. If you configure multiple RADIUS servers, OS10 attempts to connect in the order you configured them. An OS10 switch connects with the configured RADIUS servers one at a time, until a RADIUS server responds with an accept or reject response. The switch tries to connect with a server for the configured number of retransmit retries and timeout period.

Configure global settings for the timeout and retransmit attempts allowed on RADIUS servers by using the `radius-server retransmit` and `radius-server timeout` commands. By default, OS10 supports three RADIUS authentication attempts and times out after five seconds.

- Configure the number of times OS10 retransmits a RADIUS authentication request in CONFIGURATION mode (0 to 100 retries; default 3).

```
radius-server retransmit retries
```

- Configure the timeout period used to wait for an authentication response from a RADIUS server in CONFIGURATION mode (0 to 1000 seconds; default 5).

```
radius-server timeout seconds
```

Configure RADIUS server

```
OS10(config)# radius-server host 1.2.4.5
OS10(config)# radius-server retransmit 10
OS10(config)# radius-server timeout 10
```

View RADIUS server configuration

```
OS10# show running-configuration
...
radius-server host 1.2.4.5 key 9
3a95c26b2a5b96a6b80036839f296babe03560f4b0b7220d6454b3e71bdfc59b
radius-server retransmit 10
radius-server timeout 10
...
```

Delete RADIUS server

```
OS10# no radius server host 1.2.4.5
```

TACACS+ authentication

Configure a TACACS+ authentication server by entering the server's IP address or host name. You must also enter a text string for the key used to authenticate the OS10 switch on a TACACS+ host. The TCP port entry is optional.

TACACS+ provides greater data security by encrypting the entire protocol portion in a packet sent from the switch to an authentication server. RADIUS encrypts only passwords.

- Configure a TACACS+ authentication server in CONFIGURATION mode. By default, a TACACS+ server uses TCP port 49 for authentication.

```
tacacs-server host {hostname | ip-address} key {0 authentication-key | 9
authentication-key | authentication-key} [auth-port port-number]
```

Re-enter the `tacacs-server host` command multiple times to configure more than one TACACS+ server. If you configure multiple TACACS+ servers, OS10 attempts to connect in the order you configured them. An OS10 switch connects with the configured TACACS+ servers one at a time, until a TACACS+ server responds with an accept or reject response.

Configure the global timeout used on all TACACS+ servers by using the `tacacs-server timeout` command. By default, OS10 times out an authentication attempt on a TACACS+ server after five seconds.

- Enter the timeout value used to wait for an authentication response from TACACS+ servers in CONFIGURATION mode (1 to 1000 seconds; default 5).

```
tacacs-server timeout seconds
```

Configure TACACS+ server

```
OS10(config)# tacacs-server host 1.2.4.5 key mysecret
```

View TACACS+ server configuration

```
OS10# show running-configuration
...
tacacs-server host 1.2.4.5 key 9
3a95c26b2a5b96a6b80036839f296babe03560f4b0b7220d6454b3e71bdfc59b
...
```

Delete TACACS+ server

```
OS10# no tacacs server host 1.2.4.5
```

TACACS+ unknown or missing user role

When a TACACS+ server authenticates a user and does not return a role or returns an unknown role, OS10 assigns the `netoperator` role to the authenticated user by default. You can reconfigure the default `netoperator` role.

- Enter an OS10 user role in CONFIGURATION mode.

```
userrole default inherit existing-role-name
```

- *existing-role-name* — Enter a user role:
 - `sysadmin` — Full access to all commands in the system, exclusive access to commands that manipulate the file system, and access to the system shell. A system administrator can create user IDs and user roles.
 - `secadmin` — Full access to configuration commands that set security policy and system access, such as password strength, AAA authorization, and cryptographic keys. A security administrator can display security information, such as cryptographic keys, login statistics, and log information.
 - `netadmin` — Full access to configuration commands that manage traffic flowing through the switch, such as routes, interfaces, and ACLs. A network administrator cannot access configuration commands for security features or view security information.
 - `netoperator` — Access to EXEC mode to view the current configuration. A network operator cannot modify any configuration setting on a switch.

Reconfigure the default user role

```
OS10(config)# userrole default inherit sysadmin
```

SSH server

In OS10, the secure shell (SSH) server allows an SSH client to access an OS10 switch through a secure, encrypted connection. The SSH server authenticates remote clients using RADIUS challenge/response, a trusted host file, locally-stored passwords, and public keys.

Configure SSH server

- The SSH server is enabled by default. You can disable the SSH server using `no ip ssh server enable`.
- Challenge response authentication is disabled by default. To enable, use the `ip ssh server challenge-response-authentication` command.
- Host-based authentication is disabled by default. To enable, use the `ip ssh server hostbased-authentication` command.
- Password authentication is enabled by default. To disable, use the `no ip ssh server password-authentication` command.
- Public key authentication is enabled by default. To disable, use the `no ip ssh server pubkey-authentication` command.
- Password-less login is disabled by default. To enable, use the `username sshkey` or `username sshkey filename` commands.
- Configure the list of cipher algorithms using `ip ssh server cipher cipher-list`.

- Configure Key Exchange algorithms using `ip ssh server kex key-exchange-algorithm`.
- Configure hash message authentication code (HMAC) algorithms using `ip ssh server mac hmac-algorithm`.
- Configure the SSH server listening port using `ip ssh server port port-number`.
- Configure the SSH server to be reachable on the management VRF using `ip ssh server vrf`.
- Configure the SSH login timeout using the `ip ssh server login-grace-time seconds` command (0 to 300; default 60). To reset the default SSH prompt timer, enter `no ip ssh server login-grace-time`.
- Configure the maximum number of authentication attempts using the `ip ssh server max-auth-tries number` command (0 to 10; default 6). To reset the default, enter `no ip ssh server max-auth-tries`.

The `max-auth-tries` value includes all authentication attempts, including public-key and password. If both public-key based authentication and password authentication are enabled, the public-key authentication is the default and is tried first. If it fails, the number of `max-auth-tries` is reduced by one. In this case, if you configured `ip ssh server max-auth-tries 1`, the password prompt does not display.

Regenerate public keys

When enabled, the SSH server generates public keys by default and uses them for client authentication:

- A Rivest, Shamir, and Adelman (RSA) key using 2048 bits.
- An Elliptic Curve Digital Signature Algorithm (ECDSA) key using 256 bits
- An Ed25519 key using 256 bits

NOTE: RSA1 and DSA keys are not supported on the OS10 SSH server.

An SSH client must exchange the same public key to establish a secure SSH connection to the OS10 switch. If necessary, you can regenerate the keys used by the SSH server with a customized bit size. You cannot change the default size of the Ed25519 key. The `crypto key generate` command is available only to the `sysadmin` and `secadmin` roles.

1. Regenerate key for the SSH server in EXEC mode.

```
crypto ssh-key generate {rsa {2048|3072|4096} | ecdsa {256|384|521} | ed25519}
```

2. Enter `yes` at the prompt to overwrite an existing key.

```
Host key already exists. Overwrite [confirm yes/no]:yes
Generated 2048-bit RSA key
```

3. Display the SSH public keys in EXEC mode.

```
show crypto ssh-key
```

After you regenerate SSH server keys, disable and re-enable the SSH server to use the new keys. Restarting the SSH server does not impact current OS10 sessions.

Virtual terminal line

Virtual terminal line (VTY) is used to control Telnet or SSH connections to the switch.

You can enter the VTY mode by using the `line vty` command in the CONFIGURATION mode.

```
OS10(config)# line vty
OS10(config-line-vty)#
```

Control access to VTY

You can control the Telnet or SSH connections to the switch by applying access lists on VTY lines.

Create IP or IPv6 access lists with `permit` or `deny` filters.

Enter the VTY mode by using the `line vty` command in the CONFIGURATION mode.

Apply the access lists to the VTY line with the `{ip | ipv6} access-class access-list-name` command.

Example

```
OS10(config)# ip access-list permit10
OS10(config-ipv4-acl)# permit ip 172.16.0.0 255.255.0.0 any
```



```
OS10(config-ipv4-acl)# exit
OS10(config)# line vty
OS10(config-line-vty)# ip access-class permit10
OS10(config-line-vty)#
```

View VTY ACL configuration

```
OS10(config-line-vty)# show configuration
!
line vty
 ip access-class permit10
 ipv6 access-class deny10
OS10(config-line-vty)#
```

Enable AAA accounting

To record information about all user-entered commands, use the AAA accounting feature — not supported for RADIUS accounting. AAA accounting records login and command information in OS10 sessions on console connections (`console` option) and remote connections (`default` option), such as Telnet and SSH.

AAA accounting sends accounting messages:

- Sends a start notice when a process begins, and a stop notice when the process ends (`start-stop` option)
- Sends only a stop notice when a process ends (`stop-only` option)
- No accounting notices are sent (`none` option)
- Logs all accounting notices in syslog (`logging` option)
- Logs all accounting notices on configured TACACS+ servers (`group tacacs+` option)

Enable AAA accounting

- Enable AAA accounting in CONFIGURATION mode.

```
aaa accounting commands all {console | default} {start-stop | stop-only | none}
[logging] [group tacacs+]
```

Enter the `no` form of the command to disable AAA accounting.

Enable user lockout

By default, a maximum of three consecutive failed password attempts is supported on the switch. You can set a limit to the maximum number of allowed password retries with a specified lockout period for the user ID.

This feature is available only for the `sysadmin` and `secadmin` roles.

- Configure user lockout settings in CONFIGURATION mode.

```
password-attributes {[max-retry number ] [lockout-period minutes] }
```

- `max-retry number` — Sets the maximum number of consecutive failed login attempts for a user before the user is locked out (0 to 16; default 3).
- `lockout-period minutes` — Sets the amount of time that a user ID is prevented from accessing the system after exceeding the maximum number of failed login attempts (0 to 43,200; default 0).

When a user is locked out due to exceeding the maximum number of failed login attempts, other users can still access the switch.

By default, `lockout-period minutes` is 0; no lockout period is configured. Failed login attempts do not lock out a user.

Configure user lockout

```
OS10(config)# password-attributes max-retry 4 lockout period 360
```

Limit concurrent login sessions

To avoid an unlimited number of active sessions on a switch for the same user ID, you can limit the number of console and remote connections. Log in from a console connection by cabling a terminal emulator to the console serial port on the switch. Log in to the switch remotely through a virtual terminal line (VTY), such as Telnet and SSH.

- Configure the maximum number of concurrent login sessions in CONFIGURATION mode.

```
OS10(config)# login concurrent-session limit number
```

- *limit number* — Sets the maximum number of concurrent login sessions allowed for a user ID (1 to 12; default 10).

When you configure the maximum number of allowed concurrent login sessions, take into account that:

- Each remote VTY connection counts as one login session.
- All login sessions from a terminal emulator on an attached console count as one session.

Configure concurrent login sessions

```
OS10(config)# login concurrent-session limit 4
```

If you log in to the switch after the maximum number of concurrent sessions are active, an error message displays. To log in to the system, close one of your existing sessions.

```
OS10(config)# login concurrent-session limit 4

Too many logins for 'admin'.
Last login: Wed Jan 31 20:37:34 2018 from 10.14.1.213
Connection to 10.11.178.26 closed.
Current sessions for user admin:
Line      Location
2 vty 0    10.14.1.97
3 vty 1    10.14.1.97
4 vty 2    10.14.1.97
5 vty 3    10.14.1.97
```

Enable login statistics

To monitor system security, allow users to view their own login statistics when they sign in to the system. A large number of login failures or an unusual login location may indicate a system hacker. Enable the display of login information after a user successfully logs in; for example:

```
OS10 login: admin
Password:
Last login: Thu Nov  2 16:02:44 UTC 2017 on ttyS1
Linux OS10 3.16.43 #2 SMP Debian 3.16.43-2+deb8u5 x86_64
...
Time-frame for statistics      : 25 days
Role changed since last login : false
Failures since last login     : 0
Failures in time period       : 1
Successes in time period      : 14
OS10#
```

This feature is available only for the `sysadmin` and `secadmin` roles.

- Enable the display of login information in CONFIGURATION mode.

```
login-statistics enable
```

To display information about user logins, enter the `show login-statistics` command.

Enable login statistics

```
OS10(config)# login-statistics enable
```

To disable login statistics, enter the `no login-statistics enable` command.

Security commands

aaa accounting

Enables AAA accounting.

Syntax	<code>aaa accounting commands all {console default} {start-stop stop-only none} [logging] [group tacacs+]</code>
Parameters	<ul style="list-style-type: none">• <code>commands all</code> — Record all user-entered commands. This option is not supported for RADIUS accounting.• <code>console</code> — Record all user authentication and logins or all user-entered commands in OS10 sessions on console connections.• <code>default</code> — Record all user authentication and logins or all user-entered commands in OS10 sessions on remote connections; for example, Telnet and SSH.• <code>start-stop</code> — Send a start notice when a process begins, and a stop notice when the process ends.• <code>stop-only</code> — Send only a stop notice when a process ends.• <code>none</code> — No accounting notices are sent.• <code>logging</code> — Logs all accounting notices in syslog.• <code>group tacacs+</code> — Logs all accounting notices on the first reachable TACACS+ server.
Default	AAA accounting is disabled.
Command Mode	CONFIGURATION
Usage Information	You can enable the recording of accounting events in both the syslog and on TACACS+ servers. The <code>no</code> version of the command disables AAA accounting.
Example	<pre>OS10(config)# aaa accounting commands all console start-stop logging group tacacs+</pre>
Supported Releases	10.4.1.0 or later

aaa authentication login

Configures the AAA authentication method used for console, and SSH and Telnet logins.

Syntax	<code>aaa authentication login {console default} {local group radius group tacacs+}</code>
Parameters	<ul style="list-style-type: none">• <code>console</code> — Configure authentication methods for console logins.• <code>default</code> — Configure authentication methods for SSH and Telnet logins.• <code>local</code> — Use the local username, password, and role entries configured with the <code>username password role</code> command.• <code>group radius</code> — Use the RADIUS servers configured with the <code>radius-server host</code> command.• <code>group tacacs+</code> — Use the TACACS+ servers configured with the <code>tacacs-server host</code> command.
Default	Local authentication
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes all configured authentication methods and defaults to using local authentication.
Example	<pre>OS10(config)# aaa authentication login default group radius local OS10(config)# do show running-configuration aaa</pre>

```
aaa authentication login default group radius local
aaa authentication login console local
```

```
OS10(config)# no aaa authentication login default
OS10(config)# do show running-configuration aaa
aaa authentication login default local
aaa authentication login console local
```

Supported Releases 10.4.1.0 or later

aaa re-authenticate enable

Requires user re-authentication after a change in the authentication method or server.

Syntax `aaa re-authenticate enable`

Parameters None

Default Disabled

Command Mode EXEC

Usage Information

- After you enable user re-authentication and change the authentication method or server, users are logged out of the switch and are prompted to log in again to re-authenticate. User re-authentication is triggered by:
 - Adding or removing a RADIUS server as a configured server host (`radius-server host` command)
 - Adding or removing an authentication method (`aaa authentication [local | radius]` command)
- The `no` version of the command disables user re-authentication.

Example

```
OS10(config)# aaa re-authenticate enable
```

Supported Releases 10.4.0E(R1) or later

crypto ssh-key generate

Regenerate public keys used in SSH authentication.

Syntax `crypto ssh-key generate {rsa bits | ecdsa bits | ed25519}`

Parameters

- `rsa bits` — Regenerates the RSA key with the specified bit size (2048, 3072, or 4096; default 2048).
- `ecdsa bits` — Regenerates the ECDSA key with the specified bit size (256, 384, or 521; default 256).
- `ed25519` — Regenerates the Ed25519 key with the default bit size.

Default The SSH server uses default public key lengths for client authentication:

- RSA key: 2048 bits
- ECDSA key : 256 bits
- Ed25519 key: 256 bits

Command Mode EXEC

Usage Information If necessary, you can regenerate the public keys used by the SSH server with a customized bit size. You cannot change the default size of the Ed25519 key. The `crypto ssh-key generate` command is available only to the `sysadmin` and `secadmin` roles.

Example

```
OS10# crypto ssh-key generate rsa 4096
Host key already exists. Overwrite [confirm yes/no]:yes
```

```
Generated 4096-bit RSA key
OS10#
```

Supported Releases 10.4.1.0 or later

ip access-class

Filters connections based on an IPv4 access list in virtual terminal line.

Syntax `ip access-class access-list-name`

Parameters `access-list-name`—Enter the access list name.

Default Not configured

Command Mode LINE VTY CONFIGURATION

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# line vty
OS10(config-line-vty)# ip access-class deny10
```

Supported Releases 10.4.0E(R1) or later

ipv6 access-class

Filters connections based on an IPv6 access list in virtual terminal line.

Syntax `ipv6 access-class access-list-name`

Parameters `access-list-name`—Enter the access list name.

Default Not configured

Command Mode LINE VTY CONFIGURATION

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# line vty
OS10(config-line-vty)# ipv6 access-class permit10
```

Supported Releases 10.4.0E(R1) or later

ip ssh server challenge-response-authentication

Enable challenge response authentication in an SSH server.

Syntax `ip ssh server challenge-response-authentication`

Parameters None

Default Disabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables the challenge response authentication.

Example

```
OS10(config)# ip ssh server challenge-response-authentication
```

Supported Releases

10.3.0E or later

ip ssh server cipher

Configure the list of cipher algorithms in the SSH server.

Syntax

```
ip ssh server cipher cipher-list
```

Parameters

cipher-list — Enter the list of cipher algorithms separated by space. The following is the list of cipher algorithms supported by the SSH server:

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com
- blowfish-cbc
- cast128-cbc
- chacha20-poly1305@opens

Default

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com
- chacha20-poly1305@opens

Command Mode

CONFIGURATION

Usage Information

The `no` version of this command removes the configuration.

Example

```
OS10(config)# ip ssh server cipher 3des-cbc aes128-cbc
```

Supported Releases

10.3.0E or later

ip ssh server enable

Enable the SSH server.

Syntax

```
ip ssh server enable
```

Parameters

None

Default

Enabled

Command Mode

CONFIGURATION

Usage Information

The `no` version of this command disables the SSH server.

Example

```
OS10(config)# ip ssh server enable
```

Supported Releases 10.3.0E or later

ip ssh server hostbased-authentication

Enable host-based authentication in an SSH server.

Syntax `ip ssh server hostbased-authentication`

Parameters None

Default Disabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables the host-based authentication.

Example

```
OS10(config)# ip ssh server hostbased-authentication
```

Supported Releases 10.3.0E or later

ip ssh server kex

Configure the list of Key Exchange algorithms in the SSH server.

Syntax `ip ssh server kex key-exchange-algorithm`

Parameters *key-exchange-algorithm* — Enter the list of Key Exchange algorithms separated by space. The following is the list of Key Exchange algorithms supported by the SSH server:

- curve25519-sha256
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Default

- curve25519-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the configuration.

Example

```
OS10(config)# ip ssh server kex curve25519-sha256 diffie-hellman-group1-sha1
```

Supported Releases 10.3.0E or later

ip ssh server mac

Configure the list of hash message authentication code (HMAC) algorithms in the SSH server.

Syntax	<code>ip ssh server mac <i>hmac-algorithm</i></code>
Parameters	<i>hmac-algorithm</i> — Enter the list of HMAC algorithms separated by space. The following is the list of HMAC algorithms supported by the SSH server: <ul style="list-style-type: none">• hmac-md5• hmac-md5-96• hmac-ripemd160• hmac-sha1• hmac-sha1-96• hmac-sha2-256• hmac-sha2-512• umac-64@openssh.com• umac-128@openssh.com• hmac-md5-etm@openssh.com• hmac-md5-96-etm@openssh.com• hmac-ripemd160-etm@openssh.com• hmac-sha1-etm@openssh.com• hmac-sha1-96-etm@openssh.com• hmac-sha2-256-etm@openssh.com• hmac-sha2-512-etm@openssh.com• umac-64-etm@openssh.com• umac-128-etm@openssh.com
Default	<ul style="list-style-type: none">• hmac-sha1• hmac-sha2-256• hmac-sha2-512• umac-64@openssh.com• umac-128@openssh.com• hmac-sha1-etm@openssh.com• hmac-sha2-256-etm@openssh.com• hmac-sha2-512-etm@openssh.com• umac-64-etm@openssh.com• umac-128-etm@openssh.com
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the configuration.
Example	<pre>OS10(config)# ip ssh server mac hmac-md5 hmac-md5-96 hmac-ripemd160</pre>
Supported Releases	10.3.0E or later

ip ssh server password-authentication

Enable password authentication in an SSH server.

Syntax	<code>ip ssh server password-authentication</code>
Parameters	None
Default	Enabled
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command disables the password authentication.

Example

```
OS10(config)# ip ssh server password-authentication
```

Supported Releases

10.3.0E or later

ip ssh server port

Configure the SSH server listening port.

Syntax

```
ip ssh server port port-number
```

Parameters

port-number — Enter the listening port number (1 to 65535).

Default

22

Command Mode

CONFIGURATION

Usage Information

The `no` version of this command removes the configuration.

Example

```
OS10(config)# ip ssh server port 255
```

Supported Releases

10.3.0E or later

ip ssh server pubkey-authentication

Enable public key authentication in an SSH server.

Syntax

```
ip ssh server pubkey-authentication
```

Parameters

None

Default

Enabled

Command Mode

CONFIGURATION

Usage Information

The `no` version of this command disables the public key authentication.

Example

```
OS10(config)# ip ssh server pubkey-authentication
```

Supported Releases

10.3.0E or later

ip ssh server vrf

Configures the SSH server for the management VRF instance.

Syntax

```
ip ssh server vrf management
```

Parameters

- *management* — Configures the management VRF instance to be used to reach the SSH server.

Default

Not configured

Command Mode

CONFIGURATION

Usage Information

By default, the SSH server is enabled. To configure the SSH server to be reachable on the management VRF instance, use the `ip ssh server vrf` command.

Example

```
OS10(config)# ip ssh server vrf management
```

Supported Releases 10.4.0E(R1) or later

line vty

Enters the virtual terminal line mode to access the virtual terminal (VTY).

Syntax `line vty`
Parameters None
Default Not configured
Command Mode CONFIGURATION
Usage Information None

Example

```
OS10(config)# line vty
OS10(config-line-vty)#
```

Supported Releases 10.4.0E(R1) or later

login concurrent-session limit

Configures the maximum number of concurrent login sessions allowed for a user ID.

Syntax `login concurrent-session limit number`
Parameters `limit number` — Enter the limit of concurrent login sessions (1 to 12).
Default 10 concurrent login sessions are supported.
Command Mode CONFIGURATION
Usage Information The total number of concurrent login sessions for the same user ID includes all console and remote connections, where:

- Each remote VTY connection counts as one login session.
- All login sessions from a terminal emulator on an attached console count as one session.

To disable the configured number of allowed login sessions, enter the `no` version of the command.

Example

```
OS10(config)# login concurrent-session limit 7
```

Supported Releases 10.4.1.0 or later

login-statistics enable

Enables the display of login statistics to users.

Syntax `login-statistics enable`
Parameters None
Default Disabled
Command Mode CONFIGURATION
Usage Information Only the `sysadmin` and `secadmin` roles have access to this command. When enabled, user login information, including the number of successful and failed logins, role changes, and the last time a user logged in, is displayed after a successful login. To disable login statistics, enter the `no login-statistics enable` command.

Example

```
OS10(config)# login-statistics enable
```

Supported Releases

10.4.0E(R1) or later

password-attributes

Configures rules for password entries.

Syntax

```
password-attributes {[min-length number] [character-restriction {[upper number] [lower number] [numeric number] [special-char number]}]}
```

Parameters

- `min-length number` — (Optional) Sets the minimum number of required alphanumeric characters (6 to 32; default 9).
- `character-restriction:`
 - `upper number` — (Optional) Sets the minimum number of uppercase characters required (0 to 31; default 0).
 - `lower number` — (Optional) Sets the minimum number of lowercase characters required (0 to 31; default 0).
 - `numeric number` — (Optional) Sets the minimum number of numeric characters required (0 to 31; default 0).
 - `special-char number` — (Optional) Sets the minimum number of special characters required (0 to 31; default 0).

Default

- Minimum length: 9 characters
- Uppercase characters: 0
- Lowercase characters: 0
- Numeric characters: 0
- Special characters: 0

Command Mode

EXEC

Usage Information

- By default, the password you configure with the `username password` command must be at least nine alphanumeric characters.
- Use the `password-attributes` command to increase password strength. When you enter the command, at least one parameter is required. When you enter the `character-restriction` parameter, at least one option is required.
- To reset parameters to their default values, enter the `no password-attributes` command.

Example

```
OS10(config)# password-attributes min-length 6 character-restriction
upper 2 lower 2 numeric 2
```

Supported Releases

10.4.0E(R1) or later

password-attributes max-retry lockout-period

Configures maximum number of consecutive failed login attempts and the lockout period for the user ID.

Syntax

```
password-attributes {[max-retry number] [lockout-period minutes]}
```

Parameters

- `max-retry number` — (Optional) Sets the maximum number of consecutive failed login attempts for a user before the user is locked out (0 to 16).
- `lockout-period minutes` — (Optional) Sets the amount of time that a user ID is prevented from accessing the system after exceeding the maximum number of failed login attempts (0 to 43,200).

Default

- Maximum retries: 3 — A maximum of three failed login attempts is supported.
- Lockout period: 0 — No lockout period is configured. Failed login attempts do not lock out a user.

Command Mode

CONFIGURATION

- Usage Information**
- To remove the configured `max-retry` or `lockout-period` settings, enter the `no password-attributes {max-retry | lockout-period}` command.
 - When a user is locked out due to exceeding the maximum number of failed login attempts, other users can still access the switch.

Example

```
OS10(config)# password-attributes max-retry 5 lockout-period 30
```

Supported Releases 10.4.1.0 or later

radius-server host

Configures a RADIUS server and the key used to authenticate the switch on the server.

Syntax `radius-server host {hostname | ip-address} key {0 authentication-key | 9 authentication-key | authentication-key} [auth-port port-number]`

- Parameters**
- `hostname` — Enter the host name of the RADIUS server.
 - `ip-address` — Enter the IPv4 (A.B.C.D) or IPv6 (x:x:x::x) address of the RADIUS server.
 - `key 0 authentication-key` — Enter an authentication key in plain text (up to 42 characters).
 - `key 9 authentication-key` — Enter an authentication key in encrypted format (up to 128 characters).
 - `authentication-key` — Enter an authentication in plain text (up to 42 characters). It is not necessary to enter 0 before the key.
 - `auth-port port-number` — (Optional) Enter the UDP port number used on the server for authentication (0 to 65535, default 1812)

Default Not configured

Command Mode CONFIGURATION

Usage Information The authentication key must match the key configured on the RADIUS server. You cannot enter spaces in the key. The `show running-configuration` output displays both unencrypted and encrypted keys in encrypted format. Configure global settings for the timeout and retransmit attempts allowed on RADIUS servers by using the `radius-server retransmit` and `radius-server timeout` commands. The `no` version of this command removes a RADIUS server configuration.

Example

```
OS10(config)# radius-server host 1.5.6.4 key secret1
```

Supported Releases 10.2.0E or later

radius-server retransmit

Configures the number of authentication attempts allowed on RADIUS servers.

Syntax `radius-server retransmit retries`

Parameters `retries` — Enter the number of retry attempts (0 to 100).

Default An OS10 switch retransmits a RADIUS authentication request three times.

Command Mode CONFIGURATION

Usage Information Use this command to globally configure the number of retransmit attempts allowed for authentication requests on RADIUS servers. The `no` version of this command resets the value to the default.

Example

```
OS10(config)# radius-server retransmit 50
```

Supported Releases 10.2.0E or later

radius-server timeout

Configures the timeout used to resend RADIUS authentication requests.

Syntax	<code>radius-server timeout seconds</code>
Parameters	<code>seconds</code> — Enter the time in seconds for retransmission (0 to 1000).
Default	An OS10 switch stops sending RADIUS authentication requests after five seconds.
Command Mode	CONFIGURATION
Usage Information	Use this command to globally configure the timeout value used on RADIUS servers. The <code>no</code> version of this command resets the value to the default.
Example	<pre>OS10(config)# radius-server timeout 360</pre>
Supported Releases	10.2.0E or later

radius-server vrf

Configures RADIUS server for the management VRF instance.

Syntax	<code>radius-server vrf management</code>
Parameters	None
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the RADIUS server from the management VRF instance.
Example	<pre>OS10(config)# radius-server vrf management</pre>
Supported Releases	10.4.0E(R1) or later

show crypto ssh-key

Display the current host public keys used in SSH authentication.

Syntax	<code>show crypto ssh-key {rsa ecdsa ed25519}</code>
Parameters	<ul style="list-style-type: none"><code>rsa</code> — Displays the RSA public key.<code>ecdsa</code> — Displays the ECDSA public key.<code>ed25519</code> — Displays the Ed25519 key.
Default	Not configured
Command Mode	EXEC
Usage Information	After you regenerate an SSH server key with a customized bit size, disable and re-enable the SSH server to use the new key. If a remote SSH client uses strict host-key checking, copy a newly generated host key to the list of known hosts on the client.
Example	<pre>OS10# show crypto ssh-key rsa ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACogJtArA0fHJkFpioGaAcp+vrDQFC3l3XFHtd41wXY9kM0Ar+37j OzkjNIN1/8Ok+8aJtCoJKbcYaduMjmhVNrNUW5TUXoCnp1XNRpkJzgs7Lt47yi86rqrTCAQW4eSYJIJs4 +4q19b4MF2D3499Ofn8uS82Mjtj0N1011bTbP3gsF4YYdBWafqp root@OS10</pre>

Supported Releases 10.4.1.0 or later

show ip ssh

Displays the SSH server information.

Syntax show ip ssh

Parameters None

Default Not configured

Command Mode EXEC

Usage Information Use this command to view information about the established SSH sessions.

Example

```
OS10# show ip ssh

SSH Server: Enabled
-----
SSH Server Ciphers: chacha20-poly1305@openssh.com, aes128-ctr,
aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-
gcm@openssh.com
SSH Server MACs: umac-64-etm@openssh.com, umac-128-
etm@openssh.com,
hmac-sha2-256-etm@openssh.com,
hmac-sha2-512-etm@openssh.com,
hmac-sha1-
etm@openssh.com, umac-64@openssh.com,
umac-128@openssh.com, hmac-sha2-256,
hmac-sha2-512, hmac-sha1
SSH Server KEX algorithms: curve25519-sha256@libssh.org, ecdh-sha2-
nistp256,
ecdh-sha2-nistp384, ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256,
diffie-hellman-group14-sha1
Password Authentication: Enabled
Host-Based Authentication: Disabled
RSA Authentication: Enabled
Challenge Response Auth: Disabled
```

Supported Releases 10.3.0E or later

show login-statistics

Displays statistics on user logins to the system.

Syntax show login-statistics {user *user-id* | all}

Parameters

- user *user-id* — Enter an OS10 username.
- all — Displays login statistics for all system users.

Default Not configured

Command Mode EXEC

Usage Information Only the *sysadmin* and *secadmin* roles can access this command. The show output displays login information for system users, including the number of successful and failed logins, role changes, and the last time a user logged in.

Example

```
OS10# show login-statistics all
Display statistics upon user login: Enabled
```

```
Time-frame in days: 25
```

User	Role Change	#Fail since last Login	#Fail During Timeframe	#Success	Date/Time	Last Login	Location
admin	False	0	1	13	2017-11-02T16:02:44Z		in
netadmin	False	0	0	5	2017-11-02T15:59:04Z		(00:00)
mltest	False	0	0	1	2017-11-01T15:42:07Z		1001:10:16:210::4001

```
OS10# show login-statistics user mltest
User                               : mltest
Role changed since last login      : False
Failures since last login          : 0
Time-frame in days                  : 25
Failures in time period             : 0
Successes in time period            : 1
Last Login Time                     : 2017-11-01T15:42:07Z
Last Login Location                 : 1001:10:16:210::4001
```

Supported Releases

10.4.0E(R1) or later

show users

Displays information for all users logged into OS10.

Syntax `show users`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information Use this command to view current OS10 users.

Example

```
OS10# show users

Index Line   User   Role   Application  Idle   Login      Location
-----
1      ttyS0  root   root   -bash        >24h  2018-05-23 console
      T23:05:03Z
2      pts/0  admin  sysadmin bash         1.1s  2018-05-30 10.14.1.214
[ssh]                                     T20:04:27Z
```

Supported Releases 10.2.0E or later

tacacs-server host

Configures a TACACS+ server and the key used to authenticate the switch on the server.

Syntax `tacacs-server host {hostname | ip-address} key {0 authentication-key | 9 authentication-key | authentication-key} [auth-port port-number]`

- Parameters**
- `hostname` — Enter the host name of the TACACS+ server.
 - `ip-address` — Enter the IPv4 (A.B.C.D) or IPv6 (x:x:x:x:x) address of the TACACS+ server.
 - `key 0 authentication-key` — Enter an authentication key in plain text (up to 42 characters).

- `key 9 authentication-key` — Enter an authentication key in encrypted format (up to 128 characters).
- `authentication-key` — Enter an authentication in plain text (up to 42 characters). It is not necessary to enter 0 before the key.
- `key authentication-key` — Enter a text string for the encryption key used to authenticate the switch on the TACACS+ server (up to 42 characters).

Default Not configured

Command Mode CONFIGURATION

Usage Information The authentication key must match the key configured on the TACACS+ server. You cannot enter spaces in the key. The `show running-configuration` output displays both unencrypted and encrypted keys in encrypted format. Configure the global timeout allowed for authentication requests on TACACS+ servers by using the `tacacs-server timeout` command. By default, OS10 times out an authentication attempt on a TACACS+ server after five seconds. The `no` version of this command removes a TACACS+ server configuration.

Example

```
OS10(config)# tacacs-server host 1.5.6.4 key secret1
```

Supported Releases 10.4.0E(R2) or later

tacacs-server timeout

Configures the global timeout used for authentication attempts on TACACS+ servers.

Syntax `tacacs-server timeout seconds`

Parameters `seconds` — Enter the timeout period used to wait for an authentication response from a TACACS+ server (1 to 1000 seconds).

Default 5 seconds

Command Mode CONFIGURATION

Usage Information The `no` version of this command resets the TACACS+ server timeout to the default.

Example

```
OS10(config)# tacacs-server timeout 360
```

Supported Releases 10.4.0E(R2) or later

username password role

Creates an authentication entry based on a user name and password, and assigns a role to the user.

Syntax `username username password password role role`

- Parameters**
- `username username` — Enter a text string (up to 32 alphanumeric characters; 1 character minimum).
 - `password password` — Enter a text string (up to 32 alphanumeric characters; 9 characters minimum).
 - `role role` — Enter a user role:
 - `sysadmin` — Full access to all commands in the system, exclusive access to commands that manipulate the file system, and access to the system shell. A system administrator can create user IDs and user roles.
 - `secadmin` — Full access to configuration commands that set security policy and system access, such as password strength, AAA authorization, and cryptographic keys. A security administrator can display security information, such as cryptographic keys, login statistics, and log information.

- `netadmin` — Full access to configuration commands that manage traffic flowing through the switch, such as routes, interfaces, and ACLs. A network administrator cannot access configuration commands for security features or view security information.
- `netoperator` — Access to EXEC mode to view the current configuration. A network operator cannot modify any configuration setting on a switch.

Default

- User name and password entries are in clear text.
- There is no default user role.

Command Mode CONFIGURATION

Usage Information

- By default, the password must be at least nine alphanumeric characters. You can enter special characters, such as:

```
! # % & ' ( ) ; < = > [ ] * + - . / : ^ _
```

Enter the password in clear text. It is converted to SHA-512 format in the running configuration. For backward compatibility with OS10 releases 10.3.1E and earlier, passwords entered in MD-5, SHA-256, and SHA-512 format are supported.

- To increase the required password strength, use the `password-attributes` command.
- The `no` version of this command deletes authentication for a user.

Example

```
OS10(config)# username user05 password newpwd404 role sysadmin
```

Supported Releases 10.2.0E or later

username sshkey

Enables SSH password-less login using the public key for a remote client. The remote client is not prompted to enter a password.

Syntax `username user_name sshkey sshkey_string`

Parameters

- `user_name` — Enter the user name of the remote client. This value is the user name configured with the `username` command.
- `sshkey_string` — Enter the public key used by the remote client device to log in to the OS10 switch.

Default The default SSH server keys are an RSA key generated using 2048 bits, an ECDSA key with 256 bits, and an Ed25519 key.

Command Mode CONFIGURATION

Usage Information

Locate the public keys on a remote client in the `~/.ssh/id_rsa.pub` file. Use the public key as the `sshkey_string`.

The `no username user_name sshkey` command removes the SSH password-less configuration for a specified user.

To configure multiple user names for SSH password-less login, use the `username sshkey filename` command.

Example

```
OS10(config)# username user10 sshkey abcd

OS10(config)# do show running-configuration users
username admin password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8S
UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin
username user10 password
$6$rounds=656000$G10VRFTJB291ekwo$iTGf0zd4bTUcBBpIVsbr6oStnUZMydN51Ds4WE6G3XHEtWb
role sysadmin
username user10 sshkey abcd
```

Supported Releases 10.4.1.0 or later

username sshkey filename

Enables SSH password-less login for remote clients using multiple public keys. A remote client is not prompted to enter a password.

Syntax	<code>username user_name sshkey filename file_path</code>
Parameters	<ul style="list-style-type: none">• <code>user_name</code> — Enter an OS10 user name who logs in on a remote client. This value is the user name configured on the remote client.• <code>file_path</code> — Enter the absolute path name of the local file containing the public keys used by remote devices.
Default	The default SSH server keys are an RSA key generated using 2048 bits, an ECDSA key with 256 bits, and an Ed25519 key.
Command Mode	CONFIGURATION
Usage Information	Before you use the command, locate the public keys on a remote client in the <code>~/.ssh/id_rsa.pub</code> file. Create a file on the local OS10 client into the file. Enter each public key on a separate line. Download the file to your home OS10 directory.

NOTE: Entering the command when an SSH key file is not present has no effect and results in a silent failure. See [SSH Key Management](#) for more information.

The `no username user_name sshkey` command removes the SSH password-less configuration for the specified user.

Example

```
OS10(config)# username user10 sshkey filename /test_file.txt

OS10(config)# do show running-configuration users
username admin password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8S
UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin
username user10 password
$6$rounds=656000$G10VRFTJB291ekwo$iTGf0zd4bTUcBBpIVsbr6oStnUZMydN51Ds4WE6G3XHEtWb
role sysadmin
username user10 sshkey filename /test_file.txt
```

Supported Releases 10.4.1.0 or later

userrole default inherit

Reconfigures the default `netoperator` role assigned to a TACACS+-authenticated user.

Syntax	<code>userrole default inherit existing-role-name</code>
Parameters	<ul style="list-style-type: none">• <code>existing-role-name</code> — Enter a user role:<ul style="list-style-type: none">◦ <code>sysadmin</code> — Full access to all commands in the system, exclusive access to commands that manipulate the file system, and access to the system shell. A system administrator can create user IDs and user roles.◦ <code>secadmin</code> — Full access to configuration commands that set security policy and system access, such as password strength, AAA authorization, and cryptographic keys. A security administrator can display security information, such as cryptographic keys, login statistics, and log information.◦ <code>netadmin</code> — Full access to configuration commands that manage traffic flowing through the switch, such as routes, interfaces, and ACLs. A network administrator cannot access configuration commands for security features or view security information.◦ <code>netoperator</code> — Access to EXEC mode to view the current configuration. A network operator cannot modify any configuration setting on a switch.
Default	OS10 assigns the <code>netoperator</code> role to a user authenticated by a TACACS+ server with a missing or unknown role.
Command Mode	CONFIGURATION
Usage Information	<ul style="list-style-type: none">• When a TACACS+ server authenticates a user and does not return a role or returns an unknown role, OS10 assigns the <code>netoperator</code> role to the authenticated user by default. Use this command to reconfigure the default <code>netoperator</code> role.• The <code>no userrole default</code> version of the command resets the role to <code>netoperator</code>.

Example

```
OS10(config)# userrole default inherit sysadmin
```


Supported Releases

10.4.0E(R3P3) or later

Simple Network Management Protocol

Network management stations use Simple Network Management Protocol (SNMP) to retrieve or alter management data from network elements. Standard and private SNMP management information bases (MIBs) are supported, including all `get` requests. A *managed object* is a datum of management information. A MIB is a database that stores managed objects found in network elements. MIBs are hierarchically structured and use object identifiers to address managed objects. Managed objects are also known as *object descriptors*. For the list supported MIBs refer to the Release Notes of the relevant version of OS10.

OS10 supports SNMP set for SysName on System MIBs.

 **NOTE:** OS10 SNMP supports only IPv4 transport.

SNMP commands

SNMP traps: Enable SNMP notifications to be sent to network management host devices.

snmp-server community

Configures a new community string access. The management station is a member of the same community as the SNMP agent.

Syntax

```
snmp-server community community-name {ro | rw} acl aclname
```

Parameters

- *community-name* — Enter a text string to act as an SNMP password (up to 20 characters).
- *ro* — Enter to set read-only permission.
- *rw* — Enter to set read and write permission.
- *aclname* — Enter an existing ACL rule name. This option associates an IPv4 ACL to SNMP server community.

Default

Not configured

Command Mode

CONFIGURATION

Usage Information

The *community-name* parameter indexes this command. If you do not configure this command, you cannot query SNMP data. The `no` version of this command removes access to a community.

Example

```
OS10(config)# snmp-server community public ro
```

```
OS10(config)# snmp-server community public ro acl aclrule1
```

Supported Releases

10.2.0E or later

snmp-server contact

Configures contact information for troubleshooting this SNMP node.

Syntax

```
snmp-server contact text
```

Parameters

text — Enter an alphanumeric text string (up to 55 characters).

Default

Not configured

Command Mode

CONFIGURATION

Usage Information

The no version of this command deletes the SNMP server contact information.

Example

```
OS10(config)# snmp-server contact administrator
```

Supported Releases

10.2.0E or later

snmp-server enable traps

Enables SNMP traps on a switch.

Syntax

```
snmp-server enable traps [notification-type] [notification-option]
```

Parameters

- *notification-type notification-option* — Enter an SNMP notification type, and optionally, a notification option for the type.

Table 8. Notification types and options

Notification type	Notification option
entity — Enable entity change traps.	None
envmon — Enable SNMP environmental monitor traps.	<ul style="list-style-type: none"> o fan — Enable fan traps. o power-supply — Enable power-supply traps. o temperature — Enable temperature traps.
lldp — Enable LLDP state change traps.	<ul style="list-style-type: none"> o rem-tables-change — Enable the lldpRemTablesChange trap.
snmp — Enable SNMP traps.	<ul style="list-style-type: none"> o authentication — Enable authentication traps. o coldstart — Enable coldstart traps when you power on the switch and the SNMP agent initializes. o linkdown — Enable link-down traps. o linkup — Enable link-up traps. o warmstart — Enable warmstart traps when the switch reloads and the SNMP agent reinitializes.

Defaults

Not configured

Command Mode

CONFIGURATION

Usage Information

The no version of an snmp-server enable traps command disables SNMP traps on the switch.

If you do not enter a notification-type and notification-option parameter with the command, all traps are enabled.

If you enter only a notification-type, all notification-option traps associated with the type are enabled.

Re-enter the command multiple times with different notification types and options to enable specific SNMP trap types.

Example

```
OS10(config)# snmp-server enable traps envmon fan
OS10(config)# snmp-server enable traps envmon power-supply
OS10(config)# snmp-server enable traps snmp

OS10(config)# no snmp-server enable traps snmp
```

Supported Releases

10.4.1.0 or later

snmp-server host

Configures a host to receive SNMP traps.

Syntax `snmp-server host {hostname | ipv4-address | ipv6-address} {traps | version version-number| snmp-string} [udp-port port-number]`

- Parameters**
- `hostname | ipv4-address | ipv6-address` — Enter either the name or IPv4/IPv6 address of the host.
 - `version-number` — Enter the SNMP version number to be used for notification messages. OS10 supports SNMPv1 and SNMPv2c.
 - `snmp-string` — Enter SNMPv1 community string name
 - `port-number` — (Optional) Enter the UDP port number, ranging from 0 to 65535.

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables the host from receiving the SNMP traps.

Example

```
OS10(config)# snmp-server host 10.1.1.1 traps version 1 snmptest udp-port 1
```

Supported Releases 10.2.0E or later

snmp-server location

Configures the location of the SNMP server.

Syntax `snmp-server location text`

Parameters `text` — Enter an alphanumeric string (up to 55 characters).

Default United States

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the SNMP location.

Example

```
OS10(config)# snmp-server location datacenter10
```

Supported Releases 10.2.0E or later

snmp-server vrf

Configures an SNMP agent to receive SNMP traps for the management VRF instance.

Syntax `snmp-server vrf management`

Parameters None

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables the SNMP agent from receiving the SNMP traps.

Example

```
OS10(config)# snmp-server vrf management
```

Uplink Failure Detection

Uplink failure detection (UFD) indicates the loss of upstream connectivity to servers connected to the switch.

A switch provides upstream connectivity for devices, such as servers. If the switch loses upstream connectivity, the downstream devices also lose connectivity. However, the downstream devices do not generally receive an indication that the upstream connectivity was lost because connectivity to the switch is still operational. To solve this issue, use UFD.

UFD associates downstream interfaces with upstream interfaces. When upstream connectivity fails, the switch operationally disables its downstream links. Failures on the downstream links allow downstream devices to recognize the loss of upstream connectivity. This allows the downstream servers to select alternate paths, if available, to send traffic to upstream devices.

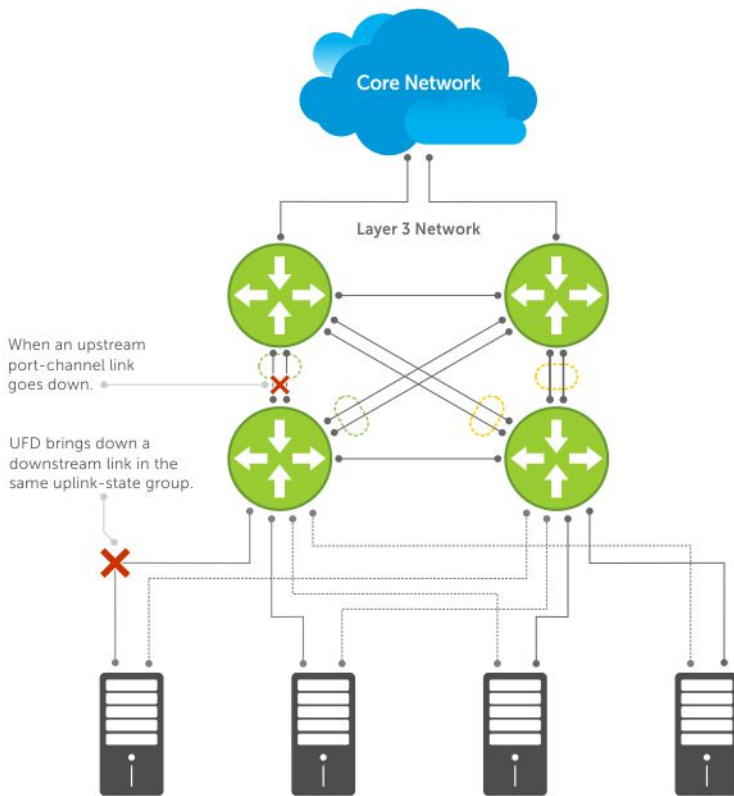
UFD creates an association between upstream and downstream interfaces known as *uplink-state group*. An interface in an uplink-state group can be a physical Ethernet or fibre channel interface or a port-channel.

An enabled uplink-state group tracks the state of all assigned upstream interfaces. The failure of upstream interfaces results in automatic disabling of downstream interfaces in the uplink-state group, as shown in the following illustration. If only one of the upstream interfaces in an uplink-state group goes down, a specific number of downstream interfaces in the same uplink-state group go down. You can configure the number of downstream interfaces that go down based on the traffic conditions from the server to upstream interfaces. This avoids overloading traffic on upstream ports.

By default, if all the upstream interfaces in an uplink-state group go down, all the downstream interfaces in the same uplink-state group are set into a link-down state.

In addition, in an uplink-state group, you can configure automatic recovery of downstream ports when there is a change in the link status of uplink interfaces.

You can also bring up downstream interfaces that are in an UFD-disabled error state manually.



Server traffic is diverted over a backup link to upstream devices.



Configure uplink failure detection

Consider the following before configuring an uplink-state group:

- You can assign a physical port or a port channel to an uplink-state group.
- You can assign an interface to only one uplink-state group at a time.
- You can designate the uplink-state group as either an upstream or a downstream interface, but not both.
- You can configure multiple uplink-state groups and operate them concurrently.
- You cannot assign both a port channel and its members to an uplink-state group, which would make the group inactive. The port channels and individual ports that are not part of any port channel can coexist as members of an uplink-state group.
- If one of the upstream interfaces in an uplink-state group goes down, you can configure to set the downstream ports in an operationally down state with an *UFD Disabled error* status. You can configure the system to disable either a user-configurable set of downstream ports or all the downstream ports in the group.
- The downstream ports are disabled in an order starting from the lowest numbered port to the highest.
- When an upstream interface in an uplink-state group that was down comes up, the set of UFD-disabled downstream ports that were down due to that particular upstream interface are brought up, and the *UFD Disabled error* clears in those downstream ports.
- If you disable an uplink-state group, the downstream interfaces are not disabled, regardless of the state of the upstream interfaces.
- If you do not assign upstream interfaces to an uplink-state group, the downstream interfaces are not disabled.

Uplink failure detection on VLT

When you create uplink-state group in a switch operating in VLT mode, ensure that all the nodes in the VLT setup have same configuration for uplink state groups with VLT port-channel as member. This makes all the nodes independently operational and to operate in sync.

When you configure VLT port-channel as upstream member in the uplink state group, the system tracks the fabric Status of VLT. When the fabric status goes down, the uplink state group in each VLT node disables the downstream VLT port-channel local to the node.

Configuration:

1. Create an uplink-state group in CONFIGURATION mode.

```
uplink-state-group group-id
```

2. Configure the upstream and downstream interfaces in UPLINK-STATE-GROUP mode.

```
upstream {interface-type | interface-range}  
downstream {interface-type | interface-range}
```

3. (Optional) Disable uplink-state group tracking in UPLINK-STATE-GROUP mode.

```
no enable
```

4. (Optional) Provide a descriptive name for the uplink-state group in UPLINK-STATE-GROUP mode.

```
name string
```

5. Configure the number of downstream interfaces to disable, when an upstream interface goes down in UPLINK-STATE-GROUP mode.

```
downstream disable links{number | all}
```

6. (Optional) Enable auto-recovery of downstream interfaces that are disabled in UPLINK-STATE-GROUP mode.

```
downstream auto-recover
```

7. (Optional) Configure timer to defer the UFD actions on downstream ports in UPLINK-STATE-GROUP mode.

```
defer-time timer
```

8. (Optional) Clear the UFD error disabled state of downstream interfaces in EXEC mode.

```
clear ufd-disable
```

Configure uplink state group

```
OS10(config)# uplink-state-group 1  
OS10(conf-uplink-state-group-1)# upstream ethernet 1/1/7:1  
OS10(conf-uplink-state-group-1)# downstream ethernet 1/1/1-1/1/5  
OS10(conf-uplink-state-group-1)# downstream ethernet 1/1/9:2-1/1/9:3  
OS10(conf-uplink-state-group-1)# enable  
OS10(conf-uplink-state-group-1)# name UFDGROUP1  
OS10(conf-uplink-state-group-1)# defer-time 10  
OS10(conf-uplink-state-group-1)# no downstream auto-recover  
OS10(conf-uplink-state-group-1)# downstream disable links 2
```

View uplink state group configuration

```
OS10#show uplink-state-group 1  
  
Uplink State Group: 1 Status: Enabled,down
```

```
OS10# show uplink-state-group 1 detail  
  
(Up): Interface up      (Dwn): Interface down   (Dis): Interface disabled  
  
Uplink State Group   : 1      Status    : Enabled,up Name   : UFDGROUP1  
Defer Time           : 10 second(s)  
Upstream Interfaces  : Eth 1/1/7:1(Up)  
Downstream Interfaces: Eth 1/1/1(Dwn)  Eth 1/1/2(Dwn)  Eth 1/1/3(Dwn)  Eth 1/1/4(Dwn)
```



```
Eth 1/1/5 (Dwn)   Eth 1/1/9:2 (Dwn) Eth 1/1/9:3 (Dwn)
```

```
OS10(conf-uplink-state-group-1)# show configuration
!
uplink-state-group 1
  downstream ethernet1/1/1-1/1/5
  downstream ethernet1/1/9:2-1/1/9:3
  upstream ethernet1/1/7:1
```

UFD commands

clear ufd-disable

Overrides the uplink-state group configuration and brings up the downstream interfaces.

Syntax `clear ufd-disable {interface interface-type | uplink-state-group group-id}`

Parameters

- *interface-type* — Enter the interface type.
- *group-id* — Enter the uplink state group ID, from 1 to 32.

Default None

Command Mode EXEC

Usage Information This command manually brings up a disabled downstream interface that is in UFD-disabled error state. After the downstream interface is up, it is not disabled until there are changes in the upstream interfaces. This command does not have effect on downstream interfaces that are already up or interfaces that are not part of the UFD group.

Example

```
OS10# clear ufd-disable interface ethernet 1/1/2
OS10# clear ufd-disable uplink-state-group 1
```

Supported Releases 10.4.0E(R3) or later

defer-time

Configures timer to defer UFD actions on downstream ports.

Syntax `defer-time timer`

Parameters *timer*— Enter the timer value in seconds, ranging from 1 to 120.

Default Disabled

Command Mode UPLINK-STATE-GROUP

Usage Information You can view the timer details configured using the `show uplink-state-group [group-id] detail` command. The `no` version of this command disables the timer.

Example

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# defer-time 120
```

Supported Releases 10.4.1.0 or later

downstream

Adds an interface or a range of interfaces as a downstream interface to the uplink-state group.

Syntax	<code>downstream {<i>interface-type</i> <i>interface-range</i>}</code>
Parameters	<ul style="list-style-type: none">• <i>interface-type</i> — Enter the interface type as Ethernet or port-channel.• <i>interface-range</i> — Enter the range of interfaces.
Default	None
Command Mode	UPLINK-STATE-GROUP
Usage Information	You cannot assign an interface that is already a member of an uplink-state group to another group. The no version of this command removes the interface from the uplink-state group.
Example	<pre>OS10(config)# uplink-state-group 1 OS10(conf-uplink-state-group-1)# downstream ethernet 1/1/1</pre>
Supported Releases	10.4.0E(R3) or later

downstream auto-recover

Enables auto-recovery of the disabled downstream interfaces.

Syntax	<code>downstream auto-recover</code>
Parameters	None
Default	Enabled
Command Mode	UPLINK-STATE-GROUP
Usage Information	The no version of this command disables the auto-recovery of downstream interfaces.
Example	<pre>OS10(config)# uplink-state-group 1 OS10(conf-uplink-state-group-1)# no downstream auto-recover</pre>
Supported Releases	10.4.1.0 or later

downstream disable links

Configures the number of downstream interfaces to disable when an upstream interface in the uplink-state group goes down.

Syntax	<code>downstream disable links{<i>number</i> all}</code>
Parameters	<ul style="list-style-type: none">• <i>number</i>—Enter the number of downstream interfaces to disable, from 1 to 1024.• <i>all</i>—Enter <i>all</i> to disable all the downstream interfaces.
Default	Not configured
Command Mode	UPLINK-STATE-GROUP
Usage Information	The no version of this command reverts the settings to the default state.
Example	<pre>OS10(config)# uplink-state-group 1 OS10(conf-uplink-state-group-1)# downstream disable links 2</pre>
Supported Releases	10.4.1.0 or later

enable

Enables tracking of an uplink-state group.

Syntax	enable
Parameters	None
Default	Disabled
Command Mode	UPLINK-STATE-GROUP
Usage Information	The no version of this command disables tracking of an uplink-state group.

Example

```
OS10 (config) # uplink-state-group 1
OS10 (conf-uplink-state-group-1) # enable
```

Supported Releases 10.4.0E(R3) or later

name

Configures a descriptive name for the uplink-state group.

Syntax	name <i>string</i>
Parameters	<i>string</i> — Enter a description for the uplink-state group. A maximum of 32 characters.
Default	Not configured
Command Mode	UPLINK-STATE-GROUP
Usage Information	The no version of this command removes the descriptive name.

Example

```
OS10 (config) # uplink-state-group 1
OS10 (conf-uplink-state-group-1) # name test_ufd_group
```

Supported Releases 10.4.0E(R3) or later

show running-configuration uplink-state-group

Displays the running configuration specific to uplink-state groups.

Syntax	show running-configuration uplink-state-group [<i>group-id</i>]
Parameters	<i>group-id</i> — Enter the uplink group ID. The running configuration of the specified group ID displays.
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show running-configuration uplink-state-group
!
uplink-state-group 1
  downstream ethernet1/1/8:1-1/1/8:4
  upstream ethernet1/1/9:1-1/1/9:4
  upstream port-channell-3
```

Supported Releases 10.4.0E(R3) or later

show uplink-state-group

Displays configured uplink-state status.

Syntax	show uplink-state-group [<i>group-id</i>] [<i>detail</i>]
Parameters	<ul style="list-style-type: none">• <i>group-id</i> — Enter the uplink group ID. The status of the specified group ID displays.• <i>detail</i> — Displays detailed information on the status of the uplink-state groups.
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show uplink-state-group
Uplink State Group: 9, Status: Enabled,down
```

```
OS10# show uplink-state-group 9
Uplink State Group: 9, Status: Enabled,down
OS10#
```

Example (detail)

```
OS10# show uplink-state-group detail
(Up): Interface up    (Dwn): Interface down  (Dis): Interface disabled
Uplink State Group   : 1      Status   : Enabled,up Name : UFDGROUP1
Defer Time           : 10 second(s)
Upstream Interfaces  : Eth 1/1/7:1(Up)
Downstream Interfaces: Eth 1/1/1(Dwn)  Eth 1/1/2(Dwn)  Eth 1/1/3(Dwn)
                    Eth 1/1/4(Dwn)
                    Eth 1/1/5(Dwn)  Eth 1/1/9:2(Dwn) Eth
1/1/9:3(Dwn)
```

```
OS10# show uplink-state-group 2 detail
(Up): Interface up    (Dwn): Interface down  (Dis): Interface disabled
Uplink State Group   : 2      Status   : Enabled,down Name:
UFDGROUPUFDGROUPUFDGROUPUFDGROUP
Upstream Interfaces  : Eth 1/1/6(Dwn)  Eth 1/1/10(Dwn)  Eth
1/1/11(Dwn)  Eth 1/1/12(Dwn)
                    Eth 1/1/13(Dwn)  Eth 1/1/14(Dwn)  Eth 1/1/15(Dwn)
Downstream Interfaces: Eth 1/1/16(Dis)  Eth 1/1/17(Dis)  Eth
1/1/18(Dis)  Eth 1/1/19(Dis)
                    Eth 1/1/20(Dis)
```

Supported Releases 10.4.0E(R3) or later

uplink-state-group

Creates an uplink-state group and enables upstream link tracking.

Syntax	uplink-state-group <i>group-id</i>
Parameters	<i>group-id</i> — Enter a unique ID for the uplink-state group, from 1 to 32.
Default	None
Command Mode	CONFIGURATION

Usage Information The no version of this command removes the uplink-state group.

Example

```
OS10(config)# uplink-state-group 1
```

Supported Releases 10.4.0E(R3) or later

upstream

Adds an interface or a range of interfaces as an upstream interface to the uplink-state group.

Syntax `upstream {interface-type | interface-range}`

Parameters

- *interface-type* — Enter the interface type as Ethernet or port-channel.
- *interface-range* — Enter the range of interfaces.

Default None

Command Mode UPLINK-STATE-GROUP

Usage Information You cannot assign an interface that is already a member of an uplink-state group to another group. The no version of this command removes the interface from the uplink-state group.

Example

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# upstream ethernet 1/1/45-1/1/48
```

Supported Releases 10.4.0E(R3) or later

OS10 image upgrade

The `image download` command simply downloads the software image — it does not install the software on your device. The `image install` command installs the downloaded image to the standby partition.

NOTE: If the active partition contains any modified text files or custom packages installed, they would not be available in the standby partition. Backup the modified files and re-install the packages after downloading the image.

1. (Optional) Backup the current running configuration to the startup configuration in EXEC mode.

```
copy running-configuration startup-configuration
```

2. Backup the startup configuration in EXEC mode.

```
copy config://startup.xml config://<backup file name>
```

3. Download the new software image from dell.com/support, extract the `bin` files from the `tar` file, and save the file in EXEC mode.

```
image download file-url
```

4. (Optional) View the current software download status in EXEC mode.

```
show image status
```

5. Install the software image in EXEC mode.

```
image install image-url
```

6. (Optional) View the status of the current software install in EXEC mode. In S5148F-ON, open a new SSH or Telnet session to check the status of the current software.

```
show image status
```

7. Change the next boot partition to the standby partition in EXEC mode. Use the `active` parameter to set the next boot partition from standby to active.

```
boot system standby
```

8. (Optional) Check whether the next boot partition has changed to standby in EXEC mode.

```
show boot detail
```

9. Reload the new software image in EXEC mode.

```
reload
```

Image download

```
OS10# image download ftp://userid:passwd@hostip:/filepath
```

Image install

```
OS10# image install image://filename.bin
```

Show version

```
OS10# show version
Dell EMC Networking OS10-Enterprise
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
OS Version: 10.4.1.0X
Build Version: 10.4.1.0.X.9
Build Time: 2018-06-12T22:18:40-0700
System Type: S4148F-ON
Architecture: x86_64
Up Time: 2 days 03:37:25
```

Boot system partition

Set the boot partition to active or standby for subsequent boot cycles. Boot OS10 from standby to load the image on the standby partition, or boot from active to load the currently running image.

1. Display current boot information in EXEC mode.

```
show boot detail
```

2. Configure the boot system in EXEC mode.

```
boot system [active | standby]
```

- `active` — Resets the running partition as the subsequent boot partition.
- `standby` — Sets the standby partition as the subsequent boot partition.

View boot detail

```
OS10# show boot detail
Current system image information detail:
=====
Type:                               Node-id 1
Boot Type:                           Flash Boot
Active Partition:                      A
Active SW Version:                     10.4.1.0X
Active SW Build Version:                10.4.1.0.X.425
Active Kernel Version:                 Linux 4.9.82
Active Build Date/Time:                2018-07-20T19:07:39Z
Standby Partition:                     B
Standby SW Version:                    10.4.1.0X
Standby SW Build Version:              10.4.1.0.X.404
Standby Build Date/Time:               2018-07-19T13:37:20Z
Next-Boot:                             active[A]
```

View boot summary

```
OS10# show boot
Current system image information:
=====
Type          Boot Type      Active          Standby          Next-Boot
-----
Node-id 1    Flash Boot     [A] 10.4.1.0X   [B] 10.4.1.0X    [A] active
```

Upgrade commands

boot system

Sets the boot partition to use during the next reboot.

Syntax `boot system {active | standby}`

Parameters

- `active` — Reset the running partition as the next boot partition.
- `standby` — Set the standby partition as the next boot partition.

Default Active

Command Mode EXEC

Usage Information Use this command to configure the location of the OS10 image used to reload the software at boot time. Use the `show boot` command to view the configured next boot image. This command is applied immediately and does not require the `commit` command.

Example

```
OS10# boot system standby
```

Supported Releases 10.2.0E or later

image cancel

Cancels an active image download.

Syntax `image cancel`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information This command attempts to cancel an active file download in progress.

Example

```
OS10# image cancel
```

Supported Releases 10.2.0E or later

image copy

Copies the entire image in the active partition to the standby partition (mirror image).

Syntax `image copy active-to-standby`

Parameters `active-to-standby` — Enter to copy the entire image in the active partition to the standby partition (mirror image).

Default Not configured

Command Mode	EXEC
Usage Information	Duplicate the active, running software image to the standby image location.
Example	<pre>OS10# image copy active-to-standby</pre>
Supported Releases	10.2.0E or later

image download

Downloads a new software image to the local file system.

Syntax	<code>image download <i>file-url</i></code>
Parameters	<p><i>file-url</i> — Set the path to the image file:</p> <ul style="list-style-type: none"> • <code>ftp://userid:passwd@hostip:/filepath</code> — Enter the path to copy from the remote FTP server. • <code>http[s]://hostip:/filepath</code> — Enter the path to copy from the remote HTTP or HTTPS server. • <code>scp://userid:passwd@hostip:/filepath</code> — Enter the path to copy from the remote SCP file system. • <code>sftp://userid:passwd@hostip:/filepath</code> — Enter the path to copy from the remote SFTP file system. • <code>tftp://hostip:/filepath</code> — Enter the path to copy from the remote TFTP file system. • <code>usb://filepath</code> — Enter the path to copy from the USB file system.
Default	Not configured
Command Mode	EXEC
Usage Information	Use the <code>show image status</code> command to view the progress.
Example	<pre>OS10# image download ftp://admin@10.206.28.174:/PKGS_OS10-Enterprise-10.3.2E.55-installer-x86_64.bin</pre> <pre>OS10# image download ftp://admin@10.206.28.174:/PKGS_OS10-Enterprise-10.4.0E.55-installer-x86_64.bin</pre>
Supported Releases	10.2.0E or later

image install

Installs a new image, either from a previously downloaded file or from a remote location.

Syntax	<code>image install <i>file-url</i></code>
Parameters	<ul style="list-style-type: none"> • <i>file-url</i> — Location of the image file: <ul style="list-style-type: none"> ○ <code>ftp://userid:passwd@hostip:/filepath</code> — Enter the path to install from a remote FTP server. ○ <code>http[s]://hostip:/filepath</code> — Enter the path to install from the remote HTTP or HTTPS server. ○ <code>scp://userid:passwd@hostip:/filepath</code> — Enter the path to install from a remote SCP file system. ○ <code>sftp://userid:passwd@hostip:/filepath</code> — Enter the path to install from a remote SFTP file system. ○ <code>tftp://hostip:/filepath</code> — Enter the path to install from a remote TFTP file system.

- o `image://filename` — Enter the path to install from a local file system.
- o `usb://filepath` — Enter the path to install from the USB file system.

Default All

Command Mode EXEC

Usage Information Use the `show image status` command to view the installation progress.

Example

```
OS10# image install ftp://10.206.28.174:/PKGS_OS10-Enterprise-10.3.2E.55-
installer-x86_64.bin

OS10# image install ftp://10.206.28.174:/PKGS_OS10-Enterprise-10.4.0E.55-
installer-x86_64.bin
```

Supported Releases 10.2.0E or later

show boot

Displays boot partition-related information.

Syntax `show boot [detail]`

Parameters `detail` — (Optional) Enter to display detailed information.

Default Not configured

Command Mode EXEC

Usage Information Use the `boot system` command to set the boot partition for the next reboot.

Example

```
OS10# show boot
Current system image information:
=====
Type          Boot Type  Active      Standby      Next-Boot
-----
Node-id 1    Flash Boot [B] 10.2.0E    [A] 10.2.0E  [B] active
```

Example (Detail)

```
OS10# show boot detail
Current system image information detail:
=====
Type:                               Node-id 1
Boot Type:                           Flash Boot
Active Partition:                      B
Active SW Version:                     10.2.0E
Active Kernel Version:                 Linux 3.16.7-ckt25
Active Build Date/Time:                 2016-10-03T23:11:14Z
Standby Partition:                     A
Standby SW Version:                    10.2.0E
Standby Build Date/Time:                2016-10-03T23:11:14Z
Next-Boot:                             active[B]
```

Supported Releases 10.2.0E or later

show image status

Displays image transfer and installation information.

Syntax `show image status`

Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show image status
Image Upgrade State:  idle
=====
File Transfer State:  idle
-----
State Detail:          No download information available
Task Start:           0000-00-00T00:00:00Z
Task End:             0000-00-00T00:00:00Z
Transfer Progress:    0 %
Transfer Bytes:       0 bytes
File Size:            0 bytes
Transfer Rate:        0 kbps

Installation State:   idle
-----
State Detail:          No install information available
Task Start:           0000-00-00T00:00:00Z
Task End:             0000-00-00T00:00:00Z
```

Supported Releases	10.2.0E or later
---------------------------	------------------

show version

Displays software version information.

Syntax	show version
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show version
Dell EMC Networking OS10-Enterprise
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
OS Version: 10.4.1.0X
Build Version: 10.4.1.0.X.9
Build Time: 2018-06-12T22:18:40-0700
System Type: S4148F-ON
Architecture: x86_64
Up Time: 2 days 03:37:25
```

Supported Releases	10.2.0E or later
---------------------------	------------------

OpenFlow

Switches implement the control plane and data plane in the same hardware. Software-defined network (SDN) decouples the software (control plane) from the hardware (data plane). A centralized SDN controller handles the control plane traffic and hardware configuration for data plane flows.

The SDN controller is the "brain" of an SDN. The SDN controller uses north-bound application programming interfaces (APIs) to communicate with the business logic applications and south-bound APIs to set up controlled network devices, such as OS10 switches.

OpenFlow is an implementation of SDN. OpenFlow enables programmable networks. You can develop SDN controller network applications using representational state transfer (REST) or JAVA APIs (north-bound APIs) to business logic applications. The SDN controller uses OpenFlow south-bound APIs to communicate with the switches and relay information from business logic applications.

Advantages of an SDN include customization, accelerating new feature development, lower operating costs, and fostering an open, multi-vendor environment.

OS10 supports OpenFlow protocol versions 1.0 and 1.3.

OS10 supports OpenFlow-only mode. In this mode, the SDN controller controls data path of the switch. The OpenFlow pipeline processes all data packets.

i **NOTE:** When the switch is in OpenFlow mode, all Layer 2 (L2) and Layer 3 (L3) protocols are disabled. Link-level protocols such as Link Layer Discovery Protocol (LLDP), Dot1x, and Virtual Link Trunking (VLT) are disabled as well.

i **NOTE:** OpenFlow Hybrid mode is not supported.

Supported Platforms

- S4048-ON
- S4048T-ON
- S4100-ON
- S4248FB-ON
- S4248FBL-ON
- S6010-ON
- Z9100-ON
- Z9264F-ON

i **NOTE:** S5148F-ON and S3048-ON are not supported.

OS10 OpenFlow implementation reserves VLANs 1 and 4095.

The following is a known OpenFlow restriction in OS10:

Converting the switch from OpenFlow mode back to Normal mode removes all OpenFlow configurations. The switch returns to the pre-Openflow status. The management, interface (maximum transmission unit (MTU) and LLDP), and authentication, authorization, and accounting (AAA) settings specified in the Normal mode are retained.

To start up the switch in Factory Default mode, you must:

1. Delete the startup configuration using the `delete startup-configuration` command.
2. Enter the `reload` command.

i **NOTE:** Do not use the `no openflow` or `no mode openflow-only` command.

```
OS10# delete startup-configuration
OS10# reload
```

OpenFlow logical switch instance

In OpenFlow-only mode, you can configure only one logical switch instance. After you enable OpenFlow mode, create a logical switch instance. The logical switch instance is disabled by default. When the logical switch instance is enabled, the OpenFlow application starts the connection with the configured controller.

When you create an OpenFlow logical switch instance, all the physical interfaces are automatically added to it.

OpenFlow controller

OS10 is qualified with the following SDN controllers:

- RYU
- Open Network Operating System (ONOS)

To establish a connection with the controller, configure the IPv4 address of the controller and port ID in the OpenFlow logical switch instance. The default port is 6653. You can connect controllers to the switch in Out-of-band Connection mode. However, you can use any of the front-panel ports as the management interface using the `in-band` command. The inband port is removed from the OpenFlow switch instance and is not controlled by the controller.

The management port MTU is 1532 and the inband port MTU is 9216.

OpenFlow uses the Transmission Control Protocol (TCP) and Transport Layer Security (TLS) protocol for communication.

If the OpenFlow switch loses connection with the controller, the switch immediately enters Fail Secure mode. All the flows the controller installs are retained on the switch. The flow entries are removed based on the hard or idle timeout that you configure.

OpenFlow version 1.3

This section provides information about OpenFlow version 1.3 specifications for OS10.

Ports

An OpenFlow switch supports the following OpenFlow ports:

Table 9. Supported port types

Port types	Support
Physical ports	Supported
Logical ports	Not supported
Reserved ports	
(Required) ALL	Supported
(Required) CONTROLLER	Supported
(Required) TABLE	Not supported
(Required) IN PORT	Not supported
(Required) ANY	Supported
(Optional) LOCAL	Not supported
(Optional) NORMAL	Not supported
(Optional) FLOOD	Not supported

Flow table

An OpenFlow flow table consists of flow entries. Each flow table entry contains the following fields:

Table 10. Supported fields

Fields	Support
match_fields	Supported
priority	Supported
counters	Supported
instructions	Supported
timeouts	Supported
cookie	Not supported

Group table

Not supported

Meter table

Not supported

Instructions

Each flow entry contains a set of instructions that execute when a packet matches the entry.

Table 11. Supported instructions

Instruction	Support
(Optional) Meter meter id	Not supported
(Optional) Apply-Actions action(s)	Supported
(Optional) Clear-Actions	Not supported
(Required) Write-Actions action(s)	Supported
(Optional) Write-Metadata metadata/mask	Not supported
(Required) Goto-table next-table-id	Not supported

Action set

An action set associates with each packet.

Table 12. Supported action sets

Action set	Support
copy TTL inwards	Not supported
pop	Not supported
push-MPLS	Not supported
push-VLAN	Not supported
copy TTL outwards	Not supported
decrement TTL	Not supported
set	Supported (selective fields)

Table 12. Supported action sets (continued)

Action set	Support
qos	Not supported
group	Not supported
output	Supported

Action types

An action type associates with each packet.

Table 13. Supported action types

Action type	Support
Output	Supported
Set-queue	Not supported
Drop	Supported
Group	Not supported
Push-tag/Pop-tag	Not supported
Set-field	Partially supported <ul style="list-style-type: none"> ● Source MAC—Supported ● Destination MAC—Supported ● VLAN ID—Supported ● VLAN PCP—Supported ● IP DSCP—Supported
change-TTL	Not supported

Counters

Counters are used for statistical purposes.

Table 14. Supported counters

Required/Optional	Counter	Bits	Support
Per flow table			
Required	Reference count (active entries)	32	Supported
Optional	Packet lookups	64	Supported
Optional	Packet matches	64	Supported
Per flow entry			
Optional	Received packets	64	Supported
Optional	Received bytes	64	Supported
Required	Duration (seconds)	32	Supported
Optional	Duration (nanoseconds)	32	Supported
Per port			
Required	Received packets	64	Supported
Required	Transmitted packets	64	Supported

Table 14. Supported counters (continued)

Required/Optional	Counter	Bits	Support
Optional	Received bytes	64	Supported
Optional	Transmitted bytes	64	Supported
Optional	Receive drops	64	Not supported
Optional	Transmit drops	64	Not supported
Optional	Receive errors	64	Supported
Optional	Transmit errors	64	Supported
Optional	Receive frame alignment errors	64	Not supported
Optional	Receive overrun errors	64	Not supported
Optional	Receive CRC errors	64	Supported
Optional	Collisions	64	Supported
Required	Duration (seconds)	32	Not supported
Optional	Duration (nanoseconds)	32	Not supported
Per queue			
Required	Transmit packets	64	Not supported
Optional	Transmit bytes	64	Not supported
Optional	Transmit overrun errors	64	Not supported
Required	Duration (seconds)	32	Not supported
Optional	Duration (nanoseconds)	32	Not supported
Per group			
Optional	Reference count (flow entries)	32	Not supported
Optional	Packet count	64	Not supported
Optional	Byte count	64	Not supported
Required	Duration (seconds)	32	Not supported
Optional	Duration (nanoseconds)	32	Not supported
Per group bucket			
Optional	Packet count	64	Not supported
Optional	Byte count	64	Not supported
Per meter			
Optional	Flow count	32	Not supported
Optional	Input packet count	64	Not supported
Optional	Input byte count	64	Not supported
Required	Duration (seconds)	32	Not supported
Optional	Duration (nanoseconds)	32	Not supported
Per meter band			
Optional	In-band packet count	64	Not supported
Optional	In-band byte count	64	Not supported

OpenFlow protocol

The OpenFlow protocol supports three message types, each with multiple subtypes:

- Controller-to-switch
- Asynchronous
- Symmetric

Controller-to-switch

Table 15. Supported controller-to-switch types

Feature request	Supported
Configuration get	Supported
Configuration set	Supported
Modify-state	Supported
Read-state	Supported
Packet-out	Supported
Barrier	Supported
Role-request	Supported

Asynchronous

Table 16. Supported asynchronous types

Packet-in	Supported
Flow-removed	Supported
Port-status	Supported
Error	Supported

Symmetric

Table 17. Supported symmetric types

Hello	Supported
Echo	Supported
Experimenter	Not supported

Connection setup TCP

Table 18. Supported modes

Connection interruption	<ul style="list-style-type: none">• fail-secure-mode—Supported• fail-standalone-mode—Not supported
TLS encryption	Supported
Multiple controller	Not supported
Auxiliary connections	Not supported
Number of logical switches	One

Supported controllers

REST APIs on

- RYU
- ONOS

Flow table modification messages

Table 19. Supported messages

OFPPC_ADD=0	Supported
OFPPC_MODIFY=1	Supported
OFPPC_MODIFY_STRICT=2	Supported
OFPPC_DELETE=3	Supported
OFPPC_DELETE_STRICT=4	Supported

Message types

Table 20. Supported message types

Message Type	Message	Support
Immutable messages	OFPT_HELLO=0	Supported
	OFPT_ERROR=1	Supported
	OFPT_ECHO_REQUEST=2	Supported
	OFPT_ECHO_REPLY=3	Supported
Switch configuration messages	OFPT_FEATURES_REQUEST=5	Supported
	OFPT_FEATURES_REPLY=6	Supported
	OFPT_GET_CONFIG_REQUEST=7	Supported
	OFPT_GET_CONFIG_REPLY=8	Supported
	OFPT_SET_CONFIG=9	Supported
Asynchronous messages	OFPT_PACKET_IN=10	Supported
	OFPT_FLOW_REMOVED=11	Supported
	OFPT_PORT_STATUS=12	Supported
Controller command messages	OFPT_PACKET_OUT=13	Supported
	OFPT_FLOW_MOD=14	Supported
	OFPT_GROUP_MOD=15	Not supported
	OFPT_PORT_MOD=16	Supported
	OFPT_TABLE_MOD=17	Not supported
Multipart messages	OFPT_MULTIPART_REQUEST=18	Supported
	OFPT_MULTIPART_REPLY=19	Supported
Barrier messages	OFPT_BARRIER_REQUEST=20	Supported
	OFPT_BARRIER_REPLY=21	Supported
Queue configuration messages	OFPT_QUEUE_GET_CONFIG_REQUEST=22	Not supported
	OFPT_QUEUE_GET_CONFIG_REPLY=23	Not supported

Table 20. Supported message types (continued)

Message Type	Message	Support
Controller role change request messages	OFPT_ROLE_REQUEST=24	Not supported
	OFPT_ROLE_REPLY=25	Not supported
Asynchronous message configuration	OFPT_GET_ASYNC_REQUEST=26	Not supported
	OFPT_GET_ASYNC_REPLY=27	Not supported
	OFPT_SET_ASYNC=28	Not supported
Meters and rate limiters configuration messages	OFPT_METER_MOD=29	Not supported

Flow match fields

Table 21. Supported fields

OFPXMT_OFB_IN_PORT = 0	Supported
OFPXMT_OFB_IN_PHY_PORT = 1	Not supported
OFPXMT_OFB_METADATA = 2	Not supported
OFPXMT_OFB_ETH_DST = 3	Supported
OFPXMT_OFB_ETH_SRC = 4	Supported
OFPXMT_OFB_ETH_TYPE = 5	Supported
OFPXMT_OFB_VLAN_VID = 6	Supported
OFPXMT_OFB_VLAN_PCP = 7	Supported
OFPXMT_OFB_IP_DSCP = 8	Supported
OFPXMT_OFB_IP_ECN = 9	Supported
OFPXMT_OFB_IP_PROTO = 10	Supported
OFPXMT_OFB_IPV4_SRC = 11	Supported
OFPXMT_OFB_IPV4_DST = 12	Supported
OFPXMT_OFB_TCP_SRC = 13	Supported
OFPXMT_OFB_TCP_DST = 14	Supported
OFPXMT_OFB_UDP_SRC = 15	Supported
OFPXMT_OFB_UDP_DST = 16	Supported
OFPXMT_OFB_SCTP_SRC = 17	Not supported
OFPXMT_OFB_SCTP_DST = 18	Not supported
OFPXMT_OFB_ICMPV4_TYPE = 19	Supported

Table 21. Supported fields (continued)

OFPXMT_OFB_ICMPV4_CODE = 20	Supported
OFPXMT_OFB_ARP_OP = 21	Not supported
OFPXMT_OFB_ARP_SPA = 22	Not supported
OFPXMT_OFB_ARP_TPA = 23	Not supported
OFPXMT_OFB_ARP_SHA = 24	Not supported
OFPXMT_OFB_ARP_THA = 25	Not supported
OFPXMT_OFB_IPV6_SRC = 26	Not supported
OFPXMT_OFB_IPV6_DST = 27	Not supported
OFPXMT_OFB_IPV6_FLABEL = 28	Not supported
OFPXMT_OFB_ICMPV6_TYPE = 29	Not supported
OFPXMT_OFB_ICMPV6_CODE = 30	Not supported
OFPXMT_OFB_IPV6_ND_TARGET = 31	Not supported
OFPXMT_OFB_IPV6_ND_SLL = 32	Not supported
OFPXMT_OFB_IPV6_ND_TLL = 33	Not supported
OFPXMT_OFB_MPLS_LABEL = 34	Not supported
OFPXMT_OFB_MPLS_TC = 35	Not supported
OFPXMT_OFB_MPLS_BOS = 36	Not supported
OFPXMT_OFB_PBB_ISID = 37	Not supported
OFPXMT_OFB_TUNNEL_ID = 38	Not supported
OFPXMT_OFB_IPV6_EXTHDR = 39	Not supported

Action structures

Table 22. Supported action structures

OFPAT_OUTPUT = 0	Supported
OFPAT_COPY_TTL_OUT = 11	Not supported
OFPAT_COPY_TTL_IN = 12	Not supported
OFPAT_SET_MPLS_TTL = 15	Not supported
OFPAT_DEC_MPLS_TTL = 16	Not supported
OFPAT_PUSH_VLAN = 17	Not supported
OFPAT_POP_VLAN = 18	Not supported

Table 22. Supported action structures (continued)

OFFPAT_PUSH_MPLS = 19	Not supported
OFFPAT_POP_MPLS = 20	Not supported
OFFPAT_SET_QUEUE = 21	Not supported
OFFPAT_GROUP = 22	Not supported
OFFPAT_SET_NW_TTL = 23	Not supported
OFFPAT_DEC_NW_TTL = 24	Not supported
OFFPAT_SET_FIELD = 25	Supported
OFFPAT_PUSH_PBB = 26	Not supported
OFFPAT_POP_PBB = 27	Not supported

Capabilities supported by the data path

Table 23. Supported capabilities

OFPC_FLOW_STATS = 1 << 0	Supported
OFPC_TABLE_STATS = 1 << 1	Not supported
OFPC_PORT_STATS = 1 << 2	Supported
OFPC_GROUP_STATS = 1 << 3	Not supported
OFPC_IP_REASM = 1 << 5	Not supported
OFPC_QUEUE_STATS = 1 << 6	Not supported
OFPC_PORT_BLOCKED = 1 << 8	Not supported

Multipart message types

Table 24. Supported message types

Message type description	Request/Reply Body	Message	Support
Description of this OpenFlow switch	<ul style="list-style-type: none"> The request body is empty The reply body is struct ofp_desc 	OFFPMP_DESC = 0	Supported
Individual flow statistics	<ul style="list-style-type: none"> The request body is struct ofp_flow_stats_request The reply body is an array of struct ofp_flow_stats 	OFFPMP_FLOW = 1	Supported
Aggregate flow statistics	<ul style="list-style-type: none"> The request body is struct ofp_aggregate_stats_request The reply body is struct ofp_aggregate_stats_reply 	OFFPMP_AGGREGATE = 2	Supported
Flow table statistics	<ul style="list-style-type: none"> The request body is empty 	OFFPMP_TABLE = 3	Supported

Table 24. Supported message types (continued)

Message type description	Request/Reply Body	Message	Support
	<ul style="list-style-type: none"> The reply body is an array of struct ofp_table_stats 		
Port statistics	<ul style="list-style-type: none"> The request body is struct ofp_port_stats_request The reply body is an array of struct ofp_port_stats 	OFPMP_PORT_STATS = 4	Supported
Queue statistics for a port	<ul style="list-style-type: none"> The request body is struct ofp_queue_stats_request The reply body is an array of struct ofp_queue_stats 	OFPMP_QUEUE = 5	Not supported
Group counter statistics	<ul style="list-style-type: none"> The request body is struct ofp_group_stats_request The reply is an array of struct ofp_group_stats 	OFPMP_GROUP = 6	Not supported
Group description	<ul style="list-style-type: none"> The request body is empty The reply body is an array of struct ofp_group_desc_stats 	OFPMP_GROUP_DESC = 7	Not supported
Group features	<ul style="list-style-type: none"> The request body is empty The reply body is struct ofp_group_features 	OFPMP_GROUP_FEATURES = 8	Not supported
Meter statistics	<ul style="list-style-type: none"> The request body is struct ofp_meter_multipart_requests The reply body is an array of struct ofp_meter_stats 	OFPMP_METER = 9	Not supported
Meter configuration	<ul style="list-style-type: none"> The request body is struct ofp_meter_multipart_requests The reply body is an array of struct ofp_meter_config 	OFPMP_METER_CONFIG = 10	Not supported
Meter features	<ul style="list-style-type: none"> The request body is empty The reply body is struct ofp_meter_features 	OFPMP_METER_FEATURES = 11	Not supported
Table features	<ul style="list-style-type: none"> The request body is empty or contains an array of struct ofp_table_features that includes the controller's desired view of the switch. If the switch is unable to set the specified view an error is returned The reply body is an array of struct ofp_table_features 	OFPMP_TABLE_FEATURES = 12	Supported
Port description	<ul style="list-style-type: none"> The request body is empty The reply body is an array of struct ofp_port 	OFPMP_PORT_DESC = 13	Supported

Switch description

The OFPMP_DESC multipart request type includes information about the switch manufacturer, hardware revision, software revision, serial number, and description.

Table 25. Supported descriptions

char mfr_desc[DESC_STR_LEN]	Supported
char hw_desc[DESC_STR_LEN]	Supported
char sw_desc[DESC_STR_LEN]	Supported
char serial_num[SERIAL_NUM_LEN]	Supported
char dp_desc[DESC_STR_LEN]	Supported

Property type

Table 26. Supported properties

OFPTFPT_INSTRUCTIONS = 0	Supported
OFPTFPT_INSTRUCTIONS_MISS = 1	Not supported
OFPTFPT_NEXT_TABLES = 2	Not supported
OFPTFPT_NEXT_TABLES_MISS = 3	Not supported
OFPTFPT_WRITE_ACTIONS = 4	Supported
OFPTFPT_WRITE_ACTIONS_MISS = 5	Not supported
OFPTFPT_APPLY_ACTIONS = 6	Supported
OFPTFPT_APPLY_ACTIONS_MISS = 7	Not supported
OFPTFPT_MATCH = 8	Supported
OFPTFPT_WILDCARDS = 10	Supported
OFPTFPT_WRITE_SETFIELD = 12	Supported
OFPTFPT_WRITE_SETFIELD_MISS = 13	Not supported
OFPTFPT_APPLY_SETFIELD = 14	Supported
OFPTFPT_APPLY_SETFIELD_MISS = 15	Not supported

Group configuration

Table 27. Supported configurations

OFPGFC_SELECT_WEIGHT = 1 << 0	Not supported
OFPGFC_SELECT_LIVENESS = 1 << 1	Not supported
OFPGFC_CHAINING = 1 << 2	Not supported
OFPGFC_CHAINING_CHECKS = 1 << 3	Not supported

Controller roles

Table 28. Supported controller roles

OFPCR_ROLE_NOCHANGE = 0	Not supported
OFPCR_ROLE_EQUAL = 1	Supported
OFPCR_ROLE_MASTER = 2	Supported
OFPCR_ROLE_SLAVE = 3	Not supported

Packet-in reasons

Table 29. Supported reasons

OFPR_NO_MATCH = 0	Supported
OFPR_ACTION = 1	Supported
OFPR_INVALID_TTL = 2	Not supported

Flow-removed reasons

Table 30. Supported reasons

OFPRR_IDLE_TIMEOUT = 0	Supported
OFPRR_HARD_TIMEOUT = 1	Supported
OFPRR_DELETE = 2	Supported
OFPRR_GROUP_DELETE = 3	Not supported

Error types from switch to controller

Table 31. Supported error types

OFPET_HELLO_FAILED = 0	Supported
OFPET_BAD_REQUEST = 1	Supported
OFPET_BAD_ACTION = 2	Supported
OFPET_BAD_INSTRUCTION = 3	Supported
OFPET_BAD_MATCH = 4	Supported
OFPET_FLOW_MOD_FAILED = 5	Supported
OFPET_GROUP_MOD_FAILED = 6	Not supported
OFPET_PORT_MOD_FAILED = 7	Supported
OFPET_TABLE_MOD_FAILED = 8	Not supported
OFPET_QUEUE_OP_FAILED = 9	Not supported

Table 31. Supported error types (continued)

OFPET_SWITCH_CONFIG_FAILED = 10	Not supported
OFPET_ROLE_REQUEST_FAILED = 11	Not supported
OFPET_METER_MOD_FAILED = 12	Not supported
OFPET_TABLE_FEATURES_FAILED = 13	Not supported
Bad request code	
OFPBRC_BAD_VERSION = 0	Supported
OFPBRC_BAD_TYPE = 1	Supported
OFPBRC_BAD_MULTIPART = 2	Not supported
OFPBRC_BAD_EXPERIMENTER = 3	Not supported
OFPBRC_BAD_EXP_TYPE = 4	Not supported
OFPBRC_EPERM = 5	Not supported
OFPBRC_BAD_LEN = 6	Supported
OFPBRC_BUFFER_EMPTY = 7	Not supported
OFPBRC_BUFFER_UNKNOWN = 8	Not supported
OFPBRC_BAD_TABLE_ID = 9	Supported
OFPBRC_IS_SLAVE = 10	Not supported
OFPBRC_BAD_PORT = 11	Supported
OFPBRC_BAD_PACKET = 12	Not supported
OFPBRC_MULTIPART_BUFFER_OVERFLOW = 13	Not supported
Bad action code	
OFPBAC_BAD_TYPE = 0	Supported
OFPBAC_BAD_LEN = 1	Supported
OFPBAC_BAD_EXPERIMENTER = 2	Not supported
OFPBAC_BAD_EXP_TYPE = 3	Not supported
OFPBAC_BAD_OUT_PORT = 4	Supported
OFPBAC_BAD_ARGUMENT = 5	Supported
OFPBAC_EPERM = 6	Not supported
OFPBAC_TOO_MANY = 7	Supported
OFPBAC_BAD_QUEUE = 8	Not supported

Table 31. Supported error types (continued)

OFPBAC_BAD_OUT_GROUP = 9	Not supported
OFPBAC_MATCH_INCONSISTENT = 10	Not supported
OFPBAC_UNSUPPORTED_ORDER = 11	Not supported
OFPBAC_BAD_TAG = 12	Not supported
OFPBAC_BAD_SET_TYPE = 13	Not supported
OFPBAC_BAD_SET_LEN = 14	Not supported
OFPBAC_BAD_SET_ARGUMENT = 15	Supported
Bad instruction code	
OFPBIC_UNKNOWN_INST = 0	Not supported
OFPBIC_UNSUP_INST = 1	Not supported
OFPBIC_BAD_TABLE_ID = 2	Not supported
OFPBIC_UNSUP_METADATA = 3	Not supported
OFPBIC_UNSUP_METADATA_MASK = 4	Not supported
OFPBIC_BAD_EXPERIMENTER = 5	Not supported
OFPBIC_BAD_EXP_TYPE = 6	Not supported
OFPBIC_BAD_LEN = 7	Not supported
OFPBIC_EPERM = 8	Not supported
Bad match code	
OFPBMC_BAD_TYPE = 0	Not supported
OFPBMC_BAD_LEN = 1	Not supported
OFPBMC_BAD_TAG = 2	Not supported
OFPBMC_BAD_DL_ADDR_MASK = 3	Not supported
OFPBMC_BAD_NW_ADDR_MASK = 4	Not supported
OFPBMC_BAD_WILDCARDS = 5	Not supported
OFPBMC_BAD_FIELD = 6	Not supported
OFPBMC_BAD_VALUE = 7	Not supported
OFPBMC_BAD_MASK = 8	Not supported
OFPBMC_BAD_PREREQ = 9	Not supported
OFPBMC_DUP_FIELD = 10	Not supported

Table 31. Supported error types (continued)

OFPBMC_EPERM = 11	Not supported
Flow modification failed code	
OFFPMFC_UNKNOWN = 0	Supported
OFFPMFC_TABLE_FULL = 1	Supported
OFFPMFC_BAD_TABLE_ID = 2	Supported
OFFPMFC_OVERLAP = 3	Supported
OFFPMFC_EPERM = 4	Not supported
OFFPMFC_BAD_TIMEOUT = 5	Not supported
OFFPMFC_BAD_COMMAND = 6	Supported
OFFPMFC_BAD_FLAGS = 7	Not supported
Group modification failed code	
OFFGMFC_GROUP_EXISTS = 0	Not supported
OFFGMFC_INVALID_GROUP = 1	Not supported
OFFGMFC_WEIGHT_UNSUPPORTED = 2	Not supported
OFFGMFC_OUT_OF_GROUPS = 3	Not supported
OFFGMFC_OUT_OF_BUCKETS = 4	Not supported
OFFGMFC_CHAINING_UNSUPPORTED = 5	Not supported
OFFGMFC_WATCH_UNSUPPORTED = 6	Not supported
OFFGMFC_LOOP = 7	Not supported
OFFGMFC_UNKNOWN_GROUP = 8	Not supported
OFFGMFC_CHAINED_GROUP = 9	Not supported
OFFGMFC_BAD_TYPE = 10	Not supported
OFFGMFC_BAD_COMMAND = 11	Not supported
OFFGMFC_BAD_BUCKET = 12	Not supported
OFFGMFC_BAD_WATCH = 13	Not supported
OFFGMFC_EPERM = 14	Not supported
Port modification failed code	
OFFPMFC_BAD_PORT = 0	Supported
OFFPMFC_BAD_HW_ADDR = 1	Supported

Table 31. Supported error types (continued)

OFPPMFC_BAD_CONFIG = 2	Not supported
OFPPMFC_BAD_ADVERTISE = 3	Not supported
OFPPMFC_EPERM = 4	Not supported
Table modification failed code	
OFPTMFC_BAD_TABLE = 0	Supported
OFPTMFC_BAD_CONFIG = 1	Not supported
OFPTMFC_EPERM = 2	Not supported
Queue operation failed code	
OFPQOFC_BAD_PORT = 0	Supported
OFPQOFC_BAD_QUEUE = 1	Not supported
OFPQOFC_EPERM = 2	Not supported
Switch configuration failed code	
OFPSCFC_BAD_FLAGS = 0	Not supported
OFPSCFC_BAD_LEN = 1	Not supported
OFPSCFC_EPERM = 2	Not supported
Role request failed code	
OFPRRFC_STALE = 0	Not supported
OFPRRFC_UNSUP = 1	Not supported
OFPRRFC_BAD_ROLE = 2	Not supported
Table features failed code	
OFPTFFC_BAD_TABLE = 0	Supported
OFPTFFC_BAD_METADATA = 1	Not supported
OFPTFFC_BAD_TYPE = 2	Not supported
OFPTFFC_BAD_LEN = 3	Not supported
OFPTFFC_BAD_ARGUMENT = 4	Not supported
OFPTFFC_EPERM = 5	Not supported

OpenFlow use cases

OS10 OpenFlow protocol support allows the flexibility of using vendor-neutral applications and to use applications that you create. For example, the OS10 OpenFlow implementation supports L2 applications similar to the ones found in the following websites:

- <https://github.com/osrg/ryu/tree/master/ryu/app> (only L2 applications are supported)
- <https://github.com/osrg/ryu/tree/master/ryu/app>

NOTE: OS10 supports applications based on OpenFlow versions 1.0 and 1.3.

- **Switching loop removal**

Consider the case of a single broadcast domain where switching loops are common. This issue occurs because of redundant paths in an L2 network.

Switching loops create broadcast storms with broadcasts and multicasts being forwarded out of every switch port. Every switch in the network repeatedly re-broadcasts the messages and floods the entire network.

To solve broadcast storms in an OpenFlow network, a centralized controller makes all the control plane decisions and manages the switches. The controller has the complete view of the topology. MAC address learning is centralized. OpenFlow identifies the correct path and forwards the packets to the relevant switch thereby avoiding switching loops.

- **Reactive flow installation**

Consider the case of dynamic learning of flows for bidirectional traffic. Flows are learnt as and when a packet arrives.

With dynamic learning in an OpenFlow network, the OpenFlow switch receives a packet that does not match the flow table entries and sends the packet to the SDN controller to process it. The controller identifies the path the packet has to traverse and updates the flow table with a new entry. The controller also decides the caching time of the flow table entries.

Configure OpenFlow

Ensure IP connectivity between the switch and the controller. When you convert the switch from Normal mode to OpenFlow mode, the switch retains the management, interface, and AAA settings.

The following example lists the minimum configuration needed to establish the connection between the OpenFlow controller and a logical switch instance.

1. Enter the OPENFLOW configuration mode.

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)#
```

2. Enable the OpenFlow-only mode.

```
OS10 (config-openflow)# mode openflow-only
```

The system prompts you to reload the switch. Enter `yes` to enable OpenFlow-only mode.

NOTE: When the switch starts up in OpenFlow mode, it disables all L2 and 3 protocols. Many CLI commands are not available when the switch is in OpenFlow-only mode. For a list of commands that are available in OpenFlow-only mode, see [CLI commands available in the OpenFlow-only mode](#).

3. Configure a logical switch instance.

- a. Option 1; for out-of-band management:

- i. Configure an IP address for the management port. Ensure that there is IP connectivity between the switch and the controller.

```
OS10# configure terminal
OS10 (config)# interface management 0/0
OS10 (conf-if-ma-0/0)# ip address 11.1.1.1/24
OS10 (conf-if-ma-0/0)# no shutdown
OS10 (conf-if-ma-0/0)# exit
```

- ii. Configure the logical switch instance, *of-switch-1*.

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
```

- b. Option 2; for in-band management:

- i. Configure one of the front-panel ports as the management port.

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# in-band-mgmt interface ethernet 1/1/1
OS10 (config-openflow)#
```

- ii. Configure an IPv4 address on the front-panel management port.

```
OS10# configure terminal
OS10 (config)# interface ethernet 1/1/1
OS10 (conf-if-eth1/1/1)# ip address 11.1.1.1/24
OS10 (conf-if-eth1/1/1)# no shutdown
```

- iii. Configure the logical switch instance, *of-switch-1*.

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
```

4. Configure the OpenFlow controller to establish a connection with the logical switch instance.

```
OS10 (config-openflow-switch)# controller ipv4 ip-address port port-id
```

```
OS10 (config-openflow-switch)# controller ipv4 10.1.1.1 port 6633
```

where a.b.c.d is the IP address of the controller and port 6633 is for OpenFlow communication.

5. Enter the `no shutdown` command to enable the logical switch instance.

```
OS10 (config-openflow-switch) no shutdown
```

Establish TLS connection

- Generate the switch and controller certificates from a server that supports public-key infrastructure (PKI). You need the following certificates:
 - Controller certificate
 - Switch certificate
 - Private key file to verify the switch certificate
- The certificates and private key files must be in the Privacy-Enhanced Mail (PEM) format.

For certificate-based authentication, you must establish a TLS connection between the switch and the controller before you configure OpenFlow on the switch. The following procedure explains how to install the controller and switch certificates on the OS10 switch. Refer to the controller documentation for information on how to install the certificates on the controller.

NOTE: This procedure is optional. Use this procedure if you want to configure certificate-based authentication between the switch and the controller.

1. Log in to the OS10 switch with administrator credentials.
2. Enter the following command to copy the certificates to the OS10 switch.

In the following commands, the destination path and the destination file name on the OS10 switch, for example, `config://../openflow/cacert.pem`, remain the same in your deployment. Ensure that you enter the destination path and destination file names as specified in the following example:

```
OS10# copy scp://username:password@server-ip/full-path-to-the-certificates/controller-
cert.pem config://../openflow/cacert.pem
OS10# copy scp://username:password@server-ip/full-path-to-the-certificates/switch-
```

```
cert.pem config://../openflow/sc-cert.pem
OS10# copy scp://username:password@server-ip/full-path-to-the-certificates/switch-
privkey.pem config://../openflow/sc-privkey.pem
```

where *server-ip* refers to the server where you have stored the certificates, and *username* and *password* refers to the credentials you need to access the server with the certificates.

3. Perform the steps described in the [Configure OpenFlow protocol on the switch](#) topic to configure OpenFlow.

OpenFlow commands

controller

Configures an OpenFlow controller that the logical switch instance connects to.

Syntax	<code>controller ipv4 <i>ipv4-address</i> [port <i>port-number</i>] [security {none tls}]</code>						
Parameters	<ul style="list-style-type: none">• <code>ipv4 <i>ipv4-address</i></code>—Enter <code>ipv4</code>, then the IP address of the controller.• <code>port <i>port-number</i></code>—Enter the keyword, then the port number, from 1 to 65,535. The default port is 6653.• <code>security {none tls}</code>—Specify the type of connection. The default is <code>security none</code>. The TCP connection is used.						
Default	TCP. The default port number is 6653.						
Command Mode	OPENFLOW SWITCH CONFIGURATION						
Usage Information	If you specify the <code>security tls</code> option, the OpenFlow application looks for the following certificates and private key in the following locations specified for certificate-based authentication. For information about obtaining certificates and installing them on the switch and the controller, see Establish TLS connection between the switch and the controller .						
	<table><tr><td>ca_cert (certificate that identifies the controller as being trustworthy)</td><td><code>/config/etc/opt/dell/os10/openflow/cacert.pem</code></td></tr><tr><td>certificate (certificate that identifies the switch as being trustworthy)</td><td><code>/config/etc/opt/dell/os10/openflow/sc-cert.pem</code></td></tr><tr><td>private key (the private key corresponding to the switch certificate)</td><td><code>/config/etc/opt/dell/os10/openflow/sc-privkey.pem</code></td></tr></table>	ca_cert (certificate that identifies the controller as being trustworthy)	<code>/config/etc/opt/dell/os10/openflow/cacert.pem</code>	certificate (certificate that identifies the switch as being trustworthy)	<code>/config/etc/opt/dell/os10/openflow/sc-cert.pem</code>	private key (the private key corresponding to the switch certificate)	<code>/config/etc/opt/dell/os10/openflow/sc-privkey.pem</code>
ca_cert (certificate that identifies the controller as being trustworthy)	<code>/config/etc/opt/dell/os10/openflow/cacert.pem</code>						
certificate (certificate that identifies the switch as being trustworthy)	<code>/config/etc/opt/dell/os10/openflow/sc-cert.pem</code>						
private key (the private key corresponding to the switch certificate)	<code>/config/etc/opt/dell/os10/openflow/sc-privkey.pem</code>						

Example The following example configures an OpenFlow controller with IP address 10.11.63.56 on port 6633 for the logical switch instance, of-switch-1.

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# controller ipv4 10.11.63.56 port 6633
OS10 (config-openflow-switch)#
```

Supported Releases 10.4.1 or later

dpid-mac-address

Specifies the MAC address bits of the datapath ID (DPID) of the logical switch instance.

Syntax `dpid-mac-address MAC-address`

Parameters `MAC-address`—48-bit MAC address in hexadecimal notation, nn:nn:nn:nn:nn:nn

Default MAC address

Command Mode OPENFLOW SWITCH CONFIGURATION

Usage Information The controller uses the DPID to identify the logical switch instance. The DPID is a 64-bit number that is sent to the controller in the `features_reply` message. The DPID is constructed from the instance ID, which is the most significant 16 bits (default to 0) and the DPID-MAC-ADDRESS, which is the least significant 48 bits. OS10 currently supports only one logical switch instance and the instance ID is automatically set to 0. This value is not configurable.

You can use this command to modify the MAC address bits of the DPID.

Example DPID MAC address is 00:00:00:00:00:0a.

```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# dpid-mac-address 00:00:00:00:00:0a
OS10 (config-openflow-switch)#
```

Supported Releases 10.4.1 or later

in-band-mgmt

To use one of the front-panel ports as the management interface that the SDN controller connects to.

Syntax `in-band-mgmt interface ethernet node/slot/port[:subport]`

Parameters `node/slot/port[:subport]`—Enter the physical port information.

Default None

Command Mode OPENFLOW CONFIGURATION

Usage Information Use this command to convert any one of the front-panel ports as the management interface. This port will not be part of the OpenFlow logical switch instance. All the ports are layer 2 ports by default. If you configure one of the front-panel ports as the management interface, the port becomes an L3 port. You can configure a layer 3 IPv4 address only to the front-panel port that you have specified in this command. Ensure that you have IP connectivity between the specified port and the controller. Running the `no` form of this command removes this configuration and the front-panel port becomes part of the OpenFlow logical switch instance.

Example

```
OS10# configure terminal
OS10(config)# openflow
OS10 (config-openflow)# in-band-mgmt interface ethernet 1/1/1
OS10 (config-openflow)# no shutdown
```

Supported Releases 10.4.1 or later

max-backoff

To configure the time interval in seconds that the logical switch instance waits after requesting a connection with the OpenFlow controller.

Syntax	<code>max-backoff interval</code>
Parameters	<i>interval</i> —Enter the amount of time in seconds that the logical switch instance waits after it attempts to establish a connection with the OpenFlow controller. The range is from 1 to 65,535.
Default	The default value is 8 seconds.
Command Mode	OPENFLOW SWITCH CONFIGURATION
Usage Information	If the interval time lapses, the logical switch instance re-attempts to establish a connection with the OpenFlow controller.

Example


```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# max-backoff 25
OS10 (config-openflow-switch)#
```

Supported Releases	10.4.1 or later
---------------------------	-----------------

mode openflow-only

To enable the OpenFlow-only mode on the switch.

Syntax	<code>mode openflow-only</code>
Parameters	None
Default	None
Command Mode	OPENFLOW CONFIGURATION
Usage Information	The <code>mode openflow-only</code> command is used to enable the OpenFlow-only mode. This command reloads the switch and the switch boots in the OpenFlow-only mode. This command deletes all layer 2 and layer 3 configurations. However, the system management and AAA configurations are retained. The <code>no</code> form of this command prompts you for a switch reload. If you enter <code>yes</code> , the switch deletes all OpenFlow configuration (including controller IP, port, certificates), reloads, and returns to the normal mode.

 **NOTE:** See [CLI commands available in the OpenFlow-only mode](#) for a list of available commands when the switch is in the OpenFlow-only mode.

Example

```
OS10 (config-openflow)# mode openflow-only
OS10 (config-openflow)#
```

Supported Releases	10.4.1 or later
---------------------------	-----------------

openflow

To enter in to the OPENFLOW configuration mode.

Syntax	<code>openflow</code>
Parameters	None
Default	None

Command Mode	CONFIGURATION
Usage Information	All OpenFlow configurations are performed from this configuration mode. Running the <code>no</code> form of this command from the OpenFlow mode prompts for a switch reload. If you enter <code>yes</code> , the system deletes all OpenFlow configurations and the switch returns to the normal mode after the reload.
Example	<pre>OS10# configure terminal OS10(config)# openflow OS10 (config-openflow)#</pre>
Supported Releases	10.4.1 or later

probe-interval

To configure the echo request interval in seconds for the controller configured with the logical switch instance.

Syntax	<code>probe-interval interval</code>
Parameters	<i>interval</i> —Enter the amount of time in seconds between the <code>keepalive</code> messages (echo requests). The range is from 1 to 65,535.
Default	The default value is 5 seconds.
Command Mode	OPENFLOW SWITCH CONFIGURATION
Usage Information	None
Example	<pre>OS10 (config)# openflow OS10 (config-openflow)# switch of-switch-1 OS10 (config-openflow-switch)# probe-interval 20 OS10 (config-openflow-switch)#</pre>
Supported Releases	10.4.1 or later

protocol-version

To specify the protocol version to be used by the logical switch interface.

Syntax	<code>protocol-version version</code>
Parameters	<p><i>version</i>—Choose from one of the following options:</p> <ul style="list-style-type: none"> <code>negotiate</code>—Enter the keyword <code>negotiate</code> to configure the switch to negotiate versions 1.0 or 1.3 with the controller. The highest of the supported versions is selected. <code>1.0</code>—Enter <code>1.0</code> to specify the logical switch instance's OpenFlow protocol version as 1.0. <code>1.3</code>—Enter <code>1.3</code> to specify the logical switch instance's OpenFlow protocol version as 1.3.
Default	By default, the protocol version is set to <code>negotiate</code> .
Command Mode	OPENFLOW SWITCH CONFIGURATION
Usage Information	<p>i NOTE: This command should be run when the logical switch instance is disabled. Use the <code>shutdown</code> command to disable the logical switch instance. After you run this command, enter the <code>no shutdown</code> command to enable the logical switch instance again.</p> <ul style="list-style-type: none"> When you specify the option, <code>negotiate</code>, the switch negotiates versions 1.0 and 1.3 with the controller and selects the highest of the versions supported by the controller. The negotiation is based on the hello handshake mechanism described in the OpenFlow Specification 1.3.

- When you specify the option, 1.0, the switch establishes a connection with the controller that supports version 1.0 only.
- When you specify the option, 1.3, the switch establishes a connection with the controller that supports version 1.3 only.

Example

The following example shows a logical switch instance, of-switch-1, configured to interact with controllers that support the OpenFlow protocol version 1.3.

```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# shutdown
OS10 (config-openflow-switch)# protocol-version 1.3
OS10 (config-openflow-switch)# no shutdown
OS10 (config-openflow-switch)#
```

Supported Releases

10.4.1 or later

rate-limit packet_in

To configure the maximum packet rate for the controller connection, and the maximum packets permitted in a burst of packets sent to the controller in a second.

Syntax

```
rate-limit packet_in controller-packet-rate [burst maximum-packets-to-controller]
```

Parameters

- *controller-packet-rate*—Rate in packets per second to be configured for the controller's OpenFlow channel connection. Range is from 100 to 268000000 seconds. The default is 0 seconds (disabled).
- *maximum-packets-to-controller*—Burst in packets configured for the controller's OpenFlow channel connection. Range is 25 to 1073000. The default is 0 seconds (disabled). This parameter is optional and is set to 25% of the configured rate value, when this value is not configured.

Default

Rate limiting is disabled on the OpenFlow connections by default.

Command Mode

OPENFLOW SWITCH CONFIGURATION

Usage Information

The rate and burst that are specified are set by the OpenFlow application for the controller's connection with the logical switch instance. Actual rate and burst on the controller can go up to a maximum of two times the configured values. For example, when a rate of 1000 PPS and a burst of 300 packet bursts per second is configured on an OpenFlow logical switch instance connected to a controller, the packets can egress on the connection at rates of up to 2000 PPS and 600 packet bursts per second. The `no` form of this command disables rate limiting on the controller connection.

NOTE: The `rate-limit packet_in` command is a software rate limiting command and is applicable only to the OpenFlow channel connection between the controller and the logical switch instance. This command is not related to the switch's data-plane rate limits.

Example

The following example configures an OpenFlow controller connection with the logical switch instance, of-switch-1 at a rate of 1000 PPS and packet bursts of 300 packets.

```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# controller ipv4 10.11.63.56 port 6633
OS10 (config-openflow-switch)# rate-limit packet_in 1000 burst 300
OS10 (config-openflow-switch)#
```

Supported Releases

10.4.1 or later

show openflow

To display general information related to OpenFlow that is applicable to the switch and the logical switch instance.

Syntax show openflow

Parameters None

Default None

Command Mode EXEC

Usage Information None

Example

```
OS10# show openflow
Manufacturer           : DELL
Hardware Description   : Z9100-ON
Software Description   : Dell Networking OS10-Premium, Dell
Networking Application Software Version: 10.4.1.0X
Serial Number          : CN0V1W3RCES0079L0018
Capabilities           : port, table, flow
Switch mode            : openflow-only
Match fields           :
  Layer-1 : in-port
  Layer-2 : eth-src, eth-dst, eth-type, vlan-id, vlan-pcp
  Layer-3 : ipv4-src, ipv4-dst, ip-protocol, ip-dscp, ip-ecn
  Layer-4 : tcp-src, tcp-dst, udp-src, udp-dst, icmpv4-type, icmpv4-
code
Instructions           : apply-actions, write-actions
Actions                : output, set-field
Set field actions      : eth-src, eth-dst, vlan-id, vlan-pcp,
ip-dscp
TLS parameters         :
  certificate identifying trustworthy controller : /config/etc/opt/
dell/os10/openflow/cacert.pem
  certificate identifying trustworthy switch    : /config/etc/opt/
dell/os10/openflow/sc-cert.pem
  private key                                   : /config/etc/opt/
dell/os10/openflow/sc-privkey.pem
```

Supported Releases 10.4.1 or later

show openflow flows

To display the OpenFlow flows for a specific logical switch instance.

Syntax show openflow switch *logical-switch-name* flows

Parameters *logical-switch-name*—Enter the logical switch instance name for which you want to view the flow information.

Default None

Command Mode EXEC

Usage Information None

Example

```
OS10# show openflow switch of-switch-1 flows
Logical switch name: of-switch-1
Total flows: 1
  Flow: 0
    Table ID: 0, Table: Ingress ACL TCAM table
```

```

Flow ID: 0
Priority: 32768, Cookie: 0
Hard Timeout: 0, Idle Timeout: 0
Packets: 0, Bytes: 0
Match Parameters:
  In Port: ethernet1/1/1
  EType: 0x800
  SMAC: 00:0b:c4:a8:22:b0/ff:ff:ff:ff:ff:ff
  DMAC: 00:0b:c4:a8:22:b1/ff:ff:ff:ff:ff:ff
  VLAN id: 2/4095
  VLAN PCP: 1
  IP DSCP: 4
  IP ECN: 1
  IP Proto: 1
  Src Ip: 10.0.0.1/255.255.255.255
  Dst Ip: 20.0.0.1/255.255.255.255
  ICMPv4 Type: 1
  ICMPv4 Code: 10
  L4 Src Port: *
  L4 Dst Port: *
Apply-Actions: Output= ethernet1/1/2, ethernet1/1/3:1
Write-Actions: Drop

```

Supported Releases 10.4.1 or later

show openflow ports

To display the openflow ports for a specific logical switch instance.

Syntax `show openflow switch logical-switch-name ports`

Parameters *logical-switch-name*—Name of the logical switch instance whose port information you want to view.

Default None

Command Mode EXEC

Usage Information None

Example

```

OS10# show openflow switch of-switch-1 ports
Logical switch name: of-switch-1
Interface Name      of-port ID  Config-State      Link-State  SPEED
  DUPLEX  AUTONEG  TYPE
ethernet1/1/1      1          PORT_UP (CLI)    LINK_UP     40GB
  FD      YES      COPPER
ethernet1/1/2      5          PORT_UP (CLI)    LINK_UP     40GB
  FD      YES      COPPER
ethernet1/1/3:1    9          PORT_UP (CLI)    LINK_UP     10GB
  FD      NO       FIBER
ethernet1/1/3:2    10         PORT_UP (CLI)    LINK_DOWN   0MB
  FD      NO       FIBER
ethernet1/1/3:3    11         PORT_UP (CLI)    LINK_DOWN   0MB
  FD      NO       FIBER
ethernet1/1/3:4    12         PORT_UP (CLI)    LINK_DOWN   0MB
  FD      NO       FIBER
ethernet1/1/4      13         PORT_UP (CLI)    LINK_UP     40GB
  FD      YES      COPPER
ethernet1/1/5:1    17         PORT_UP (CLI)    LINK_UP     10GB
  FD      NO       FIBER
ethernet1/1/5:2    18         PORT_UP (CLI)    LINK_DOWN   0MB
  FD      NO       FIBER
ethernet1/1/5:3    19         PORT_UP (CLI)    LINK_DOWN   0MB
  FD      NO       FIBER
ethernet1/1/5:4    20         PORT_UP (CLI)    LINK_DOWN   0MB
  FD      NO       FIBER
ethernet1/1/6      21         PORT_UP (CLI)    LINK_DOWN   0MB

```

FD	NO	NONE			
ethernet1/1/7		25	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/8		29	PORT_UP (CLI)	LINK_DOWN	0MB
FD	YES	COPPER			
ethernet1/1/9		33	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/10		37	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/11		41	PORT_UP (CLI)	LINK_UP	40GB
FD	YES	COPPER			
ethernet1/1/12		45	PORT_UP (CLI)	LINK_UP	40GB
FD	YES	COPPER			
ethernet1/1/13		49	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/14		53	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/15		57	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/16		61	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/17		65	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/18		69	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/19		73	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/20		77	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/21		81	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/22		85	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/23		89	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/24		93	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/25		97	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	COPPER			
ethernet1/1/26		101	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	COPPER			
ethernet1/1/27		105	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/28		109	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/29		113	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/30		117	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/31		121	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			
ethernet1/1/32		125	PORT_UP (CLI)	LINK_DOWN	0MB
FD	NO	NONE			

Supported Releases 10.4.1 or later

show openflow switch

To display OpenFlow parameters of the switch instance.

Syntax show openflow switch

Parameters None

Default None

Command Mode EXEC

Usage Information None

Example

```
OS10# show openflow switch
Logical switch name: of-switch-1
Internal switch instance ID: 0
Config state: true
Signal Version: negotiate
Data plane: secure
Max backoff (sec): 8
Probe Interval (sec): 5
DPID: 90:b1:1c:f4:a5:23
Switch Name : of-switch-1
Number of buffers: 0
Number of tables: 1
  Table ID: 0
  Table name: Ingress ACL TCAM table
  Max entries: 1000
  Active entries: 0
  Lookup count: 0
  Matched count: 0
Controllers:
  10.16.208.150:6633, Protocol: none,
  packet-in Rate limit (packet per second): 0
  packet-in Burst limit: 0
```

Supported Releases 10.4.1 or later

show openflow switch controllers

To display OpenFlow controllers for a specific logical switch instance.

Syntax `show openflow switch logical-switch-name controllers`

Parameters *logical-switch-name*—Name of the logical switch instance that you want to query.

Default None

Command Mode EXEC

Usage Information None

Example

```
OS10# show openflow switch of-switch-1 controllers
Logical switch name: of-switch-1
Total Controllers: 1
  Controller: 1
    Target: 10.16.208.150:6633
    Protocol: TCP
    Connected: NO
    Role: Equal
    Last_error: Network is unreachable
    State: BACKOFF
    sec_since_disconnect: 0
```

Supported Releases 10.4.1 or later

switch

To create a logical switch instance, or modify an existing logical switch instance.

Syntax `switch logical-switch-name`

Parameters `logical-switch-name`—Enter the name of the logical switch instance that has to be created, or modified. OS10 supports only one instance of the logical switch. The logical switch name can include a maximum of 15 characters.

Default None

Command Mode OPENFLOW CONFIGURATION

Usage Information You must configure a controller for the logical switch instance. The logical switch instance is disabled by default. To establish a connection with the controller, enable the logical switch instance using the `no shutdown` command. All physical and logical interfaces in the switch will be assigned to the configured logical switch. The `no` form of this command removes the logical switch instance.

NOTE: OS10 supports only one instance of the logical switch. If you attempt to create a second logical switch instance, the following message appears:

```
% Warning: Only one Switch instance is supported
```

Example

```
OS10# config terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# no shutdown
```

Supported Releases 10.4.1 or later

OpenFlow-only mode commands

When you configure the switch to OpenFlow-only mode, only the following commands are available; all other commands are disabled.

NOTE:

- The `ntp` subcommand under the `interface` command is not applicable when the switch is in OpenFlow mode.
- The `ip` and `ipv6` subcommands under the `interface` command are applicable only when you configure the interface as the management port using the `in-band-mgmt` command.
- The `ip` and `ipv6` commands must be used only in In-Band mode (using the `in-band-mgmt` command).

Table 32. Modes and CLI commands

Mode	Available CLI commands
CONFIGURATION	aaa
	alias
	banner
	class-map
	clock
	control-plane
	crypto
	end
	eula-consent

Table 32. Modes and CLI commands (continued)

Mode	Available CLI commands
	<p>exec-timeout</p> <p>exit</p> <p>feature</p> <p>help</p> <p>host-description</p> <p>hostname</p> <p>interface</p> <p>ip</p> <ul style="list-style-type: none"> • ip access-list • ip route • ip ssh • ip telnet <p>ipv6</p> <ul style="list-style-type: none"> • ip access-list <p>line</p> <p>logging</p> <p>login</p> <p>management</p> <p>no</p> <p>ntp</p> <p>openflow</p> <p>password-attributes</p> <p>policy-map</p> <p>radius-server</p> <p>rest</p> <p>scale-profile</p> <p>support-assist</p> <p>system</p> <p>tacacs-server</p> <p>trust</p> <p>username</p> <p>userrole</p>
EXEC	<p>All commands</p> <p>The following debug commands are not available:</p> <ul style="list-style-type: none"> • debug iscsi • debug radius • debug tacacs+
LAG INTERFACE CONFIGURATION	LAG is not supported.
LOOPBACK INTERFACE CONFIGURATION	Loopback interface is not supported.

Table 32. Modes and CLI commands (continued)

Mode	Available CLI commands
INTERFACE CONFIGURATION	description
	end
	exit
	ip
	mtu
	negotiation
	ntp
	show
shutdown	
VLAN INTERFACE CONFIGURATION	VLAN is not supported.

Access Control Lists

OS10 uses two types of access policies — hardware-based ACLs and software-based route-maps. Use an ACL to filter traffic and drop or forward matching packets. To redistribute routes that match configured criteria, use a route-map.

ACLs

ACLs are a filter containing criterion to match; for example, examine IP, TCP, or UDP packets, and an action to take such as forwarding or dropping packets at the NPU. ACLs permit or deny traffic based on MAC and/or IP addresses. The number of ACL entries is hardware-dependent.

ACLs have only two actions — forward or drop. Route-maps not only permit or block redistributed routes but also modify information associated with the route when it is redistributed into another protocol. When a packet matches a filter, the device drops or forwards the packet based on the filter's specified action. If the packet does not match any of the filters in the ACL, the packet drops (implicit deny). ACL rules do not consume hardware resources until you apply the ACL to an interface.

ACLs process in sequence. If a packet does not match the criterion in the first filter, the second filter applies. If you configured multiple hardware-based ACLs, filter rules apply on the packet content based on the priority NPU rule.

Route maps

Route-maps are software-based filtering in a routing protocol redistributing routes from one protocol to another and used in decision criterion in route advertisements. A route-map defines which of the routes from the specified routing protocol redistributed into the target routing process, see [Route-maps](#).

Route-maps with more than one match criterion, two or more matches within the same route-map sequence have different match commands. Matching a packet against this criterion is an AND operation. If no match is found in a route-map sequence, the process moves to the next route-map sequence until a match is found, or until there are no more sequences. When a match is found, the packet is forwarded and no additional route-map sequences process. If you include a continue clause in the route-map sequence, the next route-map sequence also processes after a match is found.

The S5148F-ON platform has the following limitations:

- ACL counter does not support byte count.
- ACL rule does not look up the next header for IPv6 packets.
- L2 Egress ACL does not work for unknown unicast traffic.
- L2 User ACL has higher priority than the L3 User ACL.
- You cannot modify or extend the hardware table for each ACL type.
- In Ipv6 packets, only the protocol number of first header gets matched.
- The egress Deny ACL entry does not block soft-forwarded packets and CPU-originated ICMP packets.

IP ACLs


An ACL filters packets based on the:

- IP protocol number
- Source and destination IP address
- Source and destination TCP port number
- Source and destination UDP port number

For ACL, TCP, and UDP filters, match criteria on specific TCP or UDP ports. For ACL TCP filters, you can also match criteria on established TCP sessions.

When creating an ACL, the sequence of the filters is important. You can assign sequence numbers to the filters as you enter them or OS10 can assign numbers in the order you create the filters. The sequence numbers display in the `show running-configuration` and `show ip access-lists [in | out]` command output.

Ingress and egress hot-lock ACLs allow you to append or delete new rules into an existing ACL without disrupting traffic flow. Existing entries in the CAM shuffle to accommodate the new entries. Hot-lock ACLs are enabled by default and support ACLs on all platforms.

 **NOTE:** Hot-lock ACLs support ingress ACLs only.

MAC ACLs

MAC ACLs filter traffic on the Layer 2 (L2) header of a packet. This traffic filtering is based on:

Source MAC packet address	MAC address range—address mask in 3x4 dotted hexadecimal notation, and <i>any</i> to denote that the rule matches all source addresses.
Destination MAC packet address	MAC address range—address-mask in 3x4 dotted hexadecimal notation, and <i>any</i> to denote that the rule matches all destination addresses.
Packet protocol	Set by its EtherType field contents and Assigned protocol number for all protocols.
VLAN ID	Set in the packet header
Class of service	Present in the packet header

IPv4/IPv6 and MAC ACLs apply separately for inbound and outbound packets. You can assign an interface to multiple ACLs, with a limit of one ACL per packet direction per ACL type.

Control-plane ACLs

OS10 offers control-plane ACLs to selectively restrict packets that are destined to the CPU port, thereby providing increased security. Control-plane ACLs offer:

- An option to protect the CPU from denial of service (DoS) attacks.
- Fine-grained control to allow or block traffic going to the CPU.

Control-plane ACLs apply on the front-panel and management ports. Control-plane ACLs are one of the following types:

- IP ACL
- IPv6 ACL
- MAC ACL

There is no implicit deny rule. If none of the configured conditions match, the default behavior is to permit. If you need to deny traffic that does not match any of the configured conditions, explicitly configure a deny statement.


The control-plane ACL is mutually exclusive with VTY ACL, the management ACL. VTY ACL provides secure access for session connection protocols, such as SSH or TELNET; however, control-plane ACLs permit or deny any TCP or UDP, including SSH and TELNET sessions, from specific hosts and networks, and also filters both IPv4 and IPv6 traffic.

Configure control-plane ACL

To configure control-plane ACLs, use the existing ACL template and create the appropriate rules to permit or deny traffic as needed, similar to creating an access list for VTY ACLs. However, when you apply this control-plane ACL, you must apply it in CONTROL-PLANE mode instead of VTY mode. For example:

```
OS10# configure terminal
OS10(config)# control-plane
OS10(config-control-plane)# ip access-group acl_name in
```

where *acl_name* is the name of the control-plane ACL, a maximum of 140 characters.

 **NOTE:** Apply control-plane ACLs on ingress traffic only.

Control-plane ACL qualifiers

This section lists the control-plane ACL rule qualifiers.

- IPv4 qualifiers:
 - *DST_IP*—Destination IP address
 - *SRC_IP*—Source IP address
 - *IP_TYPE*—IP type
 - *IP_PROTOCOL*—Protocols such as TCP, UDP, and so on
 - *L4_DST_PORT*—Destination port number

 **NOTE:** The destination port number qualifier supports only the `eq` option. Port range is not supported.

- IPv6 qualifiers:
 - `DST_IPv6`—Destination address
 - `SRC_IPv6`—Source address
 - `IP_TYPE`—IP Type; for example, IPv4 or IPv6
 - `IP_PROTOCOL`—TCP, UDP, and so on
 - `L4_DST_PORT`—Destination port

 **NOTE:** The destination port number qualifier supports only the `eq` option. Port range is not supported.

- MAC qualifiers:
 - `OUT_PORT`—Egress CPU port
 - `SRC_MAC`—Source MAC address
 - `DST_MAC`—Destination MAC address
 - `ETHER_TYPE`—Ethertype
 - `OUTER_VLAN_ID`—VLAN ID
 - `IP_TYPE`—IP type
 - `OUTER_VLAN_PRI`—DOT1P value

IP fragment handling

OS10 supports a configurable option to explicitly deny IP fragmented packets, particularly for the second and subsequent packets. This option extends the existing ACL command syntax with the `fragments` keyword for all Layer 3 (L3) rules:

- Second and subsequent fragments are allowed because you cannot apply a L3 rule to these fragments. If the packet is to be denied eventually, the first fragment must be denied and the packet as a whole cannot be reassembled.
- The system applies implicit permit for the second and subsequent fragment prior to the implicit deny.
- If you configure an *explicit deny*, the second and subsequent fragments do not hit the implicit permit rule for fragments.

IP fragments ACL

When a packet exceeds the maximum packet size, the packet is fragmented into a number of smaller packets that contain portions of the contents of the original packet. This packet flow begins with an initial packet that contains all of the Layer 3 (L3) and Layer 4 (L4) header information contained in the original packet, and is followed by a number of packets that contain only the L3 header information.

This packet flow contains all of the information from the original packet distributed through packets that are small enough to avoid the maximum packet size limit. This provides a particular problem for ACL processing.

If the ACL filters based on L4 information, the non-initial packets within the fragmented packet flow will not match the L4 information, even if the original packet would have matched the filter. Because of this filtering, packets are not processed by the ACL.

The examples show denying second and subsequent fragments, and permitting all packets on an interface. These ACLs deny all second and subsequent fragments with destination IP 10.1.1.1, but permit the first fragment and non-fragmented packets with destination IP 10.1.1.1. The second example shows ACLs which permits all packets — both fragmented and non-fragmented — with destination IP 10.1.1.1.

Deny second and subsequent fragments

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# deny ip any 10.1.1.1/32 fragments
OS10(conf-ipv4-acl)# permit ip any 10.1.1.1/32
```

Permit all packets on interface

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# permit ip any 10.1.1.1/32
OS10(conf-ipv4-acl)# deny ip any 10.1.1.1/32 fragments
```

L3 ACL rules

Use ACL commands for L3 packet filtering. TCP packets from host 10.1.1.1 with the TCP destination port equal to 24 are permitted, and all others are denied.

TCP packets that are first fragments or non-fragmented from host 10.1.1.1 with the TCP destination port equal to 24 are permitted, and all TCP non-first fragments from host 10.1.1.1 are permitted. All other IP packets that are non-first fragments are denied.

Permit ACL with L3 information only

If a packet's L3 information matches the information in the ACL, the packet's fragment offset (FO) is checked:

- If a packet's FO > 0, the packet is permitted
- If a packet's FO = 0, the next ACL entry processes

Deny ACL with L3 information only

If a packet's L3 information does not match the L3 information in the ACL, the packet's FO is checked:

- If a packet's FO > 0, the packet is denied
- If a packet's FO = 0, the next ACL line processes

Permit all packets from host

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# permit tcp host 10.1.1.1 any eq 24
OS10(conf-ipv4-acl)# deny ip any any fragment
```

Permit only first fragments and non-fragmented packets from host

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# permit tcp host 10.1.1.1 any eq 24
OS10(conf-ipv4-acl)# permit tcp host 10.1.1.1 any fragment
OS10(conf-ipv4-acl)# deny ip any any fragment
```

To log all packets denied and to override the implicit deny rule and the implicit permit rule for TCP/UDP fragments, use a similar configuration. When an ACL filters packets, it looks at the FO to determine whether it is a fragment:

- FO = 0 means it is either the first fragment or the packet is a non-fragment
- FO > 0 means it is the fragments of the original packet

Assign sequence number to filter

IP ACLs filter on source and destination IP addresses, IP host addresses, TCP addresses, TCP host addresses, UDP addresses, and UDP host addresses. Traffic passes through the filter by filter sequence. Configure the IP ACL by first entering IP ACCESS-LIST mode and then assigning a sequence number to the filter.

User-provided sequence number

- Enter IP ACCESS LIST mode by creating an IP ACL in CONFIGURATION mode.

```
ip access-list access-list-name
```

- Configure a drop or forward filter in IPV4-ACL mode.

```
seq sequence-number {deny | permit | remark} {ip-protocol-number | icmp | ip |
protocol | tcp | udp} {source prefix | source mask | any | host} {destination mask
| any | host ip-address} [count [byte]] [fragments]
```

Auto-generated sequence number

If you are creating an ACL with only one or two filters, you can let the system assign a sequence number based on the order in which you configure the filters. The system assigns sequence numbers to filters using multiples of ten values.

- Configure a deny or permit filter to examine IP packets in IPV4-ACL mode.

```
{deny | permit} {source mask | any | host ip-address} [count [byte]] [fragments]
```

- Configure a deny or permit filter to examine TCP packets in IPV4-ACL mode.

```
{deny | permit} tcp {source mask | any | host ip-address}} [count [byte]] [fragments]
```

- Configure a deny or permit filter to examine UDP packets in IPV4-ACL mode.

```
{deny | permit} udp {source mask | any | host ip-address}} [count [byte]] [fragments]
```

Assign sequence number to filter

```
OS10(config)# ip access-list acl1
OS10(conf-ipv4-acl)# seq 5 deny tcp any any capture session 1 count
```

View ACLs and packets processed through ACL

```
OS10# show ip access-lists in
Ingress IP access-list acl1
Active on interfaces :
  ethernet1/1/5
  seq 5 permit ip any any count (10000 packets)
```

L2 and L3 ACLs

Configure both L2 and L3 ACLs on an interface in L2 mode. Rules apply if you use both L2 and L3 ACLs on an interface.

- L3 ACL filters packets and then the L2 ACL filters packets
- Egress L3 ACL filters packets

Rules apply in order:

- Ingress L3 ACL
- Ingress L2 ACL
- Egress L3 ACL
- Egress L2 ACL

i **NOTE:** In ingress ACLs, L2 has higher priority than L3 and in egress ACLs, L3 has higher priority than L2.

Table 33. L2 and L3 targeted traffic

L2 ACL / L3 ACL	Targeted traffic
Deny / Deny	L3 ACL denies
Deny / Permit	L3 ACL permits
Permit / Deny	L3 ACL denies
Permit / Permit	L3 ACL permits

Assign and apply ACL filters

To filter an Ethernet interface, a port-channel interface, or a VLAN, assign an IP ACL filter to a physical interface. The IP ACL applies to all traffic entering a physical or port-channel interface. The traffic either forwards or drops depending on the criteria and actions you configure in the ACL filter.

To change the ACL filter functionality, apply the same ACL filters to different interfaces. For example, take ACL "ABCD" and apply it using the `in` keyword and it becomes an ingress ACL. If you apply the same ACL filter using the `out` keyword, it becomes an egress ACL.

You can apply an IP ACL filter to a physical or port-channel interface. The number of ACL filters allowed is hardware-dependent.

1. Enter the interface information in CONFIGURATION mode.

```
interface ethernet node/slot/port
```

2. Configure an IP address for the interface, placing it in L3 mode in INTERFACE mode.

```
ip address ip-address
```

3. Apply an IP ACL filter to traffic entering or exiting an interface in INTERFACE mode.

```
ip access-group access-list-name {in | out}
```

Configure IP ACL

```
OS10(config)# interface ethernet 1/1/28
OS10(conf-if-eth1/1/28)# ip address 10.1.2.0/24
OS10(conf-if-eth1/1/28)# ip access-group abcd in
```

View ACL filters applied to interface

```
OS10# show ip access-lists in
Ingress IP access-list acl1
Active on interfaces :
  ethernet1/1/28
seq 10 permit ip host 10.1.1.1 host 100.1.1.1 count (0 packets)
seq 20 deny ip host 20.1.1.1 host 200.1.1.1 count (0 packets)
seq 30 permit ip 10.1.2.0/24 100.1.2.0/24 count (0 packets)
seq 40 deny ip 20.1.2.0/24 200.1.2.0/24 count (0 packets)
seq 50 permit ip 10.0.3.0 255.0.255.0 any count (0 packets)
seq 60 deny ip 20.0.3.0 255.0.255.0 any count (0 packets)
seq 70 permit tcp any eq 1000 100.1.4.0/24 eq 1001 count (0 packets)
seq 80 deny tcp any eq 2100 200.1.4.0/24 eq 2200 count (0 packets)
seq 90 permit udp 10.1.5.0/28 eq 10000 any eq 10100 count (0 packets)
seq 100 deny tcp host 20.1.5.1 any rst psh count (0 packets)
seq 110 permit tcp any any fin syn rst psh ack urg count (0 packets)
seq 120 deny icmp 20.1.6.0/24 any fragment count (0 packets)
seq 130 permit 150 any any dscp 63 count (0 packets)
```

To view the number of packets matching the ACL, use the `count` option when creating ACL entries.

- Create an ACL that uses rules with the `count` option, see [Assign sequence number to filter](#).
- Apply the ACL as an inbound or outbound ACL on an interface in CONFIGURATION mode, and view the number of packets matching the ACL.

```
show ip access-list {in | out}
```

Ingress ACL filters

To create an ingress ACL filter, use the `ip access-group` command in EXEC mode. To configure ingress, use the `in` keyword. Apply rules to the ACL with the `ip access-list acl-name` command. To view the access-list, use the `show access-lists` command.

1. Apply an access-list on the interface with ingress direction in INTERFACE mode.

```
ip access-group access-group-name in
```

2. Return to CONFIGURATION mode.

```
exit
```

3. Create the access-list in CONFIGURATION mode.

```
ip access-list access-list-name
```

4. Create the rules for the access-list in ACCESS-LIST mode.

```
permit ip host ip-address host ip-address count
```

Apply ACL rules to access-group and view access-list

```
OS10(config)# interface ethernet 1/1/28
OS10(conf-if-eth1/1/28)# ip access-group abcd in
OS10(conf-if-eth1/1/28)# exit
OS10(config)# ip access-list acl1
OS10(conf-ipv4-acl)# permit ip host 10.1.1.1 host 100.1.1.1 count
```

Egress ACL filters

Egress ACL filters affect the traffic *leaving* the network. Configuring egress ACL filters onto physical interfaces protects the system infrastructure from a malicious and intentional attack by explicitly allowing only authorized traffic. These system-wide ACL filters eliminate the need to apply ACL filters onto each interface and achieves the same results.

You can use an egress ACL filter to restrict egress traffic. For example, when a denial of service (DOS) attack traffic is isolated to a specific interface, apply an egress ACL filter to block the flow from exiting the network and thus protect downstream devices.

1. Apply an access-list on the interface with egress direction in INTERFACE mode.

```
ip access-group access-group-name out
```

2. Return to CONFIGURATION mode.

```
exit
```

3. Create the access-list in CONFIGURATION mode.

```
ip access-list access-list-name
```

4. Create the rules for the access-list in ACCESS-LIST mode.

```
seq 10 deny ip any any count fragment
```

Apply rules to ACL filter

```
OS10(config)# interface ethernet 1/1/29
OS10(conf-if-eth1/1/29)# ip access-group egress out
OS10(conf-if-eth1/1/29)# exit
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# seq 10 deny ip any any count fragment
```

View IP ACL filter configuration

```
OS10# show ip access-lists out
Egress IP access-list abcd
Active on interfaces :
  ethernet1/1/29
seq 10 deny ip any any fragment count (100 packets)
```


Clear access-list counters

Clear IPv4, IPv6, or MAC access-list counters for a specific access-list or all lists. The counter counts the number of packets that match each permit or deny statement in an access-list. To get a more recent count of packets matching an access-list, clear the counters to start at zero. If you do not configure an access-list name, all IP access-list counters clear.

To view access-list information, use the `show access-lists` command.

- Clear IPv4 access-list counters in EXEC mode.

```
clear ip access-list counters access-list-name
```

- Clear IPv6 access-list counters in EXEC mode.

```
clear ipv6 access-list counters access-list-name
```

- Clear MAC access-list counters in EXEC mode.

```
clear mac access-list counters access-list-name
```

IP prefix-lists

IP prefix-lists control the routing policy. An IP prefix-list is a series of sequential filters that contain a matching criterion and an permit or deny action to process routes. The filters process in sequence so that if a route prefix does not match the criterion in the first filter, the second filter applies, and so on.

A route prefix is an IP address pattern that matches on bits within the IP address. The format of a route prefix is `A.B.C.D/x`, where `A.B.C.D` is a dotted-decimal address and `/x` is the number of bits that match the dotted decimal address.

When the route prefix matches a filter, the system drops or forwards the packet based on the filter's designated action. If the route prefix does not match any of the filters in the prefix-list, the route drops (implicit deny).

For example, in `112.24.0.0/16`, the first 16 bits of the address `112.24.0.0` match all addresses between `112.24.0.0` to `112.24.255.255`. Use permit or deny filters for specific routes with the `le` (less or equal) and `ge` (greater or equal) parameters, where `x.x.x.x/x` represents a route prefix:

- To deny only `/8` prefixes, enter `deny x.x.x.x/x ge 8 le 8`
- To permit routes with the mask greater than `/8` but less than `/12`, enter `permit x.x.x.x/x ge 8 le 12`
- To deny routes with a mask less than `/24`, enter `deny x.x.x.x/x le 24`
- To permit routes with a mask greater than `/20`, enter `permit x.x.x.x/x ge 20`

The following rules apply to prefix-lists:

- A prefix-list without permit or deny filters allows all routes
- An "implicit deny" is assumed — the route drops for all route prefixes that do not match a permit or deny filter
- After a route matches a filter, the filter's action applies and no additional filters apply to the route

Use prefix-lists in processing routes for routing protocols such as OSPF, RTM, and BGP.

To configure a prefix-list, use commands in PREFIX-LIST and ROUTER-BGP modes. Create the prefix-list in PREFIX-LIST mode and assign that list to commands in ROUTER-BGP modes.

Route-maps

Route-maps a series of commands that contain a matching criterion and action. They change the packets meeting the matching criterion. ACLs and prefix-lists can only drop or forward the packet or traffic while route-maps process routes for route redistribution. For example, use a route-map to filter only specific routes and to add a metric.

- Route-maps also have an *implicit deny*. Unlike ACLs and prefix-lists where the packet or traffic is dropped, if a route does not match the route-map conditions, the route is not redistributed.
- Route-maps process routes for route redistribution. For example, to add a metric, a route-map can *filter* only specific routes. If the route does not match the conditions, the route-map decides where the packet or traffic drops. The route is not redistributed if it does not match.

- Route-maps use commands to decide what to do with traffic. To remove the match criteria in a route-map, use the `no match` command.
- In a BGP route-map, if you repeat the same match statements; for example, a match metric, with different values in the same sequence number, only the last match and set values are taken into account.

Configure match metric

```
OS10(config)# route-map hello
OS10(config-route-map)# match metric 20
```

View route-map

```
OS10(config-route-map)# do show route-map
route-map hello, permit, sequence 10
  Match clauses:
    metric 20
```

Change match

```
OS10(config-route-map)# match metric 30
```

View updated route-map

```
OS10(config-route-map)# do show route-map
route-map hello, permit, sequence 10
  Match clauses:
    metric 30
```

To filter the routes for redistribution, combine route-maps and IP prefix lists. If the route or packet matches the configured criteria, the OS10 processes the route based on the `permit` or `deny` configuration of the prefix list.

When a route-map and a prefix list combine:

- For a route map with the `permit` action:
 - If a route matches a prefix-list set to `deny`, the route is denied
 - If a route matches a prefix-list set to `permit`, the route is permitted and any set of actions are apply
- For a route map with the `deny` action:
 - If a route matches a prefix-list set to `deny`, the route is denied
 - If a route matches a prefix-list set to `permit`, the route is denied

View both IP prefix-list and route-map configuration

```
OS10(config-router-bgp-neighbor-af)# do show ip prefix-list
ip prefix-list p1:
seq 1 deny 10.1.1.0/24
seq 10 permit 0.0.0.0/0 le 32
ip prefix-list p2:
seq 1 permit 10.1.1.0/24
seq 10 permit 0.0.0.0/0 le 32
```

View route-map configuration

```
OS10(config-router-bgp-neighbor-af)# do show route-map
route-map test1, deny, sequence 10
Match clauses:
ip address prefix-list p1
Set clauses:
route-map test2, permit, sequence 10
Match clauses:
ip address prefix-list p1
Set clauses:
route-map test3, deny, sequence 10
Match clauses:
ip address prefix-list p2
Set clauses:
route-map test4, permit, sequence 10
Match clauses:
```

```
ip address prefix-list p2
Set clauses:
```

Match routes

Configure match criterion for a route-map. There is no limit to the number of `match` commands per route map, but keep the number of match filters in a route-map low. The `set` commands do not require a corresponding `match` command.

- Match routes with a specific metric value in ROUTE-MAP mode, 0 to 4294967295.

```
match metric metric-value
```

- Match routes with a specific tag in ROUTE-MAP mode, 0 to 4294967295.

```
match tag tag-value
```

- Match routes whose next hop is a specific interface in ROUTE-MAP mode.

```
match interface interface
```

- `ethernet` — Enter the Ethernet interface information.
- `port-channel` — Enter the port-channel number.
- `vlan` — Enter the VLAN ID number.

Check match routes

```
OS10(config)# route-map test permit 1
OS10(conf-route-map)# match tag 250000
OS10(conf-route-map)# set weight 100
```

Set conditions

There is no limit to the number of `set` commands per route map, but keep the number of set filters in a route-map low. The `set` commands do not require a corresponding `match` command.

- Enter the IP address in A.B.C.D format of the next-hop for a BGP route update in ROUTE-MAP mode.

```
set ip next-hop address
```

- Enter an IPv6 address in A::B format of the next-hop for a BGP route update in ROUTE-MAP mode.

```
set ipv6 next-hop address
```

- Enter the range value for the BGP route's LOCAL_PREF attribute in ROUTE-MAP mode, from 0 to 4294967295.

```
set local-preference range-value
```

- Enter a metric value for redistributed routes in ROUTE-MAP mode, from 0 to 4294967295.

```
set metric {+ | - | metric-value}
```

- Enter an OSPF type for redistributed routes in ROUTE-MAP mode.

```
set metric-type {type-1 | type-2 | external | internal}
```

- Enter an ORIGIN attribute in ROUTE-MAP mode.

```
set origin {egp | igp | incomplete}
```

- Enter a tag value for the redistributed routes in ROUTE-MAP mode, from 0 to 4294967295.

```
set tag tag-value
```

- Enter a value as the route's weight in ROUTE-MAP mode, from 0 to 65535.

```
set weight value
```

Check set conditions

```
OS10(config)# route-map ip permit 1
OS10(conf-route-map)# match metric 2567
```

continue Clause

Only BGP route-maps support the `continue` clause. When a match is found, `set` clauses run and the packet is forwarded — no route-map processing occurs. If you configure the `continue` clause without configuring a module, the next sequential module processes.

If you configure the `continue` command at the end of a module, the next module processes even after a match is found. The example shows a `continue` clause at the end of a route-map module — if a match is found in the route-map `test` module 10, module 30 processes.

Route-map continue clause

```
OS10(config)# route-map test permit 10
OS10(conf-route-map)# continue 30
```

ACL flow-based monitoring

Flow-based monitoring conserves bandwidth by selecting only the required flow to be mirrored instead of mirroring entire packets from an interface. This feature is available for L2 and L3 ingress traffic. Specify flow-based monitoring using ACL rules. Flow-based monitoring copies incoming packets that match the ACL rules applied on the ingress port and forwards (mirrors) them to another port. The source port is the monitored port (MD), and the destination port is the monitoring port (MG).

When a packet arrives at a monitored port, the packet validates against the configured ACL rules. If the packet matches an ACL rule, the system examines the corresponding flow processor and performs the action specified for that port. If the mirroring action is set in the flow processor entry, the port details are sent to the destination port.

Flow-based mirroring

Flow-based mirroring is a mirroring session in which traffic matches specified policies that are mirrored to a destination port. Port-based mirroring maintains a database that contains all monitoring sessions, including port monitor sessions. The database has information regarding the sessions that are enabled or not enabled for flow-based monitoring. Flow-based mirroring is also known as *policy-based mirroring*.

To activate flow-based mirroring, use the `flow-based enable` command. Traffic with particular flows that are traversing through the ingress interfaces are examined. Appropriate ACL rules apply in the ingress direction. By default, flow-based mirroring is not enabled.

To enable the evaluation and replication of traffic traversing to the destination port, configure the `monitor` option with the `permit`, `deny`, or `seq` commands for ACLs assigned to the source or the monitored port (MD). Enter the keywords `capture session session-id` with the `seq`, `permit`, or `deny` command for the ACL rules to allow or drop IPv4, IPv6, ARP, UDP, EtherType, ICMP, and TCP packets.

IPV4-ACL mode

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count [byte]]
[fragments] [threshold-in-msgs count] [capture session session-id]
```

If you configure the `flow-based enable` command and do not apply an ACL on the source port or the monitored port, both flow-based monitoring and port mirroring do not function. Flow-based monitoring is supported only for ingress traffic.

The `show monitor session session-id` command displays output which indicates if a particular session is enabled for flow-monitoring.

View flow-based monitoring

```
OS10# show monitor session 1
S.Id  Source          Destination      Dir  SrcIP  DstIP  DSCP  TTL  State Reason
-----
1     ethernet1/1/1     ethernet1/1/4   both N/A    N/A    N/A   N/A   true  Is UP
```

Traffic matching ACL rule

```
OS10# show ip access-lists in
Ingress IP access-list testflow
Active on interfaces :
  ethernet1/1/1
seq 5 permit icmp any any capture session 1
seq 10 permit ip 102.1.1.0/24 any capture session 1
seq 15 deny udp any any capture session 2
seq 20 deny tcp any any capture session 3
```

Enable flow-based monitoring

Flow-based monitoring conserves bandwidth by mirroring only specified traffic, rather than all traffic on an interface. It is available for L2 and L3 ingress and egress traffic. Configure traffic to be monitored using ACL filters.

1. Create a monitor session in MONITOR-SESSION mode.

```
monitor session session-number type local
```

2. Enable flow-based monitoring for the mirroring session in MONITOR-SESSION mode.

```
flow-based enable
```

3. Define ACL rules that include the keywords `capture session session-id` in CONFIGURATION mode. The system only considers port monitoring traffic that matches rules with the keywords `capture session`.

```
ip access-list
```

4. Apply the ACL to the monitored port in INTERFACE mode.

```
ip access-group access-list
```

Enable flow-based monitoring

```
OS10(config)# monitor session 1 type local
OS10(conf-mon-local-1)# flow-based enable
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# seq 5 permit icmp any any capture session 1
OS10(conf-ipv4-acl)# seq 10 permit ip 102.1.1.0/24 any capture session 1
OS10(conf-ipv4-acl)# seq 15 deny udp any any capture session 2
OS10(conf-ipv4-acl)# seq 20 deny tcp any any capture session 3
OS10(conf-ipv4-acl)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip access-group testflow in
OS10(conf-if-eth1/1/1)# no shutdown
```

View access-list configuration

```
OS10# show ip access-lists in
Ingress IP access-list testflow
Active on interfaces :
  ethernet1/1/1
seq 5 permit icmp any any capture session 1
seq 10 permit ip 102.1.1.0/24 any capture session 1
seq 15 deny udp any any capture session 2
seq 20 deny tcp any any capture session 3
```

View monitor sessions

```
OS10(conf-if-eth1/1/1)# show monitor session all
S.Id  Source          Destination      Dir  SrcIP  DstIP  DSCP  TTL  State  Reason
-----
1     ethernet1/1/1  ethernet1/1/4   both N/A    N/A    N/A   N/A   true   Is UP
```

ACL commands

clear ip access-list counters

Clears ACL counters for a specific access-list.

Syntax	<code>clear ip access-list counters [access-list-name]</code>
Parameters	<i>access-list-name</i> — (Optional) Enter the name of the IP access-list to clear counters. A maximum of 140 characters.
Default	Not configured
Command Mode	EXEC
Usage Information	If you do not enter an access-list name, all IPv6 access-list counters clear. The counter counts the number of packets that match each permit or deny statement in an access-list. To get a more recent count of packets matching an access list, clear the counters to start at zero. To view access-list information, use the <code>show access-lists</code> command.
Example	<pre>OS10# clear ip access-list counters</pre>
Supported Releases	10.2.0E or later

clear ipv6 access-list counters

Clears IPv6 access-list counters for a specific access-list.

Syntax	<code>clear ipv6 access-list counters [access-list-name]</code>
Parameters	<i>access-list-name</i> — (Optional) Enter the name of the IPv6 access-list to clear counters. A maximum of 140 characters.
Default	Not configured
Command Mode	EXEC
Usage Information	If you do not enter an access-list name, all IP access-list counters clear. The counter counts the number of packets that match each permit or deny statement in an access list. To get a more recent count of packets matching an access list, clear the counters to start at zero. To view access-list information, use the <code>show access-lists</code> command.
Example	<pre>OS10# clear ipv6 access-list counters</pre>
Supported Releases	10.2.0E or later

clear mac access-list counters

Clears counters for a specific or all MAC access lists.

Syntax	<code>clear mac access-list counters [access-list-name]</code>
---------------	--

Parameters	<i>access-list-name</i> — (Optional) Enter the name of the MAC access list to clear counters. A maximum of 140 characters.
Default	Not configured
Command Mode	EXEC
Usage Information	If you do not enter an access-list name, all MAC access-list counters clear. The counter counts the number of packets that match each permit or deny statement in an access list. To get a more recent count of packets matching an access list, clear the counters to start at zero. To view access-list information, use the <code>show access-lists</code> command.
Example	<pre>OS10# clear mac access-list counters</pre>
Supported Releases	10.2.0E or later

deny

Configures a filter to drop packets with a specific IP address.

Syntax	<code>deny [protocol-number icmp ip tcp udp] [A.B.C.D A.B.C.D/x any host ip-address] [A.B.C.D A.B.C.D/x any host ip-address] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none"> • <i>protocol-number</i> — (Optional) Enter the protocol number identified in the IP header, from 0 to 255. • <i>icmp</i> — (Optional) Enter the ICMP address to deny. • <i>ip</i> — (Optional) Enter the IP address to deny. • <i>tcp</i> — (Optional) Enter the TCP address to deny. • <i>udp</i> — (Optional) Enter the UDP address to deny. • <i>A.B.C.D</i> — Enter the IP address in dotted decimal format. • <i>A.B.C.D/x</i> — Enter the number of bits to match to the dotted decimal address. • <i>any</i> — (Optional) Enter the filter type to subject routes to. <ul style="list-style-type: none"> ◦ <i>capture</i> — (Optional) Capture packets the filter processes. ◦ <i>dscp value</i> — (Optional) Deny a packet based on the DSCP values, from 0 to 63. ◦ <i>fragment</i> — (Optional) Use ACLs to control packet fragments. • <i>host ip-address</i> — (Optional) Enter the keyword and the IP address to use a host address only.
Default	Not configured
Command Mode	IPV4-ACL
Usage Information	The <code>no</code> version of this command removes the filter.
Example	<pre>OS10(config)# ip access-list testflow OS10(conf-ipv4-acl)# deny udp any any</pre>
Supported Releases	10.2.0E or later

deny (IPv6)

Configures a filter to drop packets with a specific IPv6 address.

Syntax	<code>deny [protocol-number icmp ipv6 tcp udp] [A::B A::B/x any host ipv6-address] [A::B A::B/x any host ipv6-address] [capture dscp value fragment]</code>
---------------	---

Parameters	<ul style="list-style-type: none"> • <i>protocol-number</i> — (Optional) Enter the protocol number identified in the IP header, from 0 to 255. • <i>icmp</i> — (Optional) Enter the ICMP address to deny. • <i>ipv6</i> — (Optional) Enter the IPv6 address to deny. • <i>tcp</i> — (Optional) Enter the TCP address to deny. • <i>udp</i> — (Optional) Enter the UDP address to deny. • <i>A::B</i> — Enter the IPv6 address in dotted decimal format. • <i>A::B/x</i> — Enter the number of bits to match to the IPv6 address. • <i>any</i> — (Optional) Enter so that all routes are subject to the filter: <ul style="list-style-type: none"> ◦ <i>capture</i> — (Optional) Capture packets the filter processes. ◦ <i>dscp value</i> — (Optional) Deny a packet based on the DSCP values, from 0 to 63. ◦ <i>fragment</i> — (Optional) Use ACLs to control packet fragments. • <i>host ipv6-address</i> — (Optional) Enter the keyword and the IPv6 address to use a host address only.
Default	Not configured
Command Mode	IPv6-ACL
Usage Information	The <code>no</code> version of this command removes the filter.
Example	<pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# deny ipv6 any any capture session 1</pre>
Supported Releases	10.2.0E or later

deny (MAC)

Configures a filter to drop packets with a specific MAC address.

Syntax	<code>deny {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] any} [<i>protocol-number</i> <i>capture</i> <i>cos</i> <i>vlan</i>]</code>
Parameters	<ul style="list-style-type: none"> • <i>nn:nn:nn:nn:nn:nn</i> — Enter the MAC address of the network from or to which the packets are sent. • <i>00:00:00:00:00:00</i> — (Optional) Enter which bits in the MAC address must match. If you do not enter a mask, a mask of <code>00:00:00:00:00:00</code> applies. • <i>any</i> — (Optional) Set routes which are subject to the filter. <ul style="list-style-type: none"> ◦ <i>protocol-number</i> — (Optional) MAC protocol number identified in the header, from 600 to ffff. ◦ <i>capture</i> — (Optional) Capture packets the filter processes. ◦ <i>cos</i> — (Optional) CoS value, from 0 to 7. ◦ <i>vlan</i> — (Optional) VLAN number, from 1 to 4093.
Default	Disabled
Command Mode	MAC-ACL
Usage Information	The <code>no</code> version of this command removes the filter.
Example	<pre>OS10(config)# mac access-list macacl OS10(conf-mac-acl)# deny any any cos 7 OS10(conf-mac-acl)# deny any any vlan 2</pre>
Supported Releases	10.2.0E or later

deny icmp

Configures a filter to drop all or specific Internet Control Message Protocol (ICMP) messages.

Syntax `deny icmp [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | dscp value | fragment]`

- Parameters**
- `A.B.C.D` — Enter the IP address in hexadecimal format separated by colons.
 - `A.B.C.D/x` — Enter the number of bits to match to the IP address.
 - `any` — (Optional) Set all routes subject to the filter.
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `host ip-address` — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# deny icmp any any capture session 1
```

Supported Releases 10.2.0E or later

deny icmp (IPv6)

Configures a filter to drop all or specific ICMP messages.

Syntax `deny icmp [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | dscp value | fragment]`

- Parameters**
- `A::B` — Enter the IPv6 address in hexadecimal format separated by colons.
 - `A::B/x` — Enter the number of bits to match to the IPv6 address.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `host ipv6-address` — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny icmp any any capture session 1
```

Supported Releases 10.2.0E or later

deny ip

Configures a filter to drop all or specific packets from an IPv4 address.

Syntax `deny ip [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | dscp value | fragment]`

- Parameters**
- `A.B.C.D` — Enter the IP address in dotted decimal format.
 - `A.B.C.D/x` — Enter the number of bits to match to the dotted decimal address.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `host ip-address` — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# deny ip any capture session 1 count
```

Supported Releases 10.2.0E or later

deny ipv6

Configures a filter to drop all or specific packets from an IPv6 address.

Syntax `deny ipv6 [A::B | A::B/x | any | host ipv6-address] [A::B | A:B/x | any | host ipv6-address] [capture | dscp | fragment]`

- Parameters**
- `A::B` — (Optional) Enter the source IPv6 address from which the packet was sent and the destination address.
 - `A::B/x` — (Optional) Enter the source network mask in /prefix format (/x) and the destination mask.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `host ipv6-address` — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny ipv6 any any capture session 1
```

Supported Releases 10.2.0E or later

deny tcp

Configures a filter that drops Transmission Control Protocol (TCP) packets meeting the filter criteria.

Syntax	<code>deny tcp [A.B.C.D A.B.C.D/x any host <i>ip-address</i> [<i>operator</i>]] [[A.B.C.D A.B.C.D/x any host <i>ip-address</i> [<i>operator</i>]] [ack fin psh rst syn urg] [capture dscp <i>value</i> fragment]</code>
Parameters	<ul style="list-style-type: none">• A.B.C.D — Enter the IP address in A.B.C.D format.• A.B.C.D/x — Enter the number of bits to match in A.B.C.D/x format.• any — (Optional) Enter to subject all routes to the filter:<ul style="list-style-type: none">◦ capture — (Optional) Capture packets the filter processes.◦ dscp <i>value</i> — (Optional) Deny a packet based on the DSCP values, from 0 to 63.◦ fragment — (Optional) Use ACLs to control packet fragments.◦ ack — (Optional) Set the bit as acknowledgement.◦ fin — (Optional) Set the bit as finish—no more data from sender.◦ psh — (Optional) Set the bit as push.◦ rst — (Optional) Set the bit as reset.◦ syn — (Optional) Set the bit as synchronize.◦ urg — (Optional) Set the bit set as urgent.• <i>operator</i> — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:<ul style="list-style-type: none">◦ eq — Equal to◦ gt — Greater than◦ lt — Lesser than◦ neq — Not equal to◦ range — Range of ports, including the specified port numbers.• host <i>ip-address</i> — (Optional) Enter the keyword and the IP address to use a host address only.
Default	Not configured
Command Mode	IPV4-ACL
Usage Information	The no version of this command removes the filter.
Example	<pre>OS10(config)# ip access-list testflow OS10(conf-ipv4-acl)# deny tcp any any capture session 1</pre>
Supported Releases	10.2.0E or later

deny tcp (IPv6)

Configures a filter that drops TCP IPv6 packets meeting the filter criteria.

Syntax	<code>deny tcp [A::B A::B/x any host <i>ipv6-address</i> [<i>operator</i>]] [A::B A:B/x any host <i>ipv6-address</i> [<i>operator</i>]] [ack fin psh rst syn urg] [capture dscp <i>value</i> fragment]</code>
Parameters	<ul style="list-style-type: none">• A::B — Enter the IPv6 address in hexadecimal format separated by colons.• A::B/x — Enter the number of bits to match to the IPv6 address.• any — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ capture — (Optional) Capture packets the filter processes.◦ dscp <i>value</i> — (Optional) Deny a packet based on the DSCP values, from 0 to 63.◦ fragment — (Optional) Use ACLs to control packet fragments.• <i>operator</i> — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:

- eq — Equal to
- gt — Greater than
- lt — Lesser than
- neq — Not equal to
- range — Range of ports, including the specified port numbers.
- host *ipv6-address* — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The no version of this command removes the filter.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny tcp any any capture session 1
```

Supported Releases 10.2.0E or later

deny udp

Configures a filter to drop User Datagram Protocol (UDP) packets meeting the filter criteria.

Syntax deny udp [A.B.C.D | A.B.C.D/x | any | host *ip-address* [*operator*]] [A.B.C.D | A.B.C.D/x | any | host *ip-address* [*operator*]] [ack | fin | psh | rst | syn | urg] [capture | dscp *value* | fragment]

Parameters

- A.B.C.D — Enter the IP address in dotted decimal format.
- A.B.C.D/x — Enter the number of bits to match to the dotted decimal address.
- any — (Optional) Set all routes which are subject to the filter:
 - capture — (Optional) Capture packets the filter processes.
 - dscp *value* — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - fragment — (Optional) Use ACLs to control packet fragments.
 - ack — (Optional) Set the bit as acknowledgement.
 - fin — (Optional) Set the bit as finish—no more data from sender.
 - psh — (Optional) Set the bit as push.
 - rst — (Optional) Set the bit as reset.
 - syn — (Optional) Set the bit as synchronize.
 - urg — (Optional) Set the bit set as urgent.
- *operator* — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - eq — Equal to
 - gt — Greater than
 - lt — Lesser than
 - neq — Not equal to
 - range — Range of ports, including the specified port numbers.
- host *ip-address* — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The no version of this command removes the filter.

Example

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# deny udp any any capture session 1
```

Supported Releases 10.2.0E or later

deny udp (IPv6)

Configures a filter to drop UDP IPv6 packets that match filter criteria.

Syntax `deny udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A:B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | dscp value | fragment]`

- Parameters**
- `A::B` — Enter the IPv6 address in hexadecimal format separated by colons.
 - `A::B/x` — Enter the number of bits to match to the IPv6 address.
 - `any` — (Optional) Enter for all routes to be subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `ack` — (Optional) Set the bit as acknowledgement.
 - `fin` — (Optional) Set the bit as finish—no more data from sender).
 - `psh` — (Optional) Set the bit as push.
 - `rst` — (Optional) Set the bit as reset.
 - `syn` — (Optional) Set the bit as synchronize.
 - `urg` — (Optional) Set the bit set as urgent.
 - `operator` — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - `eq` — Equal to
 - `gt` — Greater than
 - `lt` — Lesser than
 - `neq` — Not equal to
 - `range` — Range of ports, including the specified port numbers.
 - `host ipv6-address` — (Optional) Enter the keyword and the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The no version of this command removes the filter.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny udp any any capture session 1
```

Supported Releases 10.2.0E or later

description

Configures an ACL description.

Syntax `description text`

Parameters `text` — Enter the description text string. A maximum of 80 characters.

Default Disabled

Command Modes IPV4-ACL, IPV6-ACL, MAC-ACL

Usage Information The no version of this command deletes the ACL description.

Example

```
OS10(conf-ipv4-acl)# description ipacltest
```

Supported Releases

10.2.0E or later

ip access-group

Configures an IP access group.

Syntax

```
ip access-group access-list-name {in | out}
```

Parameters

- *access-list-name* — Enter the name of an IPv4 access list. A maximum of 140 characters.
- *in* — Apply the ACL to incoming traffic.
- *out* — Apply the ACL to outgoing traffic.

Default

Not configured

Command Mode

INTERFACE
CONTROL-PLANE

Usage Information

Use this command in the CONTROL-PLANE mode to apply a control-plane ACL. Control-plane ACLs are only applied on the ingress traffic. By default, the control-plane ACL is applied to the front-panel ports as well as the management port. The `no` version of this command deletes the IP ACL configuration.

Example

```
OS10(conf-if-eth1/1/8)# ip access-group testgroup in
```

Example (Control-plane ACL)

```
OS10# configure terminal
OS10(config)# control-plane
OS10(config-control-plane)# ip access-group aaa-cp-acl in
```

Supported Releases

10.2.0E or later; 10.4.1 or later (control-plane ACL)

ip access-list

Creates an IP access list to filter based on an IP address.

Syntax

```
ip access-list access-list-name
```

Parameters

access-list-name — Enter the name of an IPv4 access list. A maximum of 140 characters.

Default

Not configured

Command Mode

CONFIGURATION

Usage

None

Information**Example**

```
OS10(config)# ip access-list acl1
```

Supported Releases

10.2.0E or later

ip as-path access-list

Create an AS-path ACL filter for BGP routes using a regular expression.

Syntax

```
ip as-path access-list name {deny | permit} regex-string
```

Parameters	<ul style="list-style-type: none"> • <i>name</i> — Enter an access list name. • <i>deny</i> <i>permit</i> — Reject or accept a matching route. • <i>regex-string</i> — Enter a regular expression string to match an AS-path route attribute.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	<p>You can specify an access-list filter on inbound and outbound BGP routes. The ACL filter consists of regular expressions. If a regular expression matches an AS path attribute in a BGP route, the route is rejected or accepted. The AS path does not contain the local AS number. The <i>no</i> version of this command removes a single access list entry if you specify <i>deny</i> and a <i>regex</i>. Otherwise, the entire access list is removed.</p> <p>The question mark (?) character is not supported in the regular expressions. All other special characters are supported. When you are using backslash (\) or double quotes (") in the regular expression, precede these characters with backslash (\). For example, enter \\ or \".</p>
Example	<pre>OS10(config)# ip as-path access-list abc deny 123</pre>
Supported Release	10.3.0E or later

ip community-list standard deny

Creates a standard community list for BGP to deny access.

Syntax	<code>ip community-list standard <i>name</i> deny {<i>aa:nn</i> no-advertise local-AS no-export internet}</code>
Parameters	<ul style="list-style-type: none"> • name — Enter the name of the standard community list used to identify one more deny groups of communities. • <i>aa:nn</i> — Enter the community number in the format <i>aa:nn</i>, where <i>aa</i> is the number that identifies the autonomous system and <i>nn</i> is a number the identifies the community within the autonomous system. • <i>no-advertise</i> — Enter the keyword for BGP to not advertise this route to any internal or external peer. • <i>local-AS</i> — Enter the keyword for BGP to not advertise this route to external peers. • <i>no-export</i> — Enter the keyword for BGP to not advertise this route outside a BGP confederation boundary. • <i>internet</i> — Enter the keyword for an Internet community.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <i>no</i> version of this command removes the community list.
Example	<pre>OS10(config)# ip community-list standard STD_LIST deny local-AS</pre>
Supported Release	10.3.0E or later

ip community-list standard permit

Creates a standard community list for BGP to permit access.

Syntax	<code>ip community-list standard <i>name</i> permit {<i>aa:nn</i> no-advertise local-as no-export internet}</code>
---------------	--

Parameters	<ul style="list-style-type: none"> • name — Enter the name of the standard community list used to identify one more deny groups of communities. • <i>aa:nn</i> — Enter the community number in the format <i>aa:nn</i>, where <i>aa</i> is the number that identifies the autonomous system and <i>nn</i> is a number the identifies the community within the autonomous system. • no-advertise — Enter the keyword for BGP to not advertise this route to any internal or external peer. • local-as — Enter the keyword for BGP to not advertise this route to external peers. • no-export — Enter the keyword for BGP to not advertise this route outside a BGP confederation boundary • internet — Enter the keyword for an Internet community.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The no version of this command removes the community list.
Example	<pre>OS10(config)# ip community-list standard STD_LIST permit local-AS</pre>
Supported Release	10.3.0E or later

ip extcommunity-list standard deny

Creates an extended community list for BGP to deny access.

Syntax	<code>ip extcommunity-list standard name deny {4byteas-generic rt soo}</code>
Parameters	<ul style="list-style-type: none"> • <i>name</i> — Enter the name of the community list used to identify one or more deny groups of extended communities. • 4byteas-generic—Enter the generic extended community then the keyword transitive or non-transitive. • <i>rt</i> — Enter the route target. • <i>soo</i> — Enter the route origin or site-of-origin.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The no version of this command removes the extended community list.
Example	<pre>OS10(config)# ip extcommunity-list standard STD_LIST deny 4byteas-generic transitive 1.65534:40</pre>
Supported Release	10.3.0E or later

ip extcommunity-list standard permit

Creates an extended community list for BGP to permit access.

Syntax	<code>ip extcommunity-list standard name permit {4byteas-generic rt soo}</code>
Parameters	<ul style="list-style-type: none"> • <i>name</i> — Enter the name of the community list used to identify one or more permit groups of extended communities. • <i>rt</i> — Enter the route target. • <i>soo</i> — Enter the route origin or site-of-origin.
Defaults	Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the extended community list.

Example

```
OS10(config)# ip extcommunity-list standard STD_LIST permit 4byteas-  
generic transitive 1.65412:60
```

Supported Release 10.3.0E or later

ip prefix-list description

Configures a description of an IP prefix list.

Syntax `ip prefix-list name description`

- Parameters**
- `name` — Enter the name of the prefix list.
 - `description` — Enter the description for the named prefix list.

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the specified prefix list.

Example

```
OS10(config)# ip prefix-list TEST description TEST_LIST
```

Supported Release 10.3.0E or later

ip prefix-list deny

Creates a prefix list to deny route filtering from a specified network address.

Syntax `ip prefix-list name deny [A.B.C.D/x [ge | le]] prefix-len`

- Parameters**
- `name` — Enter the name of the prefix list.
 - `A.B.C.D/x` — (Optional) Enter the source network address and mask in /prefix format (/x).
 - `ge` — Enter to indicate the network address is greater than or equal to the range specified.
 - `le` — Enter to indicate the network address is less than or equal to the range specified.
 - `prefix-len` — Enter the prefix length.

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the specified prefix-list.

Example

```
OS10(config)# ip prefix-list denyprefix deny 10.10.10.2/16 le 30
```

Supported Release 10.3.0E or later

ip prefix-list permit

Creates a prefix-list to permit route filtering from a specified network address.

Syntax `ip prefix-list name permit [A.B.C.D/x [ge | le]] prefix-len`

Parameters	<ul style="list-style-type: none"> • <i>name</i> — Enter the name of the prefix list. • A.B.C.D/x — (Optional) Enter the source network address and mask in /prefix format (/x). • <i>ge</i> — Enter to indicate the network address is greater than or equal to the range specified. • <i>le</i> — Enter to indicate the network address is less than or equal to the range specified. • <i>prefix-len</i> — Enter the prefix length.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the specified prefix-list.
Example	<pre>OS10(config)# ip prefix-list allowprefix permit 10.10.10.1/16 ge 10</pre>
Supported Release	10.3.0E or later

ip prefix-list seq deny

Configures a filter to deny route filtering from a specified prefix list.

Syntax	<code>ip prefix-list name seq num deny {A.B.C.D/x [ge le] prefix-len}</code>
Parameters	<ul style="list-style-type: none"> • <i>name</i> — Enter the name of the prefix list. • <i>num</i> — Enter the sequence list number. • A.B.C.D/x — Enter the source network address and mask in /prefix format (/x). • <i>ge</i> — Enter to indicate the network address is greater than or equal to the range specified. • <i>le</i> — Enter to indicate the network address is less than or equal to the range specified. • <i>prefix-len</i> — Enter the prefix length.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the specified prefix list.
Example	<pre>OS10(config)# ip prefix-list seqprefix seq 65535 deny 10.10.10.1/16 ge 10</pre>
Supported Release	10.3.0E or later

ip prefix-list seq permit

Configures a filter to permit route filtering from a specified prefix list.

Syntax	<code>ipv6 prefix-list [name] seq num permit A::B/x [ge le] prefix-len</code>
Parameters	<ul style="list-style-type: none"> • <i>name</i> — Enter the name of the prefix list. • <i>num</i> — Enter the sequence list number. • A.B.C.D/x — Enter the source network address and mask in /prefix format (/x). • <i>ge</i> — Enter to indicate the network address is greater than or equal to the range specified. • <i>le</i> — Enter to indicate the network address is less than or equal to the range specified. • <i>prefix-len</i> — Enter the prefix length.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the specified prefix list.

Example

```
OS10(config)# ip prefix-list seqprefix seq 65535 permit 10.10.10.1/16 le
30
```

Supported Release 10.3.0E or later

ipv6 access-group

Configures an IPv6 access group.

Syntax `ipv6 access-group access-list-name {in | out}`

Parameters

- `access-list-name` — Enter the name of an IPv6 ACL. A maximum of 140 characters.
- `in` — Apply the ACL to incoming traffic.
- `out` — Apply the ACL to outgoing traffic.

Default Not configured

Command Mode INTERFACE
CONTROL-PLANE

Usage Information Use this command in the CONTROL-PLANE mode to apply a control-plane ACL. Control-plane ACLs are only applied on the ingress traffic. By default, the control-plane ACL is applied to the front-panel ports as well as the management port. The `no` version of this command deletes an IPv6 ACL configuration.

Example

```
OS10(conf-if-eth1/1/8)# ipv6 access-group test6 in
```

Example (Control-plane ACL)

```
OS10# configure terminal
OS10(config)# control-plane
OS10(config-control-plane)# ipv6 access-group aaa-cp-acl in
```

Supported Releases 10.2.0E or later; 10.4.1 or later (control-plane ACL)

ipv6 access-list

Creates an IP access list to filter based on an IPv6 address.

Syntax `ipv6 access-list access-list-name`

Parameters `access-list-name` — Enter the name of an IPv6 access list. A maximum of 140 characters.

Default Not configured

Command Mode CONFIGURATION

Usage Information None

Example

```
OS10(config)# ipv6 access-list acl6
```

Supported Release 10.2.0E or later

ipv6 prefix-list deny

Creates a prefix list to deny route filtering from a specified IPv6 network address.

Syntax `ipv6 prefix-list prefix-list-name deny {A::B/x [ge | le] prefix-len}`

Parameters	<ul style="list-style-type: none"> • <i>prefix-list-name</i> — Enter the IPv6 prefix list name. • <i>A::B/x</i> — Enter the IPv6 address to deny. • <i>ge</i> — Enter to indicate the network address is greater than or equal to the range specified. • <i>le</i> — Enter to indicate the network address is less than or equal to the range specified. • <i>prefix-len</i> — Enter the prefix length.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the specified prefix list.
Example	<pre>OS10(config)# ipv6 prefix-list TEST deny AB10::1/128 ge 10 le 30</pre>
Supported Release	10.3.0E or later

ipv6 prefix-list description

Configures a description of an IPv6 prefix-list.

Syntax	<code>ipv6 prefix-list name description</code>
Parameters	<ul style="list-style-type: none"> • <i>name</i> — Enter the name of the IPv6 prefix-list. • <i>description</i> — Enter the description for the named prefix-list.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the specified prefix list.
Example	<pre>OS10(config)# ipv6 prefix-list TEST description TEST_LIST</pre>
Supported Release	10.3.0E or later

ipv6 prefix-list permit

Creates a prefix-list to permit route filtering from a specified IPv6 network address.

Syntax	<code>ipv6 prefix-list prefix-list-name permit {A::B/x [ge le] prefix-len}</code>
Parameters	<ul style="list-style-type: none"> • <i>prefix-list-name</i> — Enter the IPv6 prefix-list name. • <i>A::B/x</i> — Enter the IPv6 address to permit. • <i>ge</i> — Enter to indicate the network address is greater than or equal to the range specified. • <i>le</i> — Enter to indicate the network address is less than or equal to the range specified. • <i>prefix-len</i> — Enter the prefix length.
Defaults	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the specified prefix-list.
Example	<pre>OS10(config)# ipv6 prefix-list TEST permit AB20::1/128 ge 10 le 30</pre>
Supported Release	10.3.0E or later

ipv6 prefix-list seq deny

Configures a filter to deny route filtering from a specified prefix-list.

Syntax `ipv6 prefix-list [name] seq num deny {A::B/x [ge | le] prefix-len}`

- Parameters**
- `name` — (Optional) Enter the name of the IPv6 prefix-list.
 - `num` — Enter the sequence number of the specified IPv6 prefix-list.
 - `A::B/x` — Enter the IPv6 address and mask in /prefix format (/x).
 - `ge` — Enter to indicate the network address is greater than or equal to the range specified.
 - `le` — Enter to indicate the network address is less than or equal to the range specified.
 - `prefix-len` — Enter the prefix length.

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the specified prefix-list.

Example

```
OS10(config)# ipv6 prefix-list TEST seq 65535 deny AB20::1/128 ge 10
```

Supported Release 10.3.0E or later

ipv6 prefix-list seq permit

Configures a filter to permit route filtering from a specified prefix-list.

Syntax `ipv6 prefix-list [name] seq num permit A::B/x [ge | le] prefix-len`

- Parameters**
- `name` — (Optional) Enter the name of the IPv6 prefix-list.
 - `num` — Enter the sequence number of the specified IPv6 prefix list.
 - `A::B/x` — Enter the IPv6 address and mask in /prefix format (/x).
 - `ge` — Enter to indicate the network address is greater than or equal to the range specified.
 - `le` — Enter to indicate the network address is less than or equal to the range specified.
 - `prefix-len` — Enter the prefix length.

Defaults Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the specified prefix-list.

Example

```
OS10(config)# ipv6 prefix-list TEST seq 65535 permit AB10::1/128 ge 30
```

Supported Release 10.3.0E or later

mac access-group

Configures a MAC access group.

Syntax `mac access-group access-list-name {in | out}`

- Parameters**
- `access-list-name` — Enter the name of a MAC access list. A maximum of 140 characters.
 - `in` — Apply the ACL to incoming traffic.
 - `out` — Apply the ACL to outgoing traffic.

Default Not configured

Command Mode	CONFIGURATION CONTROL-PLANE
Usage Information	Use this command in the CONTROL-PLANE mode to apply a control-plane ACL. Control-plane ACLs are only applied on the ingress traffic. By default, the control-plane ACL is applied to the front-panel ports. The no version of this command resets the value to the default.
Example	<pre>OS10(config)# mac access-group maclist in OS10(conf-mac-acl)#</pre>
Example (Control-plane ACL)	<pre>OS10# configure terminal OS10(config)# control-plane OS10(config-control-plane)# mac access-group maclist in</pre>
Supported Releases	10.2.0E or later; 10.4.1 or later (control-plane ACL)

mac access-list

Creates a MAC access list to filter based on an MAC address.

Syntax	<code>mac access-list <i>access-list-name</i></code>
Parameters	<i>access-list-name</i> — Enter the name of a MAC access list. A maximum of 140 characters.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	None
Example	<pre>OS10(config)# mac access-list maclist</pre>
Supported Releases	10.2.0E or later

permit

Configures a filter to allow packets with a specific IP address.

Syntax	<code>permit [<i>protocol-number</i> icmp ip tcp udp] [A.B.C.D A.B.C.D/x any host <i>ip-address</i>] [A.B.C.D A.B.C.D/x any host <i>ip-address</i>] [capture dscp <i>value</i> fragment]</code>
Parameters	<ul style="list-style-type: none"> • <i>protocol-number</i> — (Optional) Enter the protocol number identified in the IP header, from 0 to 255. • icmp — (Optional) Enter the ICMP address to permit. • ip — (Optional) Enter the IP address to permit. • tcp — (Optional) Enter the TCP address to permit. • udp — (Optional) Enter the UDP address to permit. • A.B.C.D — Enter the IP address in dotted decimal format. • A.B.C.D/x — Enter the number of bits that must match the dotted decimal address. • any — (Optional) Set all routes which are subject to the filter: <ul style="list-style-type: none"> ◦ capture — (Optional) Capture packets the filter processes. ◦ dscp <i>value</i> — (Optional) Permit a packet based on the DSCP values, from 0 to 63. ◦ fragment — (Optional) Use ACLs to control packet fragments. • host <i>ip-address</i> — (Optional) Enter the IP address to use a host address only.

Default Not configured
Command Mode IPV4-ACL
Usage Information The no version of this command removes the filter.

Example

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# permit udp any any capture session 1
```

Supported Releases 10.2.0E or later

permit (IPv6)

Configures a filter to allow packets with a specific IPv6 address.

Syntax permit [*protocol-number* | icmp | ipv6 | tcp | udp] [A::B | A::B/x | any | host *ipv6-address*] [A::B | A:B/x | any | host *ipv6-address*] [capture | dscp *value* | fragment]

Parameters

- *protocol-number* — (Optional) Enter the protocol number identified in the IPv6 header, from 0 to 255.
- icmp — (Optional) Enter the ICMP address to permit.
- ipv6 — (Optional) Enter the IPv6 address to permit.
- tcp — (Optional) Enter the TCP address to permit.
- udp — (Optional) Enter the UDP address to permit.
- A::B — Enter the IPv6 address in hexadecimal format separated by colons.
- A::B/x — Enter the number of bits that must match the IPv6 address.
- any — (Optional) Set all routes which are subject to the filter:
 - capture — (Optional) Capture packets the filter processes.
 - dscp *value* — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - fragment — (Optional) Use ACLs to control packet fragments.
- host *ip-address* — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured
Command Mode IPV6-ACL
Usage Information The no version of this command removes the filter.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# permit udp any any capture session 1
```

Supported Releases 10.2.0E or later

permit (MAC)

Configures a filter to allow packets with a specific MAC address.

Syntax permit {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] | any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] | any} [*protocol-number* | capture | cos | vlan]

Parameters

- nn:nn:nn:nn:nn:nn — Enter the MAC address.
- 00:00:00:00:00:00 — (Optional) Enter which bits in the MAC address must match. If you do not enter a mask, a mask of 00:00:00:00:00:00 applies.
- any — (Optional) Set which routes are subject to the filter:

- *protocol-number* — Enter the MAC protocol number identified in the MAC header, from 600 to ffff.
- *capture* — (Optional) Enter the capture packets the filter processes.
- *cos* — (Optional) Enter the CoS value, from 0 to 7.
- *vlan* — (Optional) Enter the VLAN number, from 1 to 4093.

Default Not configured

Command Mode MAC-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# mac access-list macacl
OS10(conf-mac-acl)# permit 00:00:00:00:11:11 00:00:11:11:11:11 any cos 7
OS10(conf-mac-acl)# permit 00:00:00:00:11:11 00:00:11:11:11:11 any vlan 2
```

Supported Releases 10.2.0E or later

permit icmp

Configures a filter to permit all or specific Internet Control Message Protocol (ICMP) messages.

Syntax `permit icmp [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | dscp value | fragment]`

- Parameters**
- *A.B.C.D* — Enter the IP address in dotted decimal format.
 - *A.B.C.D/x* — Enter the number of bits that must match the dotted decimal address.
 - *any* — (Optional) Set all routes which are subject to the filter:
 - *capture* — (Optional) Capture packets the filter processes.
 - *dscp value* — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - *fragment* — (Optional) Use ACLs to control packet fragments.
 - *host ip-address* — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPv4-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# permit icmp any any capture session 1
```

Supported Releases 10.2.0E or later

permit icmp (IPv6)

Configures a filter to permit all or specific ICMP messages.

Syntax `permit icmp [A::B | A::B/x | any | host ipv6-address] [A::B | A:B/x | any | host ipv6-address] [capture | dscp value | fragment]`

- Parameters**
- *A::B* — Enter the IPv6 address in hexadecimal format separated by colons.
 - *A::B/x* — Enter the number of bits that must match the IPv6 address.
 - *any* — (Optional) Set all routes which are subject to the filter:
 - *capture* — (Optional) Capture packets the filter processes.
 - *dscp value* — (Optional) Permit a packet based on the DSCP values, from 0 to 63.

- `fragment` — (Optional) Use ACLs to control packet fragments.
- `host ipv6-address` — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# permit icmp any any capture session 1
```

Supported Releases 10.2.0E or later

permit ip

Configures a filter to permit all or specific packets from an IP address.

Syntax `permit ip [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | dscp | fragments]`

- Parameters**
- `A.B.C.D` — Enter the IP address in dotted decimal format.
 - `A.B.C.D/x` — Enter the number of bits to match to the dotted decimal address.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - `fragments` — (Optional) Use ACLs to control packet fragments.
 - `host ip-address` — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(conf-ipv4-acl)# permit ip any any capture session 1
```

Supported Releases 10.2.0E or later

permit ipv6

Configures a filter to permit all or specific packets from an IPv6 address.

Syntax `permit ipv6 [A::B | A::B/x | any | host ipv6-address] [A::B | A:B/x | any | host ipv6-address] [capture| dscp | fragment]`

- Parameters**
- `A::B` — (Optional) Enter the source IPv6 address from which the packet was sent and the destination address.
 - `A::B/x` — (Optional) Enter the source network mask in /prefix format (/x) and the destination mask.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Enter to capture packets the filter processes.
 - `dscp value` — (Optional) Enter to deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Enter to use ACLs to control packet fragments.
 - `host ipv6-address` — Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPv6-ACL
Usage Information The no version of this command removes the filter.

Example

```
OS10(conf-ipv6-acl)# permit ipv6 any any count capture session 1
```

Supported Releases 10.2.0E or later

permit tcp

Configures a filter to permit TCP packets meeting the filter criteria.

Syntax `permit tcp [A.B.C.D | A.B.C.D/x | any | host ip-address [operator]]
[[A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [ack | fin | psh |
rst | syn | urg] [capture | dscp value | fragment]`

Parameters

- A.B.C.D — Enter the IP address in dotted decimal format.
- A.B.C.D/x — Enter the number of bits that must match the dotted decimal address.
- any — (Optional) Set all routes which are subject to the filter:
 - capture — (Optional) Capture packets the filter processes.
 - dscp *value* — (Optional) Permit a packet based on the DSCP values, 0 to 63.
 - fragment — (Optional) Use ACLs to control packet fragments.
 - ack — (Optional) Set the bit as acknowledgement.
 - fin — (Optional) Set the bit as finish—no more data from sender.
 - psh — (Optional) Set the bit as push.
 - rst — (Optional) Set the bit as reset.
 - syn — (Optional) Set the bit as synchronize.
 - urg — (Optional) Set the bit set as urgent.
- **i** **NOTE:** The control-plane ACLs do not support the any parameter.
- *operator* — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - eq — Equal to
 - gt — Greater than
 - lt — Lesser than
 - neq — Not equal to
 - range — Range of ports, including the specified port numbers.
- **i** **NOTE:** The control-plane ACLs support only the eq operator.
- host *ip-address* — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPv4-ACL

Usage Information The no version of this command removes the filter.

Example


```
OS10(conf-ipv4-acl)# permit tcp any any capture session 1
```

Supported Releases 10.2.0E or later

permit tcp (IPv6)

Configures a filter to permit TCP packets meeting the filter criteria.

Syntax `permit tcp [A::B | A::B/x | any | host ipv6-address [eq | lt | gt | neq | range]] [A::B | A::B/x | any | host ipv6-address [eq | lt | gt | neq | range]] [ack | fin | psh | rst | syn | urg] [capture | dscp value | fragment]`

- Parameters**
- `A::B` — Enter the IPv6 address in hexadecimal format separated by colons.
 - `A::B/x` — Enter the number of bits that must match the IPv6 address.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
-  **NOTE:** The control-plane ACLs do not support the `any` parameter.
- `host ipv6-address` — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# permit tcp any any capture session 1
```

Supported Releases 10.2.0E or later

permit udp

Configures a filter that allows UDP packets meeting the filter criteria.

Syntax `permit udp [A.B.C.D | A.B.C.D/x | any | host ip-address [eq | lt | gt | neq | range]] [[A.B.C.D | A.B.C.D/x | any | host ip-address [eq | lt | gt | neq | range]] [ack | fin | psh | rst | syn | urg] [capture | dscp value | fragment]`

- Parameters**
- `A.B.C.D` — Enter the IP address in dotted decimal format.
 - `A.B.C.D/x` — Enter the number of bits that must match the dotted decimal address.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `eq` — (Optional) Permit packets which are equal to.
 - `lt` — (Optional) Permit packets which are less than.
 - `gt` — (Optional) Permit packets which are greater than.
 - `neq` — (Optional) Permit packets which are not equal to.
 - `range` — (Optional) Permit packets with a specific source and destination address.
 - `ack` — (Optional) Set the bit as acknowledgement.
 - `fin` — (Optional) Set the bit as finish—no more data from sender.
 - `psh` — (Optional) Set the bit as push.
 - `rst` — (Optional) Set the bit as reset.
 - `syn` — (Optional) Set the bit as synchronize.
 - `urg` — (Optional) Set the bit set as urgent.

 **NOTE:** The control-plane ACL supports only the `eq` operator.

- `host ip-address` — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# permit udp any any capture session 1
```

Supported Releases 10.2.0E or later

permit udp (IPv6)

Configures a filter to permit UDP packets meeting the filter criteria.

Syntax `permit udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A:B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | dscp value | fragment]`

Parameters

- `A::B` — Enter the IPv6 address in hexadecimal format separated by colons.
- `A::B/x` — Enter the number of bits that must match the IPv6 address.
- `any` — (Optional) Enter for all routes to be subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `ack` — (Optional) Set the bit as acknowledgement.
 - `fin` — (Optional) Set the bit as finish—no more data from sender.
 - `psh` — (Optional) Set the bit as push.
 - `rst` — (Optional) Set the bit as reset.
 - `syn` — (Optional) Set the bit as synchronize.
 - `urg` — (Optional) Set the bit set as urgent.
- **NOTE:** The control-plane ACL supports only the `eq` operator.
- `operator` — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - `eq` — Equal to
 - `gt` — Greater than
 - `lt` — Lesser than
 - `neq` — Not equal to
 - `range` — Range of ports, including the specified port numbers.
- `host ipv6-address` — (Optional) Enter the keyword and the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(conf-ipv6-acl)# permit udp any any capture session 1 count
```

Supported Releases 10.2.0E or later

remark

Specifies an ACL entry description.

Syntax	<code>remark [remark-number] [description]</code>
Parameters	<ul style="list-style-type: none">• <i>remark-number</i> — (Optional) Enter a remark number, from 1 to 16777214 for IPv4, IPv6, and MAC.• <i>description</i> — (Optional) Enter a description. A maximum of 80 characters.
Default	Not configured
Command Mode	IPV4-ACL
Usage Information	Use different sequence numbers for the remark and the ACL rule. Configure up to 16777214 remarks for a given IPv4, IPv6, or MAC.
Example	<pre>OS10(conf-ipv4-acl)# remark 10 Deny rest of the traffic OS10(conf-ipv4-acl)# remark 5 Permit traffic from XYZ Inc.</pre>
Supported Releases	10.2.0E or later

seq deny

Assigns a sequence number to deny IP addresses while creating the filter.

Syntax	<code>seq sequence-number deny [protocol-number icmp ip tcp udp] [A.B.C.D A.B.C.D/x any host ip-address] [A.B.C.D A.B.C.D/x any host ip-address] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <i>sequence-number</i> — Enter the sequence number to identify the ACL for editing and sequencing number, from 1 to 16777214.• <i>protocol-number</i> — (Optional) Enter the protocol number, from 0 to 255.• <i>icmp</i> — (Optional) Enter the ICMP address to deny.• <i>ip</i> — (Optional) Enter the IP address to deny.• <i>tcp</i> — (Optional) Enter the TCP address to deny.• <i>udp</i> — (Optional) Enter the UDP address to deny.• <i>A.B.C.D</i> — Enter the IP address in dotted decimal format.• <i>A.B.C.D/x</i> — Enter the number of bits that must match the dotted decimal address.• <i>any</i> — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ <i>capture</i> — (Optional) Capture packets the filter processes.◦ <i>dscp value</i> — (Optional) Permit a packet based on the DSCP values, from 0 to 63.◦ <i>fragment</i> — (Optional) Use ACLs to control packet fragments.• <i>host ip-address</i> — (Optional) Enter the IP address to use a host address only.
Default	Not configured
Command Mode	IPV4-ACL
Usage Information	The no version of this command removes the filter, or use the <code>no seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ip access-list testflow OS10(conf-ipv4-acl)# seq 10 deny tcp any any capture session 1</pre>
Supported Releases	10.2.0E or later

seq deny (IPv6)

Assigns a sequence number to deny IPv6 addresses while creating the filter.

Syntax	<code>seq sequence-number deny [protocol-number icmp ip tcp udp] [A::B A::B/x any host ipv6-address] [A::B A::B/x any host ipv6-address] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <i>sequence-number</i> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• <i>protocol-number</i> — (Optional) Enter the protocol number, from 0 to 255.• <i>icmp</i> — (Optional) Enter the ICMP address to deny.• <i>ip</i> — (Optional) Enter the IP address to deny.• <i>tcp</i> — (Optional) Enter the TCP address to deny.• <i>udp</i> — (Optional) Enter the UDP address to deny.• <i>A::B</i> — Enter the IPv6 address in hexadecimal format separated by colons.• <i>A::B/x</i> — Enter the number of bits that must match the IPv6 address.• <i>any</i> — (Optional) Determine route types:<ul style="list-style-type: none">◦ <i>capture</i> — (Optional) Enter to capture packets the filter processes.◦ <i>dscp value</i> — (Optional) Enter to deny a packet based on the DSCP values, from 0 to 63.◦ <i>fragment</i> — (Optional) Enter to use ACLs to control packet fragments.• <i>host ipv6-address</i> — (Optional) Enter to use an IPv6 host address only.
Default	Not configured
Command Mode	IPv6-ACL
Usage Information	The <code>no</code> version of this command removes the filter, or use the <code>no seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# seq 5 deny ipv6 any any capture session 1 count</pre>
Supported Releases	10.2.0E or later

seq deny (MAC)

Assigns a sequence number to a deny filter in a MAC access list while creating the filter.

Syntax	<code>seq sequence-number deny {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] any} [protocol-number capture cos vlan]</code>
Parameters	<ul style="list-style-type: none">• <i>sequence-number</i> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• <i>nn:nn:nn:nn:nn:nn</i> — Enter the source MAC address.• <i>00:00:00:00:00:00</i> — (Optional) Enter which bits in the MAC address must match. If you do not enter a mask, a mask of <code>00:00:00:00:00:00</code> applies.• <i>any</i> — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ <i>protocol-number</i> — Protocol number identified in the MAC header, from 600 to ffff.◦ <i>capture</i> — (Optional) Capture packets the filter processes.◦ <i>cos</i> — (Optional) CoS value, from 0 to 7.◦ <i>vlan</i> — (Optional) VLAN number, from 1 to 4093.
Default	Not configured
Command Mode	CONFIG-MAC-ACL
Usage Information	The <code>no</code> version of this command removes the filter, or use the <code>no seq sequence-number</code> command if you know the filter's sequence number.

Example

```
OS10(config)# mac access-list macacl
OS10(conf-mac-acl)# seq 10 deny 00:00:00:00:11:11 00:00:11:11:11:11 any
cos 7
OS10(conf-mac-acl)# seq 20 deny 00:00:00:00:11:11 00:00:11:11:11:11 any
vlan 2
```

Supported Releases 10.2.0E or later

seq deny icmp

Assigns a filter to deny Internet Control Message Protocol (ICMP) messages while creating the filter.

Syntax `seq sequence-number deny icmp [A.B.C.D | A.B.C.D/x | any | host ip-address] [A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | dscp value | fragment]`

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - A.B.C.D — Enter the IP address in dotted decimal format.
 - A.B.C.D/x — Enter the number of bits that must match the dotted decimal address.
 - any — (Optional) Set all routes which are subject to the filter:
 - *capture* — (Optional) Capture packets the filter processes.
 - *dscp value* — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - *fragment* — (Optional) Use ACLs to control packet fragments.
 - *host ip-address* — (Optional) Enter the IP address to use a host IP address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The no version of this command removes the filter, or use the no `seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# seq 5 deny icmp any any capture session 1
```

Supported Releases 10.2.0E or later

seq deny icmp (IPv6)

Assigns a sequence number to deny ICMP messages while creating the filter.

Syntax `seq sequence-number deny icmp [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | dscp value | fragment]`

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - A::B — Enter the IPv6 address in hexadecimal format separated by colons.
 - A::B/x — Enter the number of bits that must match the IPv6 address.
 - any — (Optional) Set all routes which are subject to the filter:
 - *capture* — (Optional) Capture packets the filter processes.
 - *dscp value* — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - *fragment* — (Optional) Use ACLs to control packet fragments.
 - *host ipv6-address* — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The no version of this command removes the filter, or use the no seq *sequence-number* command if you know the filter's sequence number.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# seq 10 deny icmp any any capture session 1
```

Supported Releases 10.2.0E or later

seq deny ip

Assigns a sequence number to deny IP addresses while creating the filter.

Syntax seq *sequence-number* deny ip [A.B.C.D | A.B.C.D/x | any | host *ip-address*] [A.B.C.D | A.B.C.D/x | any | host *ip-address*] [capture | dscp *value* | fragment]

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - A.B.C.D — Enter the IP address in dotted decimal format.
 - A.B.C.D/x — Enter the number of bits that must match the dotted decimal address.
 - any — (Optional) Set all routes which are subject to the filter:
 - capture — (Optional) Capture packets the filter processes.
 - dscp *value* — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - fragment — (Optional) Use ACLs to control packet fragments.
 - host *ip-address* — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The no version of this command removes the filter, or use the no seq *sequence-number* command if you know the filter's sequence number.

Example

```
OS10(config)# ip access-list egress
OS10(config-ipv4-acl)# seq 10 deny ip any any capture session 1
```

Supported Releases 10.2.0E or later

seq deny ipv6

Assigns a filter to deny IPv6 addresses while creating the filter.

Syntax seq *sequence-number* deny ip [A::B | A::B/x | any | host *ipv6-address*] [A::B | A::B/x | any | host *ipv6-address*] [capture | dscp *value* | fragment]

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - A::B — Enter the IPv6 address in hexadecimal format separated by colons.
 - A::B/x — Enter the number of bits that must match the IPv6 address.
 - any — (Optional) Set all routes which are subject to the filter:
 - capture — (Optional) Capture packets the filter processes.
 - dscp *value* — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - fragment — (Optional) Use ACLs to control packet fragments.
 - host *ip-address* — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information	The no version of this command removes the filter, or use the no <code>seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# seq 10 deny ipv6 any any capture session 1</pre>
Supported Releases	10.2.0E or later

seq deny tcp

Assigns a filter to deny TCP packets while creating the filter.

Syntax	<code>seq sequence-number deny tcp [A.B.C.D A.B.C.D/x any host ip-address [operator]] [[A.B.C.D A.B.C.D/x any host ip-address [operator]] [ack fin psh rst syn urg] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none"> • <code>sequence-number</code> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214. • <code>A.B.C.D</code> — Enter the IP address in dotted decimal format. • <code>A.B.C.D/x</code> — Enter the number of bits that must match the dotted decimal address. • <code>any</code> — (Optional) Set all routes which are subject to the filter: <ul style="list-style-type: none"> ◦ <code>capture</code> — (Optional) Capture packets the filter processes. ◦ <code>dscp value</code> — (Optional) Deny a packet based on the DSCP values, from 0 to 63. ◦ <code>fragment</code> — (Optional) Use ACLs to control packet fragments. ◦ <code>ack</code> — (Optional) Set the bit as acknowledgement. ◦ <code>fin</code> — (Optional) Set the bit as finish—no more data from sender. ◦ <code>psh</code> — (Optional) Set the bit as push. ◦ <code>rst</code> — (Optional) Set the bit as reset. ◦ <code>syn</code> — (Optional) Set the bit as synchronize. ◦ <code>urg</code> — (Optional) Set the bit set as urgent. • <code>operator</code> — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available: <ul style="list-style-type: none"> ◦ <code>eq</code> — Equal to ◦ <code>gt</code> — Greater than ◦ <code>lt</code> — Lesser than ◦ <code>neq</code> — Not equal to ◦ <code>range</code> — Range of ports, including the specified port numbers. • <code>host ip-address</code> — (Optional) Enter the IP address to use a host address only.
Default	Not configured
Command Mode	IPV4-ACL
Usage Information	The no version of this command removes the filter, or use the no <code>seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ip access-list egress OS10(conf-ipv4-acl)# seq 10 deny tcp any any capture session 1</pre>
Supported Releases	10.2.0E or later

seq deny tcp (IPv6)

Assigns a filter to deny TCP packets while creating the filter.

Syntax	<code>seq sequence-number deny tcp [A::B A::B/x any host ipv6-address [operator]] [A::B A:B/x any host ipv6-address [operator]] [ack fin psh rst syn urg] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <i>sequence-number</i> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• <i>A::B</i> — Enter the IPv6 address in hexadecimal format separated by colons.• <i>A::B/x</i> — Enter the number of bits that must match the IPv6 address.• <i>any</i> — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ <i>capture</i> — (Optional) Capture packets the filter processes.◦ <i>dscp value</i> — (Optional) Deny a packet based on the DSCP values, from 0 to 63.◦ <i>fragment</i> — (Optional) Use ACLs to control packet fragments.◦ <i>ack</i> — (Optional) Set the bit as acknowledgement.◦ <i>fin</i> — (Optional) Set the bit as finish—no more data from sender.◦ <i>psh</i> — (Optional) Set the bit as push.◦ <i>rst</i> — (Optional) Set the bit as reset.◦ <i>syn</i> — (Optional) Set the bit as synchronize.◦ <i>urg</i> — (Optional) Set the bit set as urgent.• <i>operator</i> — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:<ul style="list-style-type: none">◦ <i>eq</i> — Equal to◦ <i>gt</i> — Greater than◦ <i>lt</i> — Lesser than◦ <i>neq</i> — Not equal to◦ <i>range</i> — Range of ports, including the specified port numbers.• <i>host ip-address</i> — (Optional) Enter the IPv6 address to use a host address only.
Default	Not configured
Command Mode	IPv6-ACL
Usage Information	The <code>no</code> version of this command removes the filter, or use the <code>no seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# seq 10 deny tcp any any capture session 1</pre>
Supported Releases	10.2.0E or later

seq deny udp

Assigns a filter to deny UDP packets while creating the filter.

Syntax	<code>seq sequence-number deny udp [A.B.C.D A.B.C.D/x any host ip-address [operator]] [[A.B.C.D A.B.C.D/x any host ip-address [operator]]] [ack fin psh rst syn urg] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <i>sequence-number</i> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• <i>A.B.C.D</i> — Enter the IP address in dotted decimal format.• <i>A.B.C.D/x</i> — Enter the number of bits that must match the dotted decimal address.• <i>any</i> — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ <i>capture</i> — (Optional) Capture packets the filter processes.◦ <i>dscp value</i> — (Optional) Deny a packet based on the DSCP values, from 0 to 63.

- `fragment` — (Optional) Use ACLs to control packet fragments.
- `ack` — (Optional) Set the bit as acknowledgment.
- `fin` — (Optional) Set the bit as finish—no more data from sender.
- `psh` — (Optional) Set the bit as push.
- `rst` — (Optional) Set the bit as reset.
- `syn` — (Optional) Set the bit as synchronize.
- `urg` — (Optional) Set the bit set as urgent.
- `operator` — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - `eq` — Equal to
 - `gt` — Greater than
 - `lt` — Lesser than
 - `neq` — Not equal to
 - `range` — Range of ports, including the specified port numbers.
- `host ip-address` — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The `no` version of this command removes the filter, or use the `no seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# seq 10 deny udp any any capture session 1
```

Supported Releases 10.2.0E or later

seq deny udp (IPv6)

Assigns a filter to deny UDP packets while creating the filter.

Syntax `seq sequence-number deny udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A:B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | dscp value | fragment]`

- Parameters**
- `sequence-number` — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - `A::B` — Enter the IPv6 address in hexadecimal format separated by colons.
 - `A::B/x` — Enter the number of bits that must match the IPv6 address.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `ack` — (Optional) Set the bit as acknowledgment.
 - `fin` — (Optional) Set the bit as finish—no more data from sender.
 - `psh` — (Optional) Set the bit as push.
 - `rst` — (Optional) Set the bit as reset.
 - `syn` — (Optional) Set the bit as synchronize.
 - `urg` — (Optional) Set the bit set as urgent.
 - `operator` — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - `eq` — Equal to
 - `gt` — Greater than
 - `lt` — Lesser than
 - `neq` — Not equal to

- *range* — Range of ports, including the specified port numbers.
- *host ipv6-address* — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter, or use the `no seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# seq 10 deny udp any any capture session 1
```

Supported Releases 10.2.0E or later

seq permit

Assigns a sequence number to permit packets while creating the filter.

Syntax `seq sequence-number permit [protocol-number A.B.C.D | A.B.C.D/x | any | host ip-address] [A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | dscp value| fragment]`

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - *protocol-number* — (Optional) Enter the protocol number, from 0 to 255.
 - *A.B.C.D* — Enter the IP address in dotted decimal format.
 - *A.B.C.D/x* — Enter the number of bits that must match the dotted decimal address.
 - *any* — (Optional) Set all routes which are subject to the filter:
 - *capture* — (Optional) Capture packets the filter processes.
 - *dscp value* — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - *fragment* — (Optional) Use ACLs to control packet fragments.
 - *host ip-address* — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The `no` version of this command removes the filter.

Example

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# seq 10 permit ip any any capture session 1
```

Supported Releases 10.2.0E or later

seq permit (IPv6)

Assigns a sequence number to permit IPv6 packets, while creating a filter.

Syntax `seq sequence-number permit protocol-number [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | dscp value | fragment]`

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - *protocol-number* — (Optional) Enter the protocol number, from 0 to 255.
 - *A::B* — Enter the IPv6 address in hexadecimal format separated by colons.
 - *A::B/x* — Enter the number of bits that must match the IPv6 address.

- `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Enter to capture packets the filter processes.
 - `dscp value` — (Optional) Enter the DSCP value to permit a packet, from 0 to 63.
 - `fragment` — (Optional) Enter to use ACLs to control packet fragments.
- `host ipv6-address` — (Optional) Enter the IPv6 address to be used as the host address.

Default Not configured

Command Mode IPv6-ACL

Usage Information The `no` version of this command removes the filter, or use the `no seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# seq 10 permit ipv6 any any capture session 1
```

Supported Releases 10.2.0E or later

seq permit (MAC)

Assigns a sequence number to permit MAC addresses while creating a filter.

Syntax `seq sequence-number permit {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] | any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] | any} [protocol-number | capture | cos | vlan]`

- Parameters**
- `sequence-number` — Enter the sequence number to identify the route-map for editing and sequencing, from 1 to 16777214.
 - `nn:nn:nn:nn:nn:nn` — Enter the MAC address of the network from or to which the packets were sent.
 - `00:00:00:00:00:00` — (Optional) Enter which bits in the MAC address must match. If you do not enter a mask, a mask of `00:00:00:00:00:00` applies.
 - `any` — (Optional) Set all routes to be subject to the filter:
 - `protocol-number` — (Optional) Enter the protocol number identified in the MAC header, from 600 to ffff.
 - `capture` — (Optional) Enter the capture packets the filter processes.
 - `cos` — (Optional) Enter the CoS value, from 0 to 7.
 - `vlan` — (Optional) Enter the VLAN number, from 1 to 4093.

Default Not configured

Command Mode MAC-ACL

Usage Information The `no` version of this command removes the filter, or use the `no seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# mac access-list macacl
OS10(conf-mac-acl)# seq 10 permit 00:00:00:00:11:11 00:00:11:11:11:11
any cos 7
OS10(conf-mac-acl)# seq 20 permit 00:00:00:00:11:11 00:00:11:11:11:11
any vlan 2
```

Supported Releases 10.2.0E or later

seq permit icmp

Assigns a sequence number to allow ICMP messages while creating the filter

Syntax	<code>seq sequence-number permit icmp [A.B.C.D A.B.C.D/x any host ip-address] [A.B.C.D A.B.C.D/x any host ip-address] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <code>sequence-number</code> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• <code>A.B.C.D</code> — Enter the IP address in dotted decimal format.• <code>A.B.C.D/x</code> — Enter the number of bits that must match the dotted decimal address.• <code>any</code> — (Optional) Set all routes are which subject to the filter:<ul style="list-style-type: none">◦ <code>capture</code> — (Optional) Capture packets the filter processes.◦ <code>dscp value</code> — (Optional) Permit a packet based on the DSCP values, from 0 to 63.◦ <code>fragment</code> — (Optional) Use ACLs to control packet fragments.• <code>host ip-address</code> — (Optional) Enter the IP address to use a host address only.
Default	Not configured
Command Mode	IPV4-ACL
Usage Information	The no version of this command removes the filter, or use the <code>no seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ip access-list egress OS10(conf-ip4-acl)# seq 5 permit icmp any any capture session 1</pre>
Supported Releases	10.2.0E or later

seq permit icmp (IPv6)

Assigns a sequence number to allow ICMP messages while creating the filter.

Syntax	<code>seq sequence-number permit icmp [A::B A::B/x any host ipv6-address] [A::B A::B/x any host ipv6-address] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <code>sequence-number</code> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• <code>A::B</code> — Enter the IPv6 address in hexadecimal format separated by colons.• <code>A::B/x</code> — Enter the number of bits that must match the IPv6 address.• <code>any</code> — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ <code>capture</code> — (Optional) Capture packets the filter processes.◦ <code>dscp value</code> — (Optional) Permit a packet based on the DSCP values, from 0 to 63.◦ <code>fragment</code> — (Optional) Use ACLs to control packet fragments.• <code>host ipv6-address</code> — (Optional) Enter the IPv6 address to use a host address only.
Default	Not configured
Command Mode	IPV6-ACL
Usage Information	The no version of this command removes the filter, or use the <code>no seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# seq 5 permit icmp any any capture session 1</pre>
Supported Releases	10.2.0E or later

seq permit ip

Assigns a sequence number to allow packets while creating the filter.

Syntax `seq sequence-number permit ip [A.B.C.D | A.B.C.D/x | any | host ip-address] [A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | dscp value | fragment]`

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - A.B.C.D — Enter the IP address in dotted decimal format.
 - A.B.C.D/x — Enter the number of bits that must match the dotted decimal address.
 - any — (Optional) Set all routes which are subject to the filter:
 - capture — (Optional) Capture packets the filter processes.
 - dscp value — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - fragment — (Optional) Use ACLs to control packet fragments.
 - host ip-address — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The no version of this command removes the filter, or use the no `seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# seq 5 permit ip any any capture session 1
```

Supported Releases 10.2.0E or later

seq permit ipv6

Assigns a sequence number to allow packets while creating the filter.

Syntax `seq sequence-number permit ipv6 [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | dscp value | fragment]`

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - A::B — Enter the IPv6 address in hexadecimal format separated by colons.
 - A::B/x — Enter the number of bits that must match the IPv6 address.
 - any — (Optional) Set all routes which are subject to the filter:
 - capture — (Optional) Capture packets the filter processes.
 - dscp value — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - fragment — (Optional) Use ACLs to control packet fragments.
 - host ipv6-address — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The no version of this command removes the filter, or use the no `seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ipv6 access-list egress
OS10(conf-ipv6-acl)# seq 5 permit ipv6 any any capture session 1
```

Supported Releases 10.2.0E or later

seq permit tcp

Assigns a sequence number to allow TCP packets while creating the filter.

Syntax	<code>seq sequence-number permit tcp [A.B.C.D A.B.C.D/x any host ip-address [operator]] [[A.B.C.D A.B.C.D/x any host ip-address [operator]]] [ack fin psh rst syn urg] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <i>sequence-number</i> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• A.B.C.D — Enter the IP address in dotted decimal format.• A.B.C.D/x — Enter the number of bits that must match the dotted decimal address.• any — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ capture — (Optional) Capture packets the filter processes.◦ dscp value — (Optional) Permit a packet based on the DSCP values, from 0 to 63.◦ fragment — (Optional) Use ACLs to control packet fragments.◦ ack — (Optional) Set the bit as acknowledgment.◦ fin — (Optional) Set the bit as finish—no more data from sender.◦ psh — (Optional) Set the bit as push.◦ rst — (Optional) Set the bit as reset.◦ syn — (Optional) Set the bit as synchronize.◦ urg — (Optional) Set the bit set as urgent.• operator — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:<ul style="list-style-type: none">◦ eq — Equal to◦ gt — Greater than◦ lt — Lesser than◦ neq — Not equal to◦ range — Range of ports, including the specified port numbers.• host ip-address — (Optional) Enter the IP address to use a host address only.
Default	Not configured
Command Mode	IPV4-ACL
Usage Information	The no version of this command removes the filter, or use the no <code>seq sequence-number</code> command if you know the filter's sequence number.
Example	<pre>OS10(config)# ip access-list egress OS10(conf-ipv4-acl)# seq 5 permit tcp any any capture session 1</pre>
Supported Releases	10.2.0E or later

seq permit tcp (IPv6)

Assigns a sequence number to allow TCP IPv6 packets while creating the filter.

Syntax	<code>seq sequence-number permit tcp [A::B A::B/x any host ipv6-address [operator]] [A::B A::B/x any host ipv6-address [operator]] [ack fin psh rst syn urg] [capture dscp value fragment]</code>
Parameters	<ul style="list-style-type: none">• <i>sequence-number</i> — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.• A::B — Enter the IPv6 address in hexadecimal format separated by colons.• A::B/x — Enter the number of bits that must match the IPv6 address.• any — (Optional) Set all routes which are subject to the filter:<ul style="list-style-type: none">◦ capture — (Optional) Capture packets the filter processes.◦ dscp value — (Optional) Permit a packet based on the DSCP values, from 0 to 63.

- `fragment` — (Optional) Use ACLs to control packet fragments.
- `ack` — (Optional) Set the bit as acknowledgment.
- `fin` — (Optional) Set the bit as finish—no more data from sender.
- `psh` — (Optional) Set the bit as push.
- `rst` — (Optional) Set the bit as reset.
- `syn` — (Optional) Set the bit as synchronize.
- `urg` — (Optional) Set the bit set as urgent.
- `operator` — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - `eq` — Equal to
 - `gt` — Greater than
 - `lt` — Lesser than
 - `neq` — Not equal to
 - `range` — Range of ports, including the specified port numbers.
- `host ipv6-address` — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter, or use the `no seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ipv6 access-list egress
OS10(conf-ipv6-acl)# seq 5 permit tcp any any capture session 1
```

Supported Releases 10.2.0E or later

seq permit udp

Assigns a sequence number to allow UDP packets while creating the filter.

Syntax `seq sequence-number permit udp [A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [[A.B.C.D | A.B.C.D/x | any | host ip-address [operator]]] [ack | fin | psh | rst | syn | urg] [capture | dscp value | fragment]`

- Parameters**
- `sequence-number` — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - `A.B.C.D` — Enter the IP address in dotted decimal format.
 - `A.B.C.D/x` — Enter the number of bits that must match the dotted decimal address.
 - `any` — (Optional) Set all routes which are subject to the filter:
 - `capture` — (Optional) Capture packets the filter processes.
 - `dscp value` — (Optional) Deny a packet based on the DSCP values, from 0 to 63.
 - `fragment` — (Optional) Use ACLs to control packet fragments.
 - `ack` — (Optional) Set the bit as acknowledgment.
 - `fin` — (Optional) Set the bit as finish—no more data from sender.
 - `psh` — (Optional) Set the bit as push.
 - `rst` — (Optional) Set the bit as reset.
 - `syn` — (Optional) Set the bit as synchronize.
 - `urg` — (Optional) Set the bit set as urgent.
 - `operator` — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - `eq` — Equal to
 - `gt` — Greater than
 - `lt` — Lesser than
 - `neq` — Not equal to

- *range* — Range of ports, including the specified port numbers.
- *host ip-address* — (Optional) Enter the IP address to use a host address only.

Default Not configured

Command Mode IPV4-ACL

Usage Information The `no` version of this command removes the filter, or use the `no seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# seq 5 permit udp any any capture session 1
```

Supported Releases 10.2.0E or later

seq permit udp (IPv6)

Assigns a sequence number to allow UDP IPv6 packets while creating a filter.

Syntax `seq sequence-number permit udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A::B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | dscp value | fragment]`

- Parameters**
- *sequence-number* — Enter the sequence number to identify the route-map for editing and sequencing number, from 1 to 16777214.
 - *A::B* — Enter the IPv6 address in hexadecimal format separated by colons.
 - *A::B/x* — Enter the number of bits that must match the IPv6 address.
 - *any* — (Optional) Set all routes which are subject to the filter:
 - *capture* — (Optional) Capture packets the filter processes.
 - *dscp value* — (Optional) Permit a packet based on the DSCP values, from 0 to 63.
 - *fragment* — (Optional) Use ACLs to control packet fragments.
 - *ack* — (Optional) Set the bit as acknowledgment.
 - *fin* — (Optional) Set the bit as finish—no more data from sender.
 - *psh* — (Optional) Set the bit as push.
 - *rst* — (Optional) Set the bit as reset.
 - *syn* — (Optional) Set the bit as synchronize.
 - *urg* — (Optional) Set the bit set as urgent.
 - *operator* — (Optional) Enter a logical operator to match the packets on the specified port number. The following options are available:
 - *eq* — Equal to
 - *gt* — Greater than
 - *lt* — Lesser than
 - *neq* — Not equal to
 - *range* — Range of ports, including the specified port numbers.
 - *host ipv6-address* — (Optional) Enter the IPv6 address to use a host address only.

Default Not configured

Command Mode IPV6-ACL

Usage Information The `no` version of this command removes the filter, or use the `no seq sequence-number` command if you know the filter's sequence number.

Example

```
OS10(config)# ipv6 access-list egress
OS10(conf-ipv6-acl)# seq 5 permit udp any any capture session 1
```

Supported Releases 10.2.0E or later

show access-group

Displays IP, MAC, or IPv6 access-group information.

Syntax `show {ip | mac | ipv6} access-group name`

Parameters

- `ip` — View IP access list information.
- `mac` — View MAC access group information.
- `ipv6` — View IPv6 access group information.
- `access-group name` — Enter the name of the access group.

Default Not configured

Command Mode EXEC

Usage Information None

Example (IP)

```
OS10# show ip access-group aaa
Ingress IP access list aaa on ethernet 3/0
Ingress IP access list aaa on ethernet 4/0
Egress IP access list aaa on ethernet 4/0
```

Example (MAC)

```
OS10# show mac access-group bbb
Ingress MAC access list aaa on ethernet 3/0
Ingress MAC access list aaa on ethernet 4/0
Egress MAC access list aaa on ethernet 4/0
```

Example (IPv6)

```
OS10# show ipv6 access-group ccc
Ingress IPV6 access list aaa on ethernet 3/0
Ingress IPV6 access list aaa on ethernet 4/0
Egress IPV6 access list aaa on ethernet 4/0
```

Example (Control-plane ACL - IP)

```
OS10# show ip access-group aaa-cp-acl
Ingress IP access-list aaa-cp-acl on control-plane data mgmt
```

Example (Control-plane ACL - MAC)

```
OS10# show mac access-group aaa-cp-acl
Ingress MAC access-list aaa-cp-acl on control-plane data
```

Example (Control-plane ACL - IPv6)

```
OS10# show ipv6 access-group aaa-cp-acl
Ingress IPV6 access-list aaa-cp-acl on control-plane data mgmt
```

Supported Releases 10.2.0E or later; 10.4.1 or later (control-plane ACL)

show access-lists

Displays IP, MAC, or IPv6 access-list information.

Syntax `show {ip | mac | ipv6} access-lists {in | out} access-list-name`

Parameters

- `ip` — View IP access list information.
- `mac` — View MAC access group information.
- `ipv6` — View IPv6 access group information.
- `access-lists in | out` — Enter either access lists in or access lists out.
- `access-list-name` — Enter the name of the access-list.

Default Not configured

Command Mode EXEC

Usage Information None

Example (MAC In)

```
OS10# show mac access-lists in
Ingress MAC access list aaa
Active on interfaces :
  ethernet 3/0
  ethernet 3/1
seq 10 permit any any
seq 20 permit 11:11:11:11:11:11 22:22:22:22:22:22 any monitor
```

Example (MAC Out)

```
OS10# show mac access-lists out
Egress MAC access list aaa
Active on interfaces :
  ethernet 3/0
  ethernet 3/1
seq 10 permit any any
seq 20 permit 11:11:11:11:11:11 22:22:22:22:22:22 any monitor
```

Example (IP In)

```
OS10# show ip access-lists in
Ingress IP access list aaaa
Active on interfaces :
  ethernet 3/0
  ethernet 3/1
seq 10 permit ip any any
seq 20 permit tcp any any
seq 30 permit udp any any
```

Example (IP Out)

```
OS10# show ip access-lists out
Egress IP access list aaaa
Active on interfaces :
  ethernet 3/0
  ethernet 3/1
seq 10 permit ip any any
seq 20 permit tcp any any
seq 30 permit udp any any
```

Example (IPv6 In)

```
OS10# show ipv6 access-lists in
Ingress IPV6 access list bbb
Active on interfaces :
  ethernet 3/0
  ethernet 3/1
seq 10 permit any any
Ingress IPV6 access list ggg
Active on interfaces :
  ethernet 3/3
seq 5 permit ipv6 11::/32 any
```

Example (IPv6 Out)

```
OS10# show ipv6 access-lists out
Egress IPV6 access list bbb
Active on interfaces :
  ethernet 3/0
  ethernet 3/1
seq 10 permit any any
Egress IPV6 access list ggg
Active on interfaces :
  ethernet 3/0
seq 5 permit ipv6 11::/32 any
```

Example (IP In - Control-plane ACL)

```
OS10# show ip access-lists in
Ingress IP access-list aaa-cp-acl
Active on interfaces :
  control-plane data
```

```
seq 10 permit ip any any
control-plane mgmt
seq 10 permit ip any any
```

Example (IPv6 Ingress - Control-plane ACL)

```
OS10# show ipv6 access-lists in
Ingress IPV6 access-list aaa-cp-acl
Active on interfaces :
control-plane data
seq 10 permit ipv6 any any
control-plane mgmt
seq 10 permit ipv6 any any
```

Example (MAC Ingress - Control-plane ACL)

```
OS10# show mac access-lists in
Ingress MAC access-list mac-cpl
Active on interfaces :
control-plane data
seq 10 deny any any count (159 packets)
```

Supported Releases 10.2.0E or later; 10.4.1 or later (control-plane ACL)

show ip as-path-access-list

Displays the configured AS path access lists.

Syntax `show ip as-path-access-list [name]`

Parameters *name* — (Optional) Specify the name of the AS path access list.

Defaults None

Command Mode EXEC

Usage Information None

Example

```
OS10# show ip as-path-access-list
ip as-path access-list hello
    permit 123
    deny 35
```

Supported Releases 10.3.0E or later

show ip community-list

Displays the configured IP community lists in alphabetic order.

Syntax `show ip community-list [name]`

Parameters *name* — (Optional) Enter the name of the standard IP community list. A maximum of 140 characters.

Defaults None

Command Mode EXEC

Usage Information None

Example

```
OS10# show ip community-list
Standard Community List hello
    deny local-AS
```

```
permit no-export
deny 1:1
```

Supported Releases 10.3.0E or later

show ip extcommunity-list

Displays the configured IP external community lists in alphabetic order.

Syntax `show ip extcommunity-list [name]`

Parameters *name* — (Optional) Enter the name of the extended IP external community list. A maximum of 140 characters.

Defaults None

Command Mode EXEC

Usage Information None

Example

```
OS10# show ip extcommunity-list
Standard Extended Community List hello
      permit RT:1:1
      deny SOO:1:4
```

Supported Releases 10.3.0E or later

show ip prefix-list

Displays configured IPv4 or IPv6 prefix list information.

Syntax `show {ip | ipv6} prefix-list [prefix-name]`

Parameters

- *ip | ipv6*—(Optional) Displays information related to IPv4 or IPv6.
- *prefix-name* — Enter a text string for the prefix list name. A maximum of 140 characters.

Defaults None

Command Mode EXEC

Usage Information None

Example

```
OS10# show ip prefix-list
ip prefix-list hello:
seq 10 deny 1.2.3.4/24
seq 20 permit 3.4.4.5/32
```

Example (IPv6)

```
OS10# show ipv6 prefix-list
ipv6 prefix-list hello:
seq 10 permit 1::1/64
seq 20 deny 2::2/64
```

Supported Releases 10.3.0E or later

Route-map commands

continue

Configures the next sequence of the route map.

Syntax	<code>continue seq-number</code>
Parameters	<code>seq-number</code> — Enter the next sequence number, from 1 to 65535.
Default	Not configured
Command Mode	ROUTE-MAP
Usage Information	The <code>no</code> version of this command deletes a match.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# continue 65535
```

Supported Releases 10.3.0E or later

match as-path

Configures a filter to match routes that have a certain AS path in their BGP paths.

Syntax	<code>match as-path as-path-name</code>
Parameters	<code>as-path-name</code> — Enter the name of an established AS-PATH ACL. A maximum of 140 characters.
Default	Not configured
Command Mode	ROUTE-MAP
Usage Information	The <code>no</code> version of this command deletes a match AS path filter.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match as-path pathtest1
```

Supported Releases 10.3.0E or later

match community

Configures a filter to match routes that have a certain COMMUNITY attribute in their BGP path.

Syntax	<code>match community community-list-name [exact-match]</code>
Parameters	<ul style="list-style-type: none">• <code>community-list-name</code> — Enter the name of a configured community list.• <code>exact-match</code> — (Optional) Select only those routes with the specified community list name.
Default	Not configured
Command Mode	ROUTE-MAP
Usage Information	The <code>no</code> version of this command deletes the community match filter.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match community commlist1 exact-match
```

Supported Releases 10.3.0E or later

match extcommunity

Configures a filter to match routes that have a certain EXTCOMMUNITY attribute in their BGP path.

Syntax `match extcommunity extcommunity-list-name [exact-match]`

Parameters

- *extcommunity-list-name* — Enter the name of a configured extcommunity list.
- *exact-match* — (Optional) Select only those routes with the specified extcommunity list name.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The no version of this command deletes the extcommunity match filter.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match extcommunity extcommlist1 exact-match
```

Supported Releases 10.3.0E or later

match interface

Configures a filter to match routes whose next-hop is the configured interface.

Syntax `match interface interface`

Parameters *interface* — Interface type:

- *ethernet node/slot/port[:subport]* — Enter the Ethernet interface information as the next-hop interface.
- *port-channel id-number* — Enter the port-channel number as the next-hop interface, from 1 to 128.
- *vlan vlan-id* — Enter the VLAN number as the next-hop interface, from 1 to 4093.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The no version of this command deletes the match.

Example

```
OS10(conf-route-map)# match interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)#
```

Supported Releases 10.2.0E or later

match ip address

Configures a filter to match routes based on IP addresses specified in IP prefix lists.

Syntax `match ip address {prefix-list prefix-list-name | access-list-name}`

Parameters

- *prefix-list-name* — Enter the name of the configured prefix list. A maximum of 140 characters.
- *access-list-name* — Enter the name of the configured access list.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The `no` version of this command deletes a match.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ip address prefix-list test10
```

Supported Releases 10.3.0E or later

match ip next-hop

Configures a filter to match based on the next-hop IP addresses specified in IP prefix lists.

Syntax `match ip next-hop prefix-list prefix-list`

Parameters *prefix-list* — Enter the name of the configured prefix list. A maximum of 140 characters.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The `no` version of this command deletes the match.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ip next-hop prefix-list test100
```

Supported Releases 10.3.0E or later

match ipv6 address

Configures a filter to match routes based on IPv6 addresses specified in IP prefix lists.

Syntax `match ipv6 address {prefix-list prefix-list | access-list}`

Parameters

- *prefix-list* — Enter the name of the configured prefix list. A maximum of 140 characters.
- *access-list* — Enter the name of the access group or list.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The `no` version of this command deletes the match.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ipv6 address test100
```

Supported Releases 10.3.0E or later

match ipv6 next-hop

Configures a filter to match based on the next-hop IPv6 addresses specified in IP prefix lists.

Syntax `match ipv6 next-hop prefix-list prefix-list`

Parameters *prefix-list* — Enter the name of the configured prefix list. A maximum of 140 characters.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The no version of this command deletes the match.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ipv6 next-hop prefix-list test100
```

Supported Releases 10.3.0E or later

match metric

Configures a filter to match on a specific value.

Syntax `match metric metric-value`

Parameters *metric-value* — Enter a value to match the route metric against, from 0 to 4294967295.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The no version of this command deletes the match.

Example

```
OS10(conf-route-map)# match metric 429132
```

Supported Releases 10.2.0E or later

match origin

Configures a filter to match routes based on the origin attribute of BGP.

Syntax `match origin {egp | igp | incomplete}`

Parameters

- `egp` — Match only remote EGP routes.
- `igp` — Match only on local IGP routes.
- `incomplete` — Match on unknown routes that are learned through some other means.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The no version of this command deletes the match.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match origin egp
```

Supported Releases 10.3.0E or later

match route-type

Configures a filter to match routes based on how the route is defined.

Syntax `match route-type {{external {type-1 | type-2} | internal | local }`

Parameters

- `external` — Match only on external OSPF routes. Enter the keyword then one of the following:

- `type-1` — Match only on OSPF Type 1 routes.
- `type-2` — Match only on OSPF Type 2 routes.
-
- `internal` — Match only on routes generated within OSPF areas.
- `local` — Match only on routes generated locally.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The `no` version of this command deletes the match.

Example

```
OS10(config)# route-map bgp
OS10(config-route-map)# match route-type external type-1
```

Supported Releases 10.3.0E or later

match tag

Configures a filter to redistribute only routes that match a specific tag value.

Syntax `match tag tag-value`

Parameters `tag-value` — Enter the tag value to match with the tag number, from 0 to 4294967295.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The `no` version of this command deletes the match.

Example

```
OS10(config-route-map)# match tag 656442
```

Supported Releases 10.2.0E or later

route-map

Enables a route-map statement and configures its action and sequence number.

Syntax `route-map map-name [permit | deny | sequence-number]`

- Parameters**
- `map-name` — Enter the name of the route-map. A maximum of 140 characters.
 - `sequence-number` — (Optional) Enter the number to identify the route-map for editing and sequencing number from 1 to 65535. The default is 10.
 - `permit` — (Optional) Set the route-map default as permit.
 - `deny` — (Optional) Set the route default as deny.

Default Not configured

Command Mode CONFIGURATION

Usage Information Use caution when you delete route-maps — if you do not enter a sequence number, all route-maps with the same map-name are deleted. The `no` version of this command removes a route-map.

Example

```
OS10(config)# route-map route1 permit 100
OS10(config-route-map)#
```

Supported Releases 10.2.0E or later

set comm-list add

Add communities in the specified list to the COMMUNITY attribute in a matching inbound or outbound BGP route.

Syntax	<code>set comm-list {community-list-name} add</code>
Parameters	<i>community-list-name</i> — Enter the name of an established community list (up to 140 characters).
Defaults	None
Command Mode	ROUTE-MAP
Usage Information	In a route map, use this <code>set</code> command to add a list of communities that pass a permit statement to the COMMUNITY attribute of a BGP route sent or received from a BGP peer. Use the <code>set comm-list delete</code> command to delete a community list from a matching route.
Example	<pre>OS10(config)# route-map bgp OS10(conf-route-map)# set comm-list comlist1 add</pre>
Supported Releases	10.4.0E(R1) or later

set comm-list delete

Remove communities in the specified list from the COMMUNITY attribute in a matching inbound or outbound BGP route.

Syntax	<code>set comm-list {community-list-name} delete</code>
Parameters	<i>community-list-name</i> — Enter the name of an established community list. A maximum of 140 characters.
Defaults	None
Command Mode	ROUTE-MAP
Usage Information	The community list you use in the <code>set comm-list delete</code> command must be configured so that each filter contains only one community. For example, the filter <code>deny 100:12</code> is acceptable, but the filter <code>deny 120:13 140:33</code> results in an error. If you configure the <code>set comm-list delete</code> command and the <code>set community</code> command in the same route map sequence, the deletion command (<code>set comm-list delete</code>) processes before the insertion command (<code>set community</code>). To add communities in a community list to the COMMUNITY attribute in a BGP route, use the <code>set comm-list add</code> command.
Example	<pre>OS10(config)# route-map bgp OS10(conf-route-map)# set comm-list comlist1 delete</pre>
Supported Releases	10.3.0E or later

set community

Sets the community attribute in BGP updates.

Syntax	<code>set community {none community-number}</code>
Parameters	<ul style="list-style-type: none"><code>none</code> — Enter to remove the community attribute from routes meeting the route map criteria.<i>community-number</i> — Enter the community number in <code>aa:nn</code> format, where <code>aa</code> is the AS number (2 bytes) and <code>nn</code> is a value specific to that AS.
Default	Not configured
Command Mode	ROUTE-MAP

Usage Information The no version of this command deletes a BGP COMMUNITY attribute assignment.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set community none
```

Supported Releases 10.3.0E or later

set extcomm-list add

Add communities in the specified list to the EXT COMMUNITY attribute in a matching inbound or outbound BGP route.

Syntax `set extcomm-list extcommunity-list-name add`

Parameter *extcommunity-list-name* — Enter the name of an established extcommunity list (up to 140 characters).

Defaults None

Command Mode ROUTE-MAP

Usage Information In a route map, use this set command to add an extended list of communities that pass a permit statement to the EXT COMMUNITY attribute of a BGP route sent or received from a BGP peer. Use the set extcomm-list delete command to delete an extended community list from a matching route.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set extcomm-list TestList add
```

Supported Releases 10.4.0E(R1) or later

set extcomm-list delete

Remove communities in the specified list from the EXT COMMUNITY attribute in a matching inbound or outbound BGP route.

Syntax `set extcomm-list extcommunity-list-name delete`

Parameter *extcommunity-list-name* — Enter the name of an established extcommunity list. A maximum of 140 characters.

Defaults None

Command Mode ROUTE-MAP

Usage Information To add communities in an extcommunity list to the EXT COMMUNITY attribute in a BGP route, use the set extcomm-list add command.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set extcomm-list TestList delete
```

Supported Releases 10.3.0E or later

set extcommunity

Sets the extended community attributes in a route map for BGP updates.

Syntax `set extcommunity rt {asn2:nn | asn4:nnnn | ip-addr:nn}`

Parameters

- `asn2:nn` — Enter an AS number in 2-byte format; for example, 1-65535:1-4294967295.

- `asn4:nnnn` — Enter an AS number in 4-byte format; for example, 1–4294967295:1–65535 or 1–65535.1–65535:1–65535.
- `ip-addr:nn` — Enter an AS number in dotted format, from 1 to 65535.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The `no` version of this command deletes the `set` clause from a route map.

Example

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set extcommunity rt 10.10.10.2:325
```

Supported Releases 10.3.0E or later

set local-preference

Sets the preference value for the AS path.

Syntax `set local-preference value`

Parameters `value` — Enter a number as the LOCAL_PREF attribute value, from 0 to 4294967295.

Default Not configured

Command Mode ROUTE-MAP

Usage Information This command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the `bgp default local-preference` command. The `no` version of this command removes the LOCAL_PREF attribute.

Example

```
OS10(conf-route-map)# set local-preference 200
```

Supported Releases 10.2.0E or later

set metric

Set a metric value for a routing protocol.

Syntax `set metric [+ | -] metric-value`

- Parameters**
- `+` — (Optional) Add a metric value to the redistributed routes.
 - `-` — (Optional) Subtract a metric value from the redistributed routes.
 - `metric-value` — Enter a new metric value, from 0 to 4294967295.

Default Not configured

Command Mode ROUTE-MAP

Usage Information To establish an absolute metric, do not enter a plus or minus sign before the metric value. To establish a relative metric, enter a plus or minus sign immediately preceding the metric value. The value is added to or subtracted from the metric of any routes matching the route map. You cannot use both an absolute metric and a relative metric within the same route map sequence. Setting either metric overrides any previously configured value. The `no` version of this command removes the filter.

Example (Absolute)

```
OS10(conf-route-map)# set metric 10
```

Example (Relative)

```
OS10(conf-route-map)# set metric -25
```

Supported Releases 10.2.0E or later

set metric-type

Set the metric type for the a redistributed routel.

Syntax `set metric-type {type-1 | type-2 | external}`

- Parameters**
- `type-1` — Adds a route to an existing community.
 - `type-2` — Sends a route in the local AS.
 - `external` — Disables advertisement to peers.

Default Not configured

Command Mode ROUTE-MAP

Usage Information

- **BGP**

Affects BGP behavior only in outbound route maps and has no effect on other types of route maps. If the route map contains both a `set metric-type` and a `set metric` clause, the `set metric` clause takes precedence. If you enter the `internal` metric type in a BGP outbound route map, BGP sets the MED of the advertised routes to the IGP cost of the next hop of the advertised route. If the cost of the next hop changes, BGP is not forced to readvertise the route.

- `external` — Reverts to the normal BGP rules for propagating the MED, the default.
- `internal` — Sets the MED of a received route that is being propagated to an external peer equal to the IGP costs of the indirect next hop.

- **OSPF**

- `external` — Sets the cost of the external routes so that it is equal to the sum of all internal costs and the external cost.
- `internal` — Sets the cost of the external routes so that it is equal to the external cost alone, the default.

The `no` version of this command removes the `set` clause from a route map.

Example

```
OS10(conf-route-map)# set metric-type internal
```

Supported Releases 10.2.0E or later

set next-hop

Sets an IPv4 or IPv6 address as the next-hop.

Syntax `set {ip | ipv6} next-hop ip-address`

Parameters `ip-address` — Enter the IPv4 or IPv6 address for the next-hop.

Default Not configured

Command Mode ROUTE-MAP

Usage Information

If you apply a route-map with the `set next-hop` command in ROUTER-BGP mode, it takes precedence over the `next-hop-self` command entered in ROUTER-NEIGHBOR mode. In a route-map configuration, to configure more than one next-hop entry, enter multiple `set {ip | ipv6} next-hop` commands. When you apply a route-map for redistribution or route updates in ROUTER-BGP mode, configure only one next-hop. Configure multiple next-hop entries only in a route-map used for other features. The `no` version of this command deletes the setting.

Example

```
OS10(conf-route-map)# set ip next-hop 10.10.10.2
```

Example (IPv6)

```
OS10(conf-route-map)# set ipv6 next-hop 11AA:22CC::9
```

Supported Releases 10.2.0E or later

set origin

Set the origin of the advertised route.

Syntax `set origin {egp | igp | incomplete}`

Parameters

- `egp` — Enter to add to existing community.
- `igp` — Enter to send inside the local-AS.
- `incomplete` — Enter to not advertise to peers.

Default Not configured

Command Mode ROUTE-MAP

Usage Information The `no` version of this command deletes the `set` clause from a route map.

Example

```
OS10(conf-route-map)# set origin egp
```

Supported Releases 10.2.0E or later

set tag

Sets a tag for redistributed routes.

Syntax `set tag tag-value`

Parameters `tag-value` — Enter a tag number for the route to redistribute, from 0 to 4294967295.

Default Not configured

Command Mode CONFIGURATION

Usage Information The `no` version of this command deletes the `set` clause from a route map.

Example

```
OS10(conf-route-map)# set tag 23
```

Supported Releases 10.2.0E or later

set weight

Set the BGP weight for the routing table.

Syntax `set weight weight`

Parameters `weight` — Enter a number as the weight the route uses to meet the route map specification, from 0 to 65535.

Default Default router-originated is 32768 — all other routes are 0.

Command Mode ROUTE-MAP

Usage Information The `no` version of the command deletes the `set` clause from the route map.

Example

```
OS10(conf-route-map)# set weight 200
```

Supported Releases

10.2.0E or later

show route-map

Displays the current route map configurations.

Syntax

```
show route-map [map-name]
```

Parameters

map-name — (Optional) Specify the name of a configured route map. A maximum of 140 characters.

Defaults

None

Command Mode

EXEC

Usage

None

Information**Example**

```
OS10# show route-map
route-map abc, permit, sequence 10
  Match clauses:
    ip address (access-lists): hello
    as-path abc
    community hello
    metric 2
    origin egp
    route-type external type-1
    tag 10
  Set clauses:
    metric-type type-1
    origin igp
    tag 100
```

Supported Releases

10.3.0E or later

Quality of service

Quality of service (QoS) reserves network resources for highly critical application traffic with precedence over less critical application traffic. QoS enables to prioritize different types of traffic and ensures the required level of quality of service.

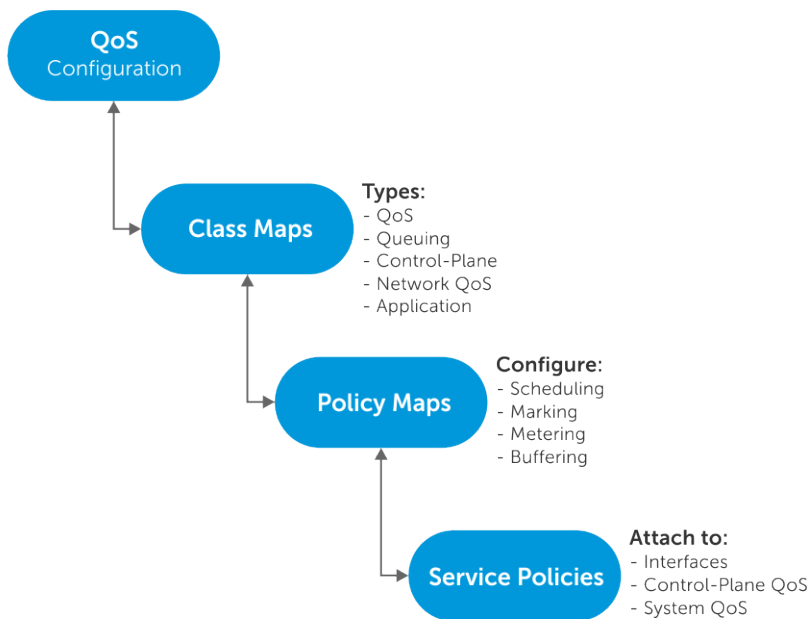
You can control the following parameters of selected traffic flows: Delay, Bandwidth, Jitter, and Drop.

The different QoS features control the above parameters, as traffic traverses a network device from ingress interfaces to egress interfaces.



Configure quality of service

Network traffic is processed based on classification and policies that are created and applied to the traffic.



Configuring QoS is a three-step process:

1. Create class-maps to classify the traffic flows. The following are the different types of class-maps:
 - qos (default)—Classifies the ingress data traffic.
 - queuing —Classifies the egress queues.
 - control-plane—Classifies the control-plane traffic.
 - network-qos—Classifies the set of traffic-class IDs for ingress buffer configurations.
 - application —Classifies the application type traffic. The reserved policy-map **policy-iscsi** defines the actions to be performed for **class-iscsi** traffic.
2. Create policy-maps to define the policies for the classified traffic flows. The following are the different types of policy-maps:
 - qos (default)—Defines the following actions on the traffic classified based on **qos** class-map.
 - Policing
 - Marking with a traffic class ID
 - Modifying packet fields such as CoS and DSCP
 - Enabling trust based classification
 - queuing —Defines the following actions on the egress queues classified based on **queuing** class-map.
 - Shaping
 - Bandwidth assignment for queues
 - Strict priority assignment for queues
 - Buffer configuration for queues
 - WRED configuration on queues
 - control-plane—Defines the policing of control queues for rate-limiting the **control-plane** traffic on CPU queues.
 - network-qos—Defines the Ingress buffer configuration for selected traffic-classes matched based on **network-qos** class-map.
 - application —Defines the following actions for the **application** classified traffic.
 - Modify packet fields like CoS and DSCP.
 - Mark with a traffic class ID.
3. Apply the policy-maps to interface (port), system (all interfaces), or control-plane traffic as follows:
 - Control-plane polices must be applied on control-plane mode.
 - The qos and network-qos policies must be applied in the input direction on physical interfaces or on system-qos mode.
 - Queuing policies must be applied in the output direction on physical interfaces or on system-qos mode.
 - Application type policy-map must be applied on system-qos mode.

When a policy is applied on system, the policy is effective on all the ports in the system. However, interface level policy gets precedence over system level policy.

Ingress traffic classification

Ingress traffic can be either data traffic or control traffic.

By default, OS10 does not classify data traffic and assigns the default traffic class ID 0 to all data traffic.

OS10 implicitly classifies all control traffic like STP, OSPF, ICMP, and so on, and forwards the traffic to control plane applications.

Data traffic classification

You can classify the data traffic based on ACL or trust.

ACL based classification consumes significant amount of network processor resources. Trust based classification allows to classify traffic in a pre-defined way without using any network processor resources.

Trust based classification

OS10 supports classification based on the 802.1p CoS field (L2) or DSCP field (L3).

802.1p CoS trust map:

Trust the 802.1p CoS field to mark with a traffic-class ID and color for the CoS flow.

Table 34. Default 802.1p CoS trust map

CoS	Traffic class ID	Color
0	1	G
1	0	G
2	2	G
3	3	G
4	4	G
5	5	G
6	6	G
7	7	G

User-defined 802.1p CoS trust map

You can override the default mapping by creating dot1p trust map. All the unspecified dot1p entries are mapped to the default traffic class ID 0.

Configure user-defined 802.1p CoS trust map

1. Create a dot1p trust map.

```
OS10(config)# trust dot1p-map dot1p-trust-map
OS10(config-tmap-dot1p-map) #
```

2. Define the set of dot1p values mapped to traffic-class (qos-group) ID.

```
OS10(config-tmap-dot1p-map) # qos-group 3 dot1p 0-4
OS10(config-tmap-dot1p-map) # qos-group 5 dot1p 5-7
```

3. Verify the map entries.

```
OS10# show qos maps type trust-map-dot1p dot1p-trust-map

DOT1P Priority to Traffic-Class Map : dot1p-trust-map

Traffic-Class      DOT1P Priority
-----
```

3	0-4
5	5-7

4. Apply the map on a specific interface or on system-qos (global) level.

- Interface level

```
OS10(config-if-eth1/1/1)# trust-map dot1p dot1p-trust-map
```

i **NOTE:** In the interface level, the no version of the command returns the configuration to system-qos level. If there is no configuration available at the system-qos level, then the configuration returns to default mapping.

- System-qos level

```
OS10(config-sys-qos)# trust-map dot1p dot1p-trust-map
```

Configure default CoS trust map

1. Create a default dot1p trust map.

```
OS10(config)# trust dot1p-map default
OS10(config-tmap-dot1p-map)#
```

2. Apply the map on a specific interface or on system-qos (global) level.

- Interface level

```
OS10(config-if-eth1/1/1)# trust-map dot1p default
```

i **NOTE:** In the interface level, the no version of the command returns the configuration to system-qos level. If there is no configuration available at the system-qos level, then the configuration returns to default mapping.

- System-qos level

```
OS10(config-sys-qos)# trust-map dot1p default
```

DSCP trust map:

Trust the DSCP field to mark with a traffic-class ID and color for the DSCP flow.

Table 35. Default DSCP trust map

DSCP values	TC id	Color
0-3	0	G
4-7	0	Y
8-11	1	G
12-15	1	Y
16-19	2	G
20-23	2	Y
24-27	3	G
28-31	3	Y
32-35	4	G
36-39	4	Y
40-43	5	G

Table 35. Default DSCP trust map (continued)

DSCP values	TC id	Color
44-47	5	Y
48-51	6	G
52-55	6	Y
56-59	7	G
60-62	7	Y
63	7	R

User-defined DSCP trust map

You can override the default mapping by creating a user defined DSCP trust map. All the unspecified DSCP entries are mapped to the default traffic class ID 0.

Configure user-defined DSCP trust map

1. Create a DSCP trust map.

```
OS10(config)# trust dscp-map dscp-trust-map
OS10(config-tmap-dscp-map)#
```

2. Define the set of dscp values mapped to traffic-class(qos-group) ID

```
OS10(config-tmap-dscp-map)# qos-group 3 dscp 0-15
OS10(config-tmap-dscp-map)# qos-group 5 dscp 16-30
```

3. Verify the map entries.

```
OS10# show qos maps type trust-map-dscp dscp-trust-map
DSCP Priority to Traffic-Class Map : dscp-trust-map
Traffic-Class      DSCP Priority
-----
3                   0-15
5                   16-30
```

4. Apply the map on a specific interface or on system-qos (global) level.

- Interface level

```
OS10(conf-if-eth1/1/1)# trust-map dscp dscp-trust-map
```

- System-qos level

```
OS10(config-sys-qos)# trust-map dscp dscp-trust-map
```

Configure default DSCP trust map

1. Create a default DSCP trust map.

```
OS10(config)# trust dscp-map default
OS10(config-tmap-dscp-map)#
```

2. Apply the map on a specific interface or on system-qos (global) level.

- Interface level

```
OS10(conf-if-eth1/1/1)# trust-map dscp default
```

- System-qos level

```
OS10(config-sys-qos)# trust-map dscp default
```

ACL based classification

Classify the ingress traffic by matching the packet fields using ACL entries.

You can classify the traffic flows based on QoS specific fields or generic fields, using IP or MAC ACLs. Create class-map template to match the fields.

OS10 allows matching *any* of the fields or *all* the fields based on the match type configured in the class-map.

Use access-group match filter to match MAC or IP ACLs. You can configure a maximum of 4 access-group filters in a class-map:

- 802.1p CoS
- VLAN ID (802.1.Q)
- DSCP + ECN
- IP precedence

OS10 supports configuring a range of or comma separated values of match filters. When you apply the same match filter with new values, the system overwrites the previous values with the new values.

Configure ACL based classification

1. Create a class-map of type *qos*.

```
OS10(config)# class-map cmap
```

2. Define the fields to be matched, based on:

- 802.1p CoS

```
OS10(config-cmap-qos)# match cos 0,4-7
```

- all the 802.1p CoS values excluding a few

```
OS10(config-cmap-qos)# match not cos 3,4
```

- VLAN ID (range of or comma separated VLAN match is not supported)

```
OS10(config-cmap-qos)# match vlan 100
```

- IP DSCP

```
OS10(config-cmap-qos)# match ip dscp 3,5,20-30
```

- IP DSCP + ECN

```
OS10(config-cmap-qos)# match ip dscp 3,5,20-30 ecn 2
```

- IP precedence

```
OS10(config-cmap-qos)# match ip precedence 2
```

- IPv6 DSCP

```
OS10(config-cmap-qos)# match ipv6 dscp 3,5,20-30
```

- IPv6 DSCP + ECN

```
OS10(config-cmap-qos)# match ipv6 dscp 3,5,20-30 ecn 2
```

- IPv6 precedence

```
OS10(config-cmap-qos)# match ipv6 precedence 2
```

- any IP (IPv4 or IPv6) precedence

```
OS10(config-cmap-qos)# match ip-any precedence 2
```

- Pre-defined IP access-list

```
OS10(config-cmap-qos)# match ip access-group name ip-acl-1
```

- Pre-defined IPv6 access-list

```
OS10(config-cmap-qos)#match ipv6 access-group name ACLv6
```

- Pre-defined MAC access-list

```
OS10(config-cmap-qos)# match mac access-group name mac-acl-1
```

3. Create a qos type policy-map to refer the classes.

```
OS10(config)# policy-map cos-policy
```

4. Refer the class-maps in the policy-map and define the required action for the flows.

```
OS10(config-pmap-qos)# class cmap
OS10(config-pmap-c-qos)# ?

OS10(config-pmap-qos)# class cmap
OS10(config-pmap-c-qos)#
end      Exit to the exec Mode
exit    Exit from current mode
no      Negate a command or set its defaults
police  Rate police input traffic
set     Mark input traffic
show    show configuration
trust   Specify dynamic classification to trust[dscp/dot1p]
```

ACL based classification with trust

This section describes how to configure ACL based classification when trust-based classification is configured.

You can configure ACL based classification when trust-based classification is configured.

1. Create a user defined dscp or dot1p trust-map.

```
OS10(config)# trust dscp-map userdef-dscp
OS10(config-tmap-dscp-map)# qos-group 3 dscp 15
OS10(config-tmap-dscp-map)# qos-group 5 dscp 30
```

2. Apply user-defined trust map to an interface or in system QoS.

```
OS10(conf-if-eth1/1/1)# trust-map dscp userdef-dscp
or
OS10(config)# system qos
OS10(config-sys-qos)# trust-map dscp userdef-dscp
```

3. Create a class-map and attach it to a policy where fallback trust is configured.

```
OS10(config)# class-map c1
OS10(config-cmap-qos)# match cos 1
OS10(config-cmap-qos)# exit

OS10(config)# policy-map p1
OS10(config-pmap-qos)# class c1
OS10(config-pmap-c-qos)# set qos-group 1
```

4. Attach the policy map to an interface or in system QoS mode.

```
OS10(config)# interface ethernet 1/1/1
```



```

OS10(conf-if-eth1/1/1)# service-policy input type qos p1
or
OS10(config)# system qos
OS10(config-sys-qos)# service-policy input type qos p1

```

Control-plane policing

Control-plane policing (CoPP) increases security on the system by protecting the route processor from unnecessary traffic and giving priority to important control plane and management traffic. CoPP uses a dedicated control plane configuration through the QoS CLIs to set rate-limiting capabilities for control plane packets.

If the rate of control packets towards the CPU is higher than the packet rate that the CPU can handle, CoPP provides a method to selectively drop some of the control traffic so that the CPU can process high-priority control traffic. You can use CoPP to rate-limit traffic through each CPU port queue of the network processor (NPU).

CoPP applies policy actions on all control-plane traffic. The control-plane class map does not use any match criteria. To enforce rate-limiting or rate policing on control-plane traffic, create policy maps. You can use the `control-plane` command to attach the CoPP service policies directly to the control-plane.

The default rate limits apply to 12 CPU queues and the protocols mapped to each CPU queue. The control packet type to CPU ports control queue assignment is fixed. The only way you can limit the traffic towards the CPU is choose a low priority queue, and apply rate-limits on that queue to find a high rate of control traffic flowing through that queue.

By default CoPP traffic towards the CPU is classified into different queues as shown in the following table.

Table 36. CoPP queues

Queue	Protocol
0	IPv6
1	
2	IGMP
3	VLT, NDS
4	ICMPv6, ICMPv4
5	ARP Requet, ICMPV6-RS-NS, ISCSI snooping, ISCSI-COS
6	ICMPv6-RA-NA, SSH, TELNET,TACACS, NTP,FTP
7	RSTP,PVST, MSTP,LACP
8	Dot1X,LLDP, FCOE-FPORT
9	BGPv4, OSPFv6
10	DHCPv6, DHCPv4, VRRP
11	OSPF Hello, OpenFlow

See [show control-plane info](#) for information on the current protocol to queue mapping and the rate-limit configured per queue.

Configure control-plane policing

Rate-limiting the protocol CPU queues requires configuring control-plane type QoS policies.

- Create QoS policies (class maps and policy maps) for the desired CPU-bound queue.
- Associate the QoS policy with a particular rate-limit.

- Assign the QoS service policy to control plane queues.

By default, the peak information rate (`pir`) and committed information rate (`cir`) values are in packets per second (pps) for control plane. CoPP for CPU queues converts the input rate from kilobits per second (kbps) to packets per second (pps), assuming 64 bytes is the average packet size, and applies that rate to the corresponding queue – 1 kbps is roughly equivalent to 2 pps.

1. Create a class-map of type `control-plane` and configure a name for the class-map in CONFIGURATION mode.

```
class-map type control-plane class-map-name
```

2. Return to CONFIGURATION mode.

```
exit
```

3. Create an input policy-map to assign the QoS policy to the desired service queues in CONFIGURATION mode.

```
policy-map type control-plane policy-map-name
```

4. Associate a policy-map with a class-map in POLICY-MAP mode.

```
class class-name
```

5. Configure marking for a specific queue number in POLICY-MAP-CLASS-MAP mode (0 to 11).

```
set qos-group queue-number
```

6. Configure rate policing on incoming traffic in POLICY-MAP-CLASS-MAP mode.

```
police {cir committed-rate | pir peak-rate}
```

- `cir committed-rate`—Enter a committed rate value in pps (0 to 4000000).
- `pir peak rate` — Enter a peak-rate value in pps (0 to 40000000).

Create QoS policy for CoPP

```
OS10(config)# class-map type control-plane copp
OS10(conf-cmap-control-plane)# exit
OS10(config)# policy-map type control-plane copp1
OS10(conf-pmap-control-plane)# class copp
OS10(conf-pmap-c)# set qos-group 2
OS10(conf-pmap-c)# police cir 100 pir 100
```

View policy-map

```
OS10(conf-pmap-c)# do show policy-map
Service-policy(control-plane) input: copp1
Class-map (control-plane): copp
  set qos-group 2
  police cir 100 bc 100 pir 100 be 100
```

Assign service-policy

Rate controlling control traffic towards CPU requires configuring **control-plane** type policy. To enable CoPP, you need to apply the defined policy-map to CONTROL-PLANE mode.

1. Enter CONTROL-PLANE mode from CONFIGURATION mode.

```
control-plane
```

2. Define a service-policy of type `input` and configure a name for the service policy in CONTROL-PLANE mode.

```
service-policy input service-policy-name
```

Assign control-plane service-policy

```
OS10(config)# control-plane
OS10(conf-control-plane)# service-policy input copp1
```

View control-plane service-policy

```
OS10(conf-control-plane)# do show qos control-plane
Service-policy (input): copp1
```

View configuration

Use the show commands to display the protocol traffic assigned to each control-plane queue and the current rate-limit applied to each queue. You can also use the show command output to verify the CoPP configuration.

View CoPP configuration

```
OS10# show qos control-plane
Service-policy (input): pmap1
```

View CMAP1 configuration

```
OS10# show class-map type control-plane cmap1
Class-map (control-plane): cmap1 (match-any)
```

View CoPP service-policy

```
OS10# show policy-map type control-plane
Service-policy(control-plane) input: pmap1
Class-map (control-plane): cmap1
  set qos-group 6
  police cir 200 bc 100 pir 200 be 100
```

View CoPP information

```
OS10# show control-plane info
Queue  Rate Limit(in pps)  Protocols
0      600
1      1000
2      300
3      1300
4      2000              VLT NDS
5      400              ARP_REQ IPV6_ICMP_REQ
6      400              ARP_RESP IPV6_ICMP IPV6_ICMP_RESP IPV4_ICMP SSH TELNET TACACS
NTP FTP
7      400              RSTP PVST MSTP LACP
8      600              DOT1X LLDP
9      600              IPV6_OSPF IPV4_BGP IPV4_OSPF
10     600              IPV6_DHCP IPV4_DHCP SERVICEABILITY
11     300              OPEN_FLOW
```

View CoPP statistics

```
OS10# show control-plane statistics
Queue  Packets Bytes      Dropped Packets Dropped Bytes
0      0      0      0      0
1      0      0      0      0
2      0      0      0      0
3      0      0      0      0
4      0      0      0      0
5      2      172    0      0
6      0      0      0      0
7      32048  2180484  0      0
8      14140  2569184  0      0
9      0      0      0      0
10     0      0      0      0
11     0      0      0      0
```

Egress traffic classification

Egress traffic is classified into different queues based on the traffic-class ID marked on the traffic flow.

You can set the traffic class ID for a flow by enabling trust or by classifying ingress traffic and mark it with a traffic class ID using a policy map. By default, the value of traffic class ID for all the traffic is 0.

The order of precedence for qos-map is:

1. Interface level map
2. System-qos level map
3. Default map

Table 37. Default mapping of traffic class ID to queue

Traffic class ID	Queue ID
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

User-defined QoS map

You can override the default mapping by creating QoS map.

Configure user-defined QoS map

1. Create a QoS map

```
OS10(config)# qos-map traffic-class tc-q-map
```

2. Define the set of traffic class values mapped to a queue

```
OS10(config-qos-map)# queue 3 qos-group 0-3
```

3. Verify the map entries.

```
OS10# show qos maps type tc-queue
Traffic-Class to Queue Map: tc-q-map
Queue          Traffic-Class
-----
3              0-3
```

4. Apply the map on a specific interface or on system-qos (global) level.

- Interface level

```
OS10(conf-if-eth1/1/1)# qos-map traffic-class tc-q-map
```

- System-qos level

```
OS10(config-sys-qos)# qos-map traffic-class tc-q-map
```

Choose all traffic classified for a queue

1. Create a class-map of type queuing to match queue 5

```
OS10(config)# class-map type queuing q5
```

2. Define the queue to match

```
OS10(config-cmap-queuing)# match queue 5
```

Policing traffic

Use policing to limit the rate of ingress traffic flow. The flow can be all the ingress traffic on a port or a particular flow assigned with a traffic class ID.

In addition, you can use policing to color the traffic.

- When traffic arrives at a rate less than the committed rate, the color is green.
- When traffic propagates at an average rate greater than or equal to the committed rate and less than peak-rate, the color is yellow.
- When the traffic rate is above the configured peak-rate, the traffic is dropped to guarantee a bandwidth limit for an ingress traffic flow.

Peak rate is the maximum rate for traffic arriving or leaving an interface under normal traffic conditions. Peak burst size indicates the maximum size of unused peak bandwidth that is aggregated. This aggregated bandwidth enables brief durations of burst traffic that exceeds the peak rate.

Configure Interface rate policing

1. Create a QoS type empty class-map to match all the traffic

```
OS10(config)# class-map cmap-all-traffic
```

2. Create a QoS type policy-map to define a policer

```
OS10(config)# policy-map interface-policer
OS10(config-pmap-qos)# class cmap-all-traffic
OS10(config-pmap-c-qos)# police cir 4000 pir 6000
```

Configure flow rate policing

1. Create a QoS type class-map to match the traffic flow

```
OS10(config)# class-map cmap-cos3
OS10(config-cmap-qos)# match cos 3
```

2. Create a QoS type policy-map to define a policer and assign a traffic class ID for the CoS flow

```
OS10(config)# policy-map flow-policer
OS10(config-pmap-qos)# class cmap-cos3
OS10(config-pmap-c-qos)# set qos-group 3
OS10(config-pmap-c-qos)# police cir 4000 pir 6000
```

Mark Traffic

You can select a flow and mark with a traffic class ID. The traffic flow is identified by the traffic class ID when the traffic reaches egress for queue scheduling.

Mark traffic

1. Create a QoS type class-map to match the traffic flow

```
OS10(config)# class-map cmap-cos3
OS10(config-cmap-qos)# match cos 3
```

2. Create a QoS type policy-map to mark with a traffic class ID and assign it for the CoS flow.

```
OS10(config)# policy-map cos3-TC3
OS10(config-pmap-qos)# class cmap-cos3
OS10(config-pmap-c-qos)# set qos-group 3
```

Color traffic

You can select a traffic flow and mark it with a color.

You can color the traffic flow based on:

- Metering. See [Policing traffic](#) on page 637.
- Default trust. See [Trust based classification](#) on page 628.
- DSCP, ECN capable traffic (ECT), or non-ECT.

Color traffic based on DSCP, ECT, or non-ECT

1. Create a QoS type class-map to match the traffic flow.

```
OS10(config)# class-map cmap-dscp-3-ect
OS10(config-cmap-qos)# match ip dscp 3 ecn 1
```

2. Create a QoS type policy-map to color the traffic flow.

```
OS10(config)# policy-map ect-color
OS10(config-pmap-qos)# class cmap-dscp-3-ect
OS10(config-pmap-c-qos)# set qos-group 3
OS10(config-pmap-c-qos)# set color yellow
```

Modify packet fields

You can modify the value of CoS or DSCP fields.

1. Create a QoS type class-map to match a traffic flow

```
OS10(config)# class-map cmap-dscp-3
OS10(config-cmap-qos)# match ip dscp 3
```

2. Modify the policy-map to update the DSCP field.

```
OS10(config)# policy-map modify-dscp
OS10(config-pmap-qos)# class cmap-dscp-3
OS10(config-pmap-c-qos)# set qos-group 3
OS10(config-pmap-c-qos)# set dscp 10
```

Shaping traffic

You can configure to shape the rate of egress traffic. When you enable rate shaping, the system buffers all traffic exceeding the specified rate till buffer memory is exhausted. The rate shaping mechanism uses all buffers reserved for an interface or queue and then shared buffer memory, till it reaches the configured threshold.

Configure traffic shaping

1. Enter the policy-map type as `queuing` and configure a policy-map name in CONFIGURATION mode.

```
policy-map type queuing policy-map-name
```

2. Enter a class name to apply to the shape rate in POLICY-MAP-QUEUEING mode—up to 32 characters.

```
class class-name
```

- (Optional) If you need rate shaping on a specific queue, match the corresponding qos-group in the class-map. If you do not configure the `match qos-group` command, rate shaping applies to all queues.

```
match qos-group queue-number
```

- Enter a minimum and maximum shape rate value in POLICY-MAP-QUEUEING-CLASS mode.

```
shape {min {kbps | mbps}min-value} {max {kbps | mbps}max-value}
```

- 0 to 40000000—kilobits per second kilobits per second—kbps
- 0 to 40000 — megabits per second—mbps

Bandwidth allocation

You can allocate relative bandwidth to limit large flows and prioritize smaller flows. Allocate the relative amount of bandwidth to nonpriority queues when priorities queues are consuming maximum link bandwidth.

Each egress queue of an interface can be scheduled as per Weighted Deficit Round Robin (WDRR) or by strict-priority (SP), which are mutually exclusive. If the `bandwidth percent` command is present, you cannot configure the `priority` command as it is used to assign bandwidth to a queue.

In S5148F-ON, bandwidth weight is equally applied to UC and MC.

- Create a class-map of type `queuing` and configure a name for the class-map in CONFIGURATION mode.

```
class-map type queuing class-map-name
```

- Apply the match criteria for the QoS group in CLASS-MAP mode.

```
qos-group queue-number
```

- Return to the CONFIGURATION mode.

```
exit
```

- Create a policy-map of type `queuing` and configure a policy-map name in CONFIGURATION mode.

```
policy-map type queuing policy-map-name
```

- Configure a queuing class in POLICY-MAP mode.

```
class class-name
```

- Assign a bandwidth percent (1 to 100) to nonpriority queues in POLICY-MAP-CLASS-MAP mode.

```
bandwidth percent value
```

Configure bandwidth allocation

```
OS10(config)# class-map type queuing solar
OS10(conf-cmap-queuing)# match qos-group 5
OS10(conf-cmap-queuing)# exit
OS10(config)# policy-map lunar
OS10(config)# policy-map type queuing lunar
OS10(conf-pmap-queuing)# class solar
OS10(conf-pmap-c-que)# bandwidth percent 80
```

View class-map

```
OS10(conf-cmap-queuing)# do show class-map
Class-map (queuing): solar (match-any)
Match: qos-group 5
```

View policy-map

```
OS10(conf-pmap-c-que)# do show policy-map
Service-policy (queuing) output: solar
```

```
Class-map (queuing): lunar
  bandwidth percent 80
```

Strict priority queuing

OS10 uses queues for egress QoS policy-types. You can enable priorities to dequeue all packets from the assigned queue before servicing any other queues. When more than one queue is assigned strict priority, the highest number queue receives the highest priority. You can configure strict priority to any number of queues. By default, all queues schedule traffic per WDRR.

You can use the `priority` command to assign the priority to a single unicast queue—this configuration supersedes the `bandwidth percent` configuration. A queue with priority enabled can starve other queues for the same egress interface.

Consider the following when enabling priority queuing in S5148F-ON:

- In a port, one H2 node and three H1 nodes are supported. The H1 node holds 8 unicast queues for data traffic, 8 unicast queues for control traffic, and 8 multicast queues for data traffic.
- The H1 nodes mapped to data traffic are scheduled with DWRR and weight of 50 each. The H1 node mapped to control traffic is scheduled with strict priority.
- The weights corresponding to each traffic class are applied at queue levels for both unicast and multicast queues.
- The bandwidth distribution might go to a minimum of 50, based on the traffic flow in a port. This is determined by the weight of a particular traffic class and traffic type.
- The bandwidth sharing based on ETS happens only between same type of queues.
- You can enable strict priority queuing only for the same type of traffic.

Create class-map

1. Create a class-map, and configure a name for the class-map in CONFIGURATION mode.

```
class-map type queuing class-map-name
```

2. Configure a match criteria in CLASS-MAP mode.

```
match queue queue-id
```

Define a policy-map

1. Define a policy-map, and create a policy-map name CONFIGURATION mode.

```
policy-map type queuing policy-map-name
```

2. Create a QoS class and configure a name for the policy-map in POLICY-MAP mode.

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

3. Set the scheduler as the strict priority in POLICY-MAP-CLASS-MAP mode.

```
priority
```

Apply policy-map

1. You can now apply the policy-map to the interface (INTERFACE mode) or all interfaces—SYSTEM-QOS mode.

```
system qos
```

OR

```
interface ethernet node/slot/port[:subport]
```

2. Enter the output service-policy in SYSTEM-QOS mode or INTERFACE mode.

```
service-policy {output} type {queuing} policy-map-name
```

Enable strict priority on class-map

```
OS10(config)# class-map type queuing magnum
OS10(conf-cmap-queuing)# match queue 7
OS10(conf-cmap-queuing)# exit
```



```
OS10(config)# policy-map type queuing solar
OS10(conf-pmap-queuing)# class magnum
OS10(conf-pmap-c-que)# priority
OS10(conf-pmap-c-que)# exit
OS10(conf-pmap-queuing)# exit
OS10(config)# system qos
OS10(conf-sys-qos)# service-policy output solar
```

View QoS system

```
OS10(conf-sys-qos)# do show qos system
Service-policy (output)(queuing): solar
```

Enable strict priority on interface

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# service-policy output type queuing solar
```

View policy-map

```
OS10(conf-if-eth1/1/5)# do show policy-map
Service-policy(queuing) output: solar
Class-map (queuing): magnum
priority
```

Buffer management

OS10 devices distribute the total available buffer resources into two buffer pools at ingress direction and three buffer pools at egress direction of all the physical ports.

All ports in a system are allocated a certain amount of buffers from corresponding pools, based on the configuration state of each priority-group or queue. The remaining buffers in the pool are shared across all similarly configured ports.

The following buffer pools are available:

- Ingress buffer pools:
 - Lossy pool (default)
 - Lossless pool (PFC)
- Egress buffer pools:
 - Lossy pool (default)
 - Lossless pool (PFC)
 - CPU pool (CPU control traffic)

For example, when all ports are allocated reserved buffers from the lossy (default) pool, the remaining buffers in the lossy pool are shared across all ports, except the CPU port.

When you enable priority flow control (PFC) on the ports, all the PFC enabled queues and priority-groups use the buffers from the lossless pool.

OS10 dedicates a separate buffer pool for CPU traffic. All default reserved buffers for CPU port queues are from the CPU pool, and the remaining buffers are shared across all CPU queues. You can modify the buffer settings of CPU queues.

OS10 allows configuration of buffers per priority-group and queue for each port.

The buffer usage accounting happens for ingress packets on ingress pools and egress packets on egress pool. You can configure ingress packets buffer accounting per priority-group and egress packet buffer accounting per queue level.

Configure ingress buffer

Default settings

In the default settings for ingress buffers, all traffic classes are mapped to the default priority group and the buffers are reserved per default priority group ID 7. All buffers are part of the default pool and all ports share buffers from the default pool.

The reserved buffer size is 9360 bytes for the speed of 10G, 25G, 40G, 50G, and 100G. The supported speed varies for different platforms.

The following table lists the maximum buffer size for different platforms.

Table 38. Maximum buffer size

Platforms	Max buffer size
S4000	12 MB
S6010-ON, S4048-ON	16 MB
S41xx	12 MB
Z9100-ON	16 MB

Default settings for Link-level flow control (LLFC)

The following table lists the LLFC buffer settings for the default priority group 7.

Table 39. Default setting for LLFC

Speed	10G	25G	40G	50G	100G
Default reserved buffer	45KB	45KB	111KB	111KB	111KB
Default Xoff threshold	36KB	36KB	75KB	75KB	75KB
Default Xon threshold	9KB	9KB	36KB	36KB	36KB

Default settings for Priority flow control (PFC)

The following table lists the PFC buffer settings per PFC priority group.

Table 40. Default settings for PFC

Speed	10G	25G	40G	50G	100G
Default reserved buffer for S4000, S4048-ON, S6010-ON	9KB	NA	9KB	NA	NA
Default reserved buffer for S41xx, Z9100-ON	9KB	9KB	18KB	18KB	36KB
Default Xoff threshold	36KB	45KB	75KB	91KB	142KB
Default Xon threshold	9KB	9KB	9KB	9KB	9KB
Default dynamic share buffer threshold(alpha value)	9KB	9KB	9KB	9KB	9KB

NOTE: The supported speed varies for different platforms. After the reserved buffers are utilized, each PFC starts consuming shared buffers from the lossless pool with the threshold determined by the alpha value.

Configure priority group buffer settings

You can override the default priority group settings when LLFC or PFC is enabled.

1. Create network-qos type class-map to match the traffic classes. For LLFC match all the traffic classes(0-7) and for PFC, match the required traffic class.

```
OS10(config)# class-map type network-qos tc
OS10 (config-cmap-nqos)# match qos-group 0-7
```

2. Create network-qos type policy-map to define the actions for traffic classes, like buffer configuration and thresholds.

```
OS10(config)# policy-map type network-qos buffer
OS10(config-pmap-network-qos)# class tc
OS10 (config-pmap-c-nqos)# pause buffer-size 300 pause-threshold 200 resume-threshold
100
OS10 (config-pmap-c-nqos)# queue-limit thresh-mode dynamic 5
```

Configure egress buffer

Default settings

All port queues are allocated with reserved buffers and when the reserved buffers are consumed, each queue starts using the shared buffer from the default pool.

The reserved buffer per queue is 1664 bytes for the speed of 10G, 25G, 40G, 50G, and 100G. The default dynamic shared buffer threshold value is 8.

Configure queue buffer settings

1. Create queuing type class-map to match the queue.

```
OS10(config)# class-map type queuing q1
OS10(config-cmap-queuing)# match queue 1
```

2. Create queuing type policy-map to define the actions for queues, like buffer configuration and thresholds.

```
OS10(config)# policy-map type queuing q-buffer
OS10(config-pmap-queuing)# class q1
OS10(config-pmap-c-que)# queue-limit queue-len 200 thresh-mode dynamic 5
```

Congestion avoidance

Congestion avoidance is a predictive method to anticipate and take necessary action to avoid congestion. The following are the different mechanisms used to avoid congestion:

- **Tail drop**—Packets are buffered at traffic queues. When the buffers are exhausted or reach the configured threshold, excess packets are dropped. By default, OS10 uses tail drop for congestion avoidance.
- **Random early detection (RED)**—In tail drop mechanism, different flows are not considered in buffer utilization. When multiple hosts start retransmission, tail drop causes TCP global re-synchronization. Instead of waiting for the queue to get filled up completely, RED starts dropping excess packets with a certain drop-probability, when the average queue length exceeds the configured minimum threshold. The early drop ensures that only some of TCP sources slow down, which avoids global TCP re-synchronization.
- **Weighted random early detection (WRED)**—This mechanism allows different drop-probabilities and thresholds for each color (red, yellow, green) of traffic. You can configure the drop characteristics for 3 different flows by assigning the colors to the flow. You can assign colors to a particular flow or traffic by various methods, like ingress policing, qos input policy-maps, and so on.
- **Explicit congestion notification (ECN)**—This is an extension of WRED. Instead of dropping the packets when the average queue length crosses the minimum threshold values, ECN marks the Congestion Experienced (CE) bit of ECN field in a packet as ECN-capable traffic (ECT).

Configure congestion avoidance

1. Configure WRED profile in the CONFIGURATION mode.

```
OS10(config)# wred wred_prof_1
```

2. Configure WRED threshold parameters for different colors in the WRED CONFIGURATION mode.

```
OS10(config-wred)# random-detect color yellow minimum-threshold 100 maximum-threshold 300 drop-probability 40
```

3. Configure the exponential weight value for the WRED profile in the WRED CONFIGURATION mode.

```
OS10(config-wred)# random-detect weight 4
```

4. Enable ECN.

```
OS10(config-wred)# random-detect ecn
```

5. Enable WRED/ECN on a queue.

```
OS10(config)# class-map type queuing c1
OS10(config-cmap-queuing)# match queue 2
OS10(config-cmap-queuing)# exit
OS10(config)# policy-map type queuing p1
OS10(config-pmap-queuing)# class c1
OS10(config-pmap-c-que)# random-detect wred_prof_1
```

6. Enable WRED/ECN on a port.

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# random-detect wred_prof_1
```

7. Enable WRED/ECN on a service-pool.

```
OS10(config)# system qos
OS10(config-sys-qos)# random-detect pool 0 wred_prof_1
```

Configure congestion avoidance for the S4200

NOTE: For the S4200 platform, ECN can be enabled globally only. Also, ECN configurations can be applied only at the queue level. You cannot configure ECN at interface and service pool levels. In the S4200, if you try to apply the ECN configure at interface or service pool levels, the configuration is not accepted.

1. Configure WRED profile in the CONFIGURATION mode.

```
OS10(config)# wred wred_prof_1
```

2. Configure WRED threshold parameters for different colors in the WRED CONFIGURATION mode.

```
OS10(config-wred)# random-detect color yellow minimum-threshold 100 maximum-threshold 300 drop-probability 40
```

3. Configure the exponential weight value for the WRED profile in the WRED CONFIGURATION mode.

```
OS10(config-wred)# random-detect weight 4
```

4. Configure the ECN threshold parameters in the WRED CONFIGURATION mode.

```
OS10(config-wred)#random-detect ecn minimum-threshold 100 maximum-threshold 300 drop-probability 40
```

5. Exit the WRED CONFIGURATION mode.

```
OS10(config-wred)#exit
```

6. Enter QOS POLICY-MAP mode and create a queuing policy type.

```
OS10(config)#policy-map type queuing pol-map-1
```

7. Create a QoS class for the queuing policy type.

```
OS10(config-pmap-queuing)#class default
```

8. Assign a WRED profile to the specified queue.

```
OS10(config-pmap-c-que)#random-detect prof1
```

9. Exit class map and policy map modes.

```
OS10(config-pmap-c-que)#exit
OS10(config-pmap-queuing)#exit
```

10. Enter the SYSTEM QOS mode.

```
OS10(config)#configure system-qos
```

11. Enable ECN globally.

```
OS10(config-sys-qos)#random-detect ecn
```

After you enable ECN globally, ECN marks the CE bit of ECN field in a packet as ECT.

In the S4200, you can configure separate thresholds for ECT. If ECN is enabled, ECN capable traffic (ECT) is marked based on the configured ECN threshold and non-ECT is dropped based on the WRED thresholds.

Storm control


Traffic storms created by packet flooding or other reasons may degrade the performance of the network.

The storm control feature allows you to control unknown unicast, multicast, and broadcast traffic on Layer 2 and Layer 3 physical interfaces.

In the storm control unknown unicast configuration, both the unknown unicast and unknown multicast traffic are rate-limited.

OS10 device monitors the current level of traffic rate at fixed intervals, compares the traffic rate with configured levels, and drops excess traffic.

By default, storm control is disabled on all interfaces. You can enable storm control using the `storm-control { broadcast | multicast | unknown-unicast } rate-in-pps` command in the INTERFACE mode.

 **NOTE:** In S5148F-ON, there is a 2% of deviation in the storm control configuration.

Configure storm control

- The following example enables broadcast storm control with a rate of 1000 packets per second (pps) on Ethernet 1/1/1.

```
OS10(conf-if-eth1/1/1)# storm-control broadcast 1000
```

RoCE for faster access and lossless connectivity

Remote Direct Memory Access (RDMA) is a technology that enables memory transfers between two computers in a network without involving the CPU of either computer.

RDMA networks provide high bandwidth and low latency without any appreciable CPU overhead, which is required for improved application performance, storage and data center utilization, and simplified network management. RDMA was traditionally supported only in an InfiniBand environment. Currently, RDMA over Converged Ethernet (RoCE) is also implemented in data centers that use Ethernet or a mixed-protocol environment.

OS10 devices support RoCE v1 and RoCE v2 protocols.

- RoCE v1 – An Ethernet layer protocol that allows for communication between two hosts that are in the same Ethernet broadcast domain.
- RoCE v2 – An Internet layer protocol that allows RoCE v2 packets to be routed and hence called Routable RoCE (RRoCE).

To enable RRoCE, configure the QoS service policy on the switch, and in the ingress and egress directions on all the interfaces. See [Configure RoCE on the switch](#) for more information about this configuration.

Configure RoCE on the switch

The following example describes the steps that you need to perform to configure RoCE on the switch. This configuration example uses priority 3 for RoCE.

1. Enter in to the CONFIGURATION mode.

```
OS10# configure terminal
OS10 (config)#
```

2. Enable the Data Center Bridging Exchange protocol (DCBX).

```
OS10 (config)# dcbx enable
```

3. Create a VLAN. In this example, we use VLAN 55 to switch the RoCE traffic. You can configure any value from 1 to 4093.

```
OS10 (config)# interface vlan 55
```

4. Create a network-qos type class-map for priority flow control (PFC).

```
OS10 (config)# class-map type network-qos pfcdot1p3
OS10 (config)# match qos-group 3
```

5. Create queuing-type class-maps for enhanced transmission selection (ETS).

```
OS10 (config)# class-map type queuing Q0
OS10 (config)# match queue 0
OS10 (config)# class-map type queuing Q3
OS10 (config)# match queue 3
```

6. Create a QoS map for ETS.

```
OS10 (config)# qos-map traffic-class 2Q
OS10 (config)# queue 0 qos-group 0-2, 4-7
OS10 (config)# queue 3 qos-group 3
```

7. Create a policy-map for PFC.

```
OS10 (config)# policy-map type network-qos pfcdot1p3
OS10 (config)# class pfcdoclp3
OS10 (config)# pause
```

8. Create an egress policy-map.

```
OS10 (config)# policy-map type queuing 2Q
OS10 (config)# class Q0 bandwidth percent 30
OS10 (config)# class Q3 bandwidth percent 70
```

9. Apply the dot1p trust globally or at the interface level. In this example, the dot1p trust is applied globally.

```
OS10 (config)# system qos
OS10 (config)# trust-map dot1p default
```

10. Perform the following configurations on all switch interfaces where you want to support RoCE.

- a. Enter in to the INTERFACE mode and enter the `no shutdown` command.

```
OS10# configure terminal
OS10 (config)# interface ethernet 1/1/1
OS10 (conf-if-eth1/1/1)# no shutdown
```

- b. Change the switch port mode to trunk mode.

```
OS10 (conf-if-eth1/1/1)# switchport mode trunk
```

- c. Specify the allowed VLANs on the trunk port.

```
OS10 (conf-if-eth1/1/1)# switchport trunk allowed vlan 55
```

- d. Apply the network-qos type policy-map to the interface.

```
OS10 (conf-if-eth1/1/1)# service-policy input type network-qos pfcdot1p3
```

- e. Apply the queuing policy to egress traffic on the interface.

```
OS10 (conf-if-eth1/1/1)# service-policy output type queuing 2Q
```

- f. Enable enhanced transmission selection (ETS) on the interface.

```
OS10 (conf-if-eth1/1/1)# ets mode on
```

- g. Apply the qos-map for ETS configurations on the interface.

```
OS10 (conf-if-eth1/1/1)# qos-map traffic-class 2Q
```

- h. Enable PFC on the interface.

```
OS10 (conf-if-eth1/1/1)# priority-flow-control mode on
```

QoS commands

bandwidth

Assigns a percentage of weight to the queue.

Syntax	<code>bandwidth percent value</code>
Parameters	<code>percent value</code> — Enter the percentage assignment of bandwidth to the queue (1 to 100).
Default	Not configured
Command Mode	POLICY-MAP QUEUE
Usage Information	If you configure this command, you cannot use the <code>priority</code> command for the class.
Example	<pre>OS10(conf-pmap-que)# bandwidth percent 70</pre>
Supported Releases	10.2.0E or later

class

Creates a QoS class for a type of policy-map.

Syntax	<code>class class-name</code>
Parameters	<code>class-name</code> — Enter a name for the class-map (up to 32 characters).
Default	Not configured
Command Mode	POLICY-MAP-QUEUEING POLICY-MAP-QOS POLICY-MAP-NQOS POLICY-MAP-CP POLICY-MAP-APPLICATION
Usage Information	If you define a class-map under a policy-map, the type (<code>qos</code> , <code>queuing</code> , or <code>control-plane</code>) is the same as the policy-map. You must create this map in advance. The only exception to this rule is when the policy-map type is <code>trust</code> , where the class type must be <code>qos</code> .
Example	<pre>OS10(conf-pmap-qos)# class c1</pre>
Supported Releases	10.2.0E or later

class-map

Creates a QoS class-map which filters traffic to match packets to the corresponding policy created for your network.

Syntax	<code>class-map [type {qos queuing control-plane}] [{match-any match-all}] class-map-name</code>
Parameters	<ul style="list-style-type: none"><code>type</code> — Enter a class-map type.<code>qos</code> — Enter a <code>qos</code> type class-map.<code>queuing</code> — Enter a <code>queuing</code> type class-map.<code>control-plane</code> — Enter a <code>control-plane</code> type class-map.

- `match-all` — Determines how packets are evaluated when multiple match criteria exist. Enter the keyword to determine that all packets must meet the match criteria to be assigned to a class.
- `match-any` — Determines how packets are evaluated when multiple match criteria exist. Enter the keyword to determine that packets must meet at least one of the match criteria to be assigned to a class.
- `class-map-name` — Enter a class-map name (up to 32 characters).

Defaults

- `qos` — class-map type
- `match-any` — class-map filter

Command Mode CLASS-MAP-QOS

Usage Information Apply `match-any` or `match-all` class-map filters to `control-plane`, `qos`, and queuing type class-maps.

Example

```
OS10(config)# class-map type qos match-all c1
OS10(conf-cmap-qos)#
```

Command History 10.2.0E or later

clear interface

Clears the statistics per-port or for all ports.

Syntax `clear interface [interface node/slot/port[:subport]]`

- Parameters**
- `interface` — (Optional) Enter the interface type.
 - `node/slot/port[:subport]` — (Optional) Enter the port information.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# clear interface ethernet 1/1/1
```

Supported Releases 10.3.0E or later

clear qos statistics

Clears all QoS related statistics in the system.

Syntax `clear qos statistics`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# clear qos statistics
```

Supported Releases 10.2.0E or later

clear qos statistics type

Clears all queue counters for the control-plane, qos, and queuing.

Syntax	<code>clear qos statistics type {{qos queuing control-plane} [interface ethernet <i>node/slot/port[:subport]</i>]}</code>
Parameters	<ul style="list-style-type: none">• <code>qos</code> — Clears qos type statistics.• <code>queuing</code> — Clears queuing type statistics.• <code>control-plane</code> — Clears control-plane type statistics.• <code>interface ethernet <i>node-id/slot/port-id</i> [:<i>subport</i>]</code> — Clears QoS statistics for an Ethernet interface configured for qos, queuing, or control-plane.
Default	Not configured
Command Mode	EXEC
Usage Information	None
Example	<pre>OS10# clear qos statistics type qos interface ethernet 1/1/5</pre>
Example (control-plane)	<pre>OS10# clear qos statistics type control-plane interface ethernet 1/1/7</pre>
Example (queuing)	<pre>OS10# clear qos statistics type queuing interface ethernet 1/1/2</pre>
Supported Releases	10.2.0E or later

control-plane


Enters Control-Plane mode.

Syntax	<code>control-plane</code>
Parameters	None
Default	Not configured
Command Mode	CONTROL-PLANE
Usage Information	If you attach an access-list to the class-map type of control-plane, the access-list ignores the permit and deny keywords.
Example (class-map)	<pre>OS10(config)# class-map type control-plane match-any c1 OS10(conf-cmap-control-plane)#</pre>
Example (policy-map)	<pre>OS10(config)# policy-map type control-plane p1 OS10(conf-pmap-control-plane)#</pre>
Supported Releases	10.2.0E or later

flowcontrol

Enables or disables link-level flow control on an interface.

Syntax	<code>flowcontrol [receive transmit] [on off]</code>
Parameters	<ul style="list-style-type: none">• <code>receive</code> — (Optional) Indicates the port can receive flow control packets from a remote device.

 **NOTE:** In S5148F-ON, when `receive` is turned on, it enables decoding of both LLFC and PFC frames on that port.

- `transmit` — (Optional) Indicates the local port can send flow control packets to a remote device.
- `on` — (Optional) When used with `receive`, allows the local port to receive flow control traffic. When used with `transmit`, allows the local port to send flow control traffic to the remote device.
- `off` — (Optional) When used with `receive`, disables the remote device from sending flow control traffic to the local port. When used with `transmit`, disables the local port from sending flow control traffic to the remote device.

Default Disabled (`off`)

Command Mode INTERFACE

Usage Information The `no` version of this command returns the value to the default.

Example

```
OS10(conf-if-eth1/1/2)# flowcontrol transmit on
```

Supported Releases 10.3.0E or later

match

Configures match criteria for the QoS policy.

Syntax `match {cos cos-number | ip [access-group name name | dscp dscp-value | precedence value] | ipv6 [access-group name name [set dscp dscp-value]] | mac access-group acl-name | not [ip | cos] vlan vlan-id} [set dscp dscp-value]`

- Parameters**
- `cos cos-number` — Enter a queue number for the CoS match criteria (0 to 7).
 - `ip` — Enter the IPv4 match criteria.
 - `access-group name name` — (Optional) Enter the IPv4 access-group name.
 - `dscp dscp-value` — (Optional) Enter a DSCP value for Layer 3 DSCP match criteria (0 to 63).
 - `precedence value` — (Optional) Enter a precedence value for Layer 3 precedence match criteria (0 to 7).
 - `ipv6` — Enter the IPv6 match criteria.
 - `access-group name name` — (Optional) Enter the IPv6 access-group name.
 - `set dscp dscp-value` — (Optional) Configure a DSCP value for Layer 3 DSCP match criteria (0 to 63).
 - `mac access-group name name` — Enter an access-group name for the MAC access-list match criteria (up to 140 characters).
 - `set dscp dscp-value` — Enter a DSCP value for marking the DSCP packets (0 to 63).
 - `not` — Enter the IP or CoS to negate the match criteria.
 - `vlan vlan-id` — Enter a VLAN number for VLAN match criteria (1 to 4093).

Default Not configured

Command Mode CLASS-MAP

Usage Information In a `match-any` class, you can enter multiple match criteria. In a `match-all` class, if the match case is `access-group`, no other match criteria is allowed. If you attach the `access-list` to `class-map type control-plane`, the `access-list` ignores the `permit` and `deny` keywords.

Example

```
OS10(conf-cmap-qos)# match ip access-group name ag1
OS10(config-cmap-qos)# match ipv6 access-group name ACLv6 set dscp 40
```

Supported Releases 10.2.0E or later

match cos

Matches a cost of service (CoS) value to L2 dot1p packets.

Syntax	<code>match [not] cos cos-value</code>
Parameters	<ul style="list-style-type: none">• <code>cos-value</code> — Enter a CoS value (0 to 7).• <code>not</code> — Enter <code>not</code> to cancel the match criteria.
Default	Not configured
Command Modes	CLASS-MAP
Usage Information	You cannot have two match statements with the same filter-type. If you enter two match statements with the same filter-type, the second statement overwrites the first statement.
Example	<pre>OS10(conf-cmap-qos)# match cos 3</pre>
Supported Releases	10.2.0E or later

match dscp

Configures a DSCP value as a match criteria for a class-map.

Syntax	<code>match [not] {ip ipv6 ip-any } dscp [dscp-list dscp-list]</code>
Parameters	<ul style="list-style-type: none">• <code>not</code> — (Optional) Enter to cancel a previously applied match criteria.• <code>ip</code> — Enter to use IPv4 protocol as the match protocol.• <code>ipv6</code> — Enter to use IPv6 protocol as the match protocol.• <code>ip-any</code> — Enter to use both IPv4 and IPv6 as the match protocol.• <code>dscp dscp-list dscp-list</code> — Enter a DSCP value in single numbers, comma separated, or a hyphenated range (0 to 63).
Default	Not configured
Command Mode	CLASS-MAP
Usage Information	You cannot enter two match statements with the same filter-type. If you enter two match statements with the same filter-type, the second statement overwrites the first statement. The <code>match-all</code> option in a class-map does not support <code>ip-any</code> . Select either <code>ip</code> or <code>IPv6</code> for the <code>match-all</code> criteria. If you select <code>ip-any</code> , you cannot select <code>ip</code> or <code>ipv6</code> for the same filter type.
Example	<pre>OS10(conf-cmap-qos)# match ip-any dscp 17-20</pre>
Supported Releases	10.2.0E or later

match precedence

Configures IP precedence values as a match criteria.

Syntax	<code>match [not] {ip ipv6 ip-any} precedence precedence-list</code>
Parameters	<ul style="list-style-type: none">• <code>not</code> — Enter to cancel a previously applied match precedence rule.• <code>ip</code> — Enter to use IPv4 as the match precedence rule.• <code>ipv6</code> — Enter to use IPv6 as the match precedence rule.• <code>ip-any</code> — Enter to use both IPv4 and IPv6 as the match precedence rule.• <code>precedence precedence-list</code> — Enter a precedence-list value (0 to 7).
Default	Not configured

Command Mode	CLASS-MAP
Usage Information	You cannot enter two match statements with the same filter-type. If you enter two match statements with the same filter-type, the second statement overwrites the first statement.
Example	<pre>OS10(conf-cmap-qos)# match not ipv6 precedence 3</pre>
Supported Releases	10.2.0E or later

match queue

Configures a match criteria for a queue.

Syntax	<code>match queue <i>queue-number</i></code>
Parameters	<i>queue-number</i> — Enter a queue number (0 to 7).
Default	Not configured
Command Mode	CLASS-MAP
Usage Information	You can configure this command only when the class-map type is <code>queuing</code> . You cannot enter two match statements with the same filter-type. If you enter two match statements with the same filter-type, the second statement overwrites the first statement.
Example	<pre>OS10(conf-cmap-queuing)# match queue 1</pre>
Supported Releases	10.2.0E or later

match vlan

Configures a match criteria based on the VLAN ID number.

Syntax	<code>match vlan <i>vlan-id</i></code>
Parameters	<i>vlan-id</i> — Enter a VLAN ID number (1 to 4093).
Default	Not configured
Command Mode	CLASS-MAP
Usage Information	You cannot enter two match statements with the same filter-type. If you enter two match statements with the same filter-type, the second statement overwrites the first statement.
Example	<pre>OS10(conf-cmap-qos)# match vlan 100</pre>
Supported Releases	10.2.0E or later

mtu

Calculates the buffer size allocation for matched flows.

Syntax	<code>mtu <i>size</i></code>
Parameters	<i>size</i> — Enter the size of the buffer (1500 to 9216).
Default	9216
Command Mode	POLICY-MAP-CLASS-MAP

Usage Information The no version of this command returns the value to the default.

Example

```
OS10(conf-pmap-nqos-c)# mtu 2500
```

Supported Releases 10.3.0E or later

pause

Enables a pause based on buffer limits for the port to start or stop communication to the peer.

Syntax `pause [buffer-size size pause-threshold xoff-size resume-threshold xon-size]`

Parameters

- `buffer-size size` — (Optional) Enter the ingress buffer size which is used as a guaranteed buffer in KB.
 - Default values for PFC: 10G–166KB, 25G–195.5KB, 40G–315.5KB, 100G–512KB
 - Default values for LLFC: 10G,25G— 234.5KB, 40G,100G—339.5KB
- `pause-threshold xoff-size` — (Optional) Enter the buffer limit for the port to start or initiate a pause to the peer in KB .
 - Default values for PFC: 10G–96KB, 25G–96KB, 40G–192KB, 100G–232KB
 - Default values for LLFC: 10G,25G–198.5KB, 40G,100G–264.5KB
- `resume-threshold xon-size` — (Optional) Enter the buffer limit for the port to stop or cancel sending a pause to the peer in KB .
 - Default values for PFC: 10G–87KB, 25G–87KB, 40G–183KB, 100G–223KB
 - Default values for LLFC: 10G,25G–9KB, 40G,100G–36KB

Default See parameter values

Command Mode POLICY-MAP-CLASS-MAP

Usage Information This command can only be used under `network-qos` policy type. Buffer-size, pause-thresholds, and resume-thresholds vary based on platform. The no version of this command returns the value to the default. Add the policy-map with `pause` to `system-qos` to service an input to enable pause on all ports, based on a per-port link-level flow-control mode. The `xoff` and `xon` threshold settings for link-level flow-control are applied on ports where all traffic classes must be mapped to a single PG. Platform-specific default values are based on MTU sizes of 9216 and cable length of 100 meters.

Example

```
OS10(conf-pmap-c-nqos)# pause buffer-size 45 pause-threshold 25 resume-threshold 10
```

Example (global and shared buffer)

```
OS10(config)# policy-map type network-qos nqGlobalpolicy1
OS10(conf-cmap-nqos)# class CLASS-NAME
OS10(conf-cmap-nqos-c)# pause buffer-size 45 pause-threshold 30 resume-threshold 30
```

```
OS10(config)# policy-map type network-qos nqGlobalpolicy1
OS10(conf-cmap-nqos)# class type network-qos nqclass1
OS10(conf-cmap-nqos-c)# pause buffer-size 45 pause-threshold 30 resume-threshold 10
```

Supported Releases 10.3.0E or later

pfc-cos

Configures priority flow-control for cost of service (CoS).

Syntax	<code>pfc-cos cos-value</code>
Parameters	<code>cos-value</code> — Enter a single, comma-delimited, or hyphenated range of CoS values for priority flow-control to enable (0 to 7).
Default	Not configured
Command Mode	POLICY-MAP-CLASS-MAP
Usage Information	To configure link-level flow-control, do not configure <code>pfc-cos</code> for the matched class for this policy. Add the policy-map with the <code>pfc-cos</code> configuration to <code>system-qos</code> to service an input to enable priority flow-control behavior on all ports, based on a per-port priority flow-control enable mode. Add the policy-map with the <code>pfc-cos</code> configuration to interface configurations to service at input to enable priority flow-control on that particular port, based on the port's priority flow-control enable mode. If you configure 40G to 10G mode on interfaces and <code>pause (no drop)</code> is enabled on <code>system-qos</code> , all queues may or may not drop traffic based on the availability of buffers. The <code>no</code> version of this command returns the value to the default.

Example

```
OS10 (conf-pmap-c-nqos) # pfc-cos 0-2
```

Example (global buffer/shared buffer)

```
OS10 (config) # policy-map type network-qos nqGlobalpolicy1
OS10 (conf-cmap-nqos) # class CLASS-NAME
OS10 (conf-cmap-nqos-c) # pause buffer-size 45 pause-threshold 25 resume-
threshold 10
OS10 (conf-cmap-nqos-c) # pfc-cos 0-2
OS10 (conf-cmap-nqos-c) # queue-limit 140
```

Supported Releases 10.3.0E or later

pfc-max-buffer-size

Configures the maximum buffer size for the priority flow-control enabled flows.

Syntax	<code>pfc-max-buffer-size max-buffer-size</code>
Parameters	<code>max-buffer-size</code> — Enter the maximum buffer size in KB.
Default	None
Command Mode	SYSTEM-QOS
Usage Information	This command configures maximum size of the lossless buffer pool.. The <code>no</code> version of this command removes the maximum buffer size limit.

Example

```
OS10 (config-sys-qos) # pfc-max-buffer-size 2000
```

Supported Releases 10.4.0E(R1) or later

pfc-shared-buffer-size


Changes the shared buffers size limit for priority flow-control enabled flows.

Syntax	<code>pfc-shared-buffer-size buffer-size</code>
Parameters	<code>buffer-size</code> — Enter the size of the priority flow-control buffer in KB (0 to 8911).
Default	832 KB

Command Mode	SYSTEM-QOS
Usage Information	The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(conf-sys-qos)# pfc-shared-buffer-size 2000</pre>
Supported Releases	10.3.0E or later

pfc-shared-headroom-buffer-size

Configures the shared headroom size for absorbing the packets after pause frames are generated.

 **NOTE:** This command is available only on Z9100-ON and HE-IOM.

Syntax	<code>pfc-shared-headroom-buffer-size headroom-buffer-size</code>
Parameters	<code>headroom-buffer-size</code> — Enter the size of the priority flow-control headroom buffer in KB (1 to 3399).
Default	1024 KB
Command Mode	SYSTEM-QOS
Usage Information	This command is used to configure the shared headroom size. All PFC enabled priority groups can use the shared headroom space. Headroom is the buffer space which absorbs the incoming packets after the PFC frames reach the sender. Once the threshold is reached PFC frames are generated towards the sender. The packets sent by the sender after the PFC frames are generated are absorbed into the Headroom buffer. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(conf-sys-qos)# pfc-shared-headroom-buffer-size 2000</pre>
Supported Releases	10.4.0E(R1) or later

police

Configures traffic policing on incoming traffic.

Syntax	<code>police {cir committed-rate [bc committed-burst-size]} {pir peak-rate [be peak-burst-size]}</code>
Parameters	<ul style="list-style-type: none"> • <code>cir committed-rate</code> — Enter a committed rate value in kilo bits per second (0 to 4000000). • <code>bc committed-burst-size</code> — (Optional) Enter committed burst size in packets for control plane policing and in KB for data packets. (16 to 200000). • <code>pir peak-rate</code> — Enter a peak-rate value in kilo bits per second (0 to 40000000). • <code>be peak-burst-size</code> — (Optional) Enter a peak burst size in kilo bytes (16 to 200000).
Defaults	<ul style="list-style-type: none"> • <code>bc committed-burst-size</code> value is 200 KB for control plane and 100 KB for all other class-map types • <code>be peak-burst-size</code> value is 200 KB for control plane and 100 KB for all other class-map types
Command Mode	POLICY-MAP-CLASS-MAP
Usage Information	If you do not provide the peak-rate <code>pir</code> values, the committed-rate <code>cir</code> values are taken as the <code>pir</code> values. Only the ingress QoS policy type supports this command. For control-plane policing, the rate values are in pps.
Example	<pre>OS10(conf-pmap-c-qos)# police cir 5 bc 30 pir 20 be 40</pre>

Supported Releases 10.2.0E or later

policy-map

Enters QoS POLICY-MAP mode and creates or modifies a QoS policy-map.

Syntax `policy-map policy-map-name [type {qos | queuing | control-plane | application | network-qos }]`

Parameters

- *policy-map-name* — Enter a class name for the policy-map (up to 32 characters).
- *type* — Enter the policy-map type.
 - *qos* — Create a *qos* policy-map type.
 - *queuing* — Create a *queuing* policy-map type.
 - *control-plane* — Create a *control-plane* policy-map type.
 - *application* — Create an *application* policy-map type.
 - *network-qos* — Create a *network-qos* policy-map type.

Defaults *qos* = class-map type and *match-any* = class-map filter

Command Mode CONFIGURATION

Usage Information The *no* version of this command deletes a policy-map.

Example

```
OS10(config)# policy-map p1
```

Example (Queuing)

```
OS10(config)# policy-map type queuing p1
```

Supported Releases 10.2.0E or later

priority

Sets the scheduler as a strict-priority.

Syntax `priority`

Parameters None

Default WDRR — when *priority* is mentioned, it moves to SP with default level 1

Command Mode POLICY-MAP-CLASS-MAP

Usage Information If you use this command, bandwidth is not allowed. Only the egress QoS policy type supports this command.

Example

```
OS10(conf-pmap-que)# priority
```

Supported Releases 10.2.0E or later

priority-flow-control mode

Enables or disables priority flow-control mode on an interface.

Syntax `priority-flow-control mode [on]`

Parameters

- *on* — (Optional) Enables priority flow-control mode.

Default Disabled

Command Mode	INTERFACE
Usage Information	Before enabling priority flow-control on a interface, verify a matching <code>network-qos</code> type policy is configured with the <code>pfm-cos</code> value for an interface. Use this command to disable priority flow-control if you are not using a <code>network-qos</code> type policy for an interface. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(conf-if-eth1/1/2)# priority-flow-control mode on</pre>
Supported Releases	10.3.0E or later

qos-group dot1p

Configures a dot1p trust map to the traffic class.

Syntax	<code>qos-group tc-list [dot1p values]</code>
Parameters	<ul style="list-style-type: none"> • <code>qos-group tc-list</code> — Enter the traffic single value class ID (0 to 7). • <code>dot1p values</code> — (Optional) Enter either single, comma-delimited, or a hyphenated range of dot1p values (0 to 7).
Default	0
Command Mode	TRUST-MAP
Usage Information	If the trust map does not define dot1p values to any traffic class, those flows are mapped to the default traffic class (0). If some of the dot1p values are already mapped to an existing traffic class, you will receive an error. You should have a 1:1 dot1p to traffic class mapping for PFC-enabled CoS values. You should also have a common dot1p trust map for all interfaces using DCB. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(conf-tmap-dot1p-qos)# qos-group 5 dot1p 5</pre>
Supported Releases	10.3.0E or later

qos-group dscp

Configures a dscp trust map to the traffic class.

Syntax	<code>qos-group tc-list [dscp values]</code>
Parameters	<ul style="list-style-type: none"> • <code>qos-group tc-list</code> — Enter the traffic single value class ID (0 to 7). • <code>dscp values</code> — (Optional) Enter either single, comma-delimited, or a hyphenated range of dscp values (0 to 63).
Default	0
Command Mode	TRUST-MAP
Usage Information	If the trust map does not define dscp values to any traffic class, those flows are mapped to the default traffic class (0). If some of the dscp values are already mapped to an existing traffic class, you will receive an error. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(conf-tmap-dscp-qos)# qos-group 5 dscp 42</pre>
Supported Releases	10.3.0E or later

queue-limit

Configures static or dynamic shared buffer thresholds.

Syntax `queue-limit {queue-len value | thresh-mode [dynamic threshold-alpha-value | static threshold-value]}`

- Parameters**
- `queue-len value` — Enter the guaranteed size for queue (0 to 8911).
 - 45 KB (10G)/111 KB (40G) if queue is priority flow control enabled
 - 2 KB (10G)/8 KB (40G) if queue is lossy/link-level flow control
 - If this is a priority flow-control queue, this configuration is invalid
 - Only supported for POLICY-MAP-CLASS-MAP (pmap-c-queue) mode
 - `thresh-mode` — (Optional) Buffer threshold mode.
 - `dynamic thresh-alpha-value` — (Optional) Enter the value indexes to calculate the shared threshold to the enabled dynamic shared buffer threshold (0 to 10). Defaults:
 - 0 = 1/128
 - 1 = 1/64
 - 2 = 1/32
 - 3 = 1/16
 - 4 = 1/8
 - 5 = 1/4
 - 6 = 1/2
 - 7 = 1
 - 8 = 2
 - 9 = 4
 - 10 = 8
 - `static thresh-value` — (Optional) Enter the static shared buffer threshold value in Bytes.(1 to 65535).

Default Not configured

Command Mode POLICY-MAP-CLASS-MAP

Usage Information Use the `queue-len value` parameter to set the minimum guaranteed queue length for a queue. The `no` version of this command returns the value to the default.

Example

```
OS10(config)# policy-map type network-qos nqGlobalpolicy1
OS10(conf-cmap-nqos)# class type network-qos nqclass1
OS10(conf-cmap-nqos-c)# pause buffer-size 45 pause-threshold 30 resume-
threshold 10
OS10(conf-cmap-nqos-c)# queue-limit 150
```

Example (queue)

```
OS10(config)# policy-map type queuing pmap1
OS10(config-pmap-queuing)# class cmap1
OS10(config-pmap-c-que)# queue-limit queue-len 100
OS10(config-pmap-c-que)# queue-limit thresh-mode static 50
```

Supported Releases 10.3.0E or later

queue bandwidth

Configures a bandwidth for a given queue on interface.

Syntax `queue queue-number bandwidth bandwidth-percentage`

- Parameters**
- `queue-number` — Enter the queue number.
 - `bandwidth-percentage` — Enter the percentage of bandwidth.

Default Not configured

Command Mode	POLICY-MAP-CLASS-MAP
Usage Information	The <code>no</code> version of this command removes the bandwidth from the queue.
Example	
Supported Releases	10.4.0E(R1) or later

queue qos-group

Configures a dot1p traffic class to a queue.

Syntax	<code>queue number [qos-group dot1p-values]</code>
Parameters	<ul style="list-style-type: none"> • <code>queue number</code> — Enter the traffic single value queue ID (0 to 7). • <code>qos-group dot1p-values</code> — (Optional) Enter either single, comma-delimited, or a hyphenated range of dot1p values (0 to 7).
Default	0
Command Mode	TRUST-MAP
Usage Information	If the trust map does not define traffic class values to a queue, those flows are mapped to the default queue (0). If some of the traffic class values are already mapped to an existing queue, you will receive an error. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(conf-tmap-tc-queue-qos)# queue 2 qos-group 5</pre>
Supported Releases	10.3.0E or later

random-detect (interface)

Assigns a WRED profile to the specified interface.

Syntax	<code>random-detect wred-profile</code>
Parameters	<code>wred-profile</code> — Enter the name of an existing WRED profile.
Default	Not configured
Command Mode	INTERFACE
Usage Information	The <code>no</code> version of this command removes the WRED profile from the interface.
Example	<pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# random-detect test_wred</pre>
Supported Releases	10.4.0E(R1) or later

random-detect (queue)

Assigns a WRED profile to the specified queue.

Syntax	<code>random-detect wred-profile-name</code>
Parameters	<code>wred-profile-name</code> — Enter the name of an existing WRED profile.
Default	Not configured

Command Mode PMAP-C-QUE

Usage Information The no version of this command removes the WRED profile from the queue.

Example

```
OS10(config)# policy-map type queuing p1
OS10(config-pmap-queuing)# class c1
OS10(config-pmap-c-que)# random-detect test_wred
```

Supported Releases 10.4.0E(R1) or later

random-detect color

Configures the threshold of WRED profile for available colors.

Syntax random-detect color *color-name* minimum-threshold *minimum-value* maximum-threshold *maximum-value* drop-probability *drop-rate*

- Parameters**
- *color-name* — Enter the color of drop precedence for the WRED profile. The available options are: green, yellow, and red.
 - *minimum-value* — Enter the minimum threshold value for the specified color (1 to 12480).
 - *maximum-value* — Enter the maximum threshold value for the specified color (1 to 12480).
 - *drop-rate* — Enter the rate of drop precedence in percentage (0 to 100).

Default Not configured

Command Mode WRED CONFIGURATION

Usage Information The no version of this command removes the WRED profile.

Example

```
OS10(config)# wred test_wred
OS10(config-wred)# random-detect color green minimum-threshold 100
maximum-threshold 300 drop-probability 40
```

Supported Releases 10.4.0E(R1) or later

random-detect ecn

Enables Explicit Congestion Notification (ECN) for the WRED profile.

Syntax random-detect ecn

Parameters None

Default Not configured

Command Mode WRED CONFIGURATION

Usage Information The no version of this command disables ECN.

Example

```
OS10(config)# wred test_wred
OS10(config-wred)# random-detect ecn
```

Supported Releases 10.4.0E(R1) or later

random-detect ecn

Enables Explicit Congestion Notification (ECN) for the system globally.

Syntax `random-detect ecn`

Default Not configured

Command Mode SYSTEM QOS

Usage Information The `no` version of this command disables ECN globally.

NOTE: The function of this command to enable ECN globally is supported only on the S4200 platform. In the SYSTEM QOS mode, this command is not available on other platforms. Also, for S4200, ECN can be configured only per queue; you cannot configure ECN on an interface or a service pool.

Example

```
applicableOS10(config)# system-qos
OS10(config-sys-qos)# random-detect ecn
```

Supported Releases 10.4.1.0 or later

random-detect pool

Assigns a WRED profile to the specified global buffer pool.

Syntax `random-detect pool pool-value wred-profile-name`

Parameters

- `pool-value` — Enter the pool value (0 to 1).
- `wred-profile-name` — Enter the name of an existing WRED profile.

Default Not configured

Command Mode SYSTEM-QOS

Usage Information The `no` version of this command removes the WRED profile from the interface.

Example

```
OS10(config)# system qos
OS10(config-sys-qos)# random-detect pool 0 test_wred
```

Supported Releases 10.4.0E(R1) or later

random-detect weight

Configures the exponential weight value used to calculate the average queue depth for the WRED profile.

Syntax `random-detect weight weight-value`

Parameters `weight-value` — Enter a value for the weight (1 to 15).

Default Not configured

Command Mode WRED CONFIGURATION

Usage Information The `no` version of this command removes the weight factor from the WRED profile.

Example

```
OS10(config)# wred test_wred
OS10(config-wred)# random-detect weight 10
```

Supported Releases 10.4.0E(R1) or later

service-policy

Configures the input and output service policies.

Syntax `service-policy {input | output} [type {qos | queuing | network-qos}]
policy-map-name`

- Parameters**
- `input` — Enter to assign a QoS policy to the interface input.
 - `output` — Enter to assign a QoS policy to the interface output.
 - `qos` — Enter to assign a `qos` type policy-map.
 - `queuing` — Enter to assign the `queuing` type policy-map.
 - `network-qos` — Enter to assign the `network-qos` type policy-map.
 - `policy-map-name` — Enter the policy-map name (up to 32 characters).

Default Not configured

Command Mode INTERFACE

Usage Information Attach only one policy-map to the interface input and output for each `qos` and `queuing` policy-map type. You can attach four service-policies to the system QoS — one each for `qos`, `queueing`, and `network-qos` type policy-maps. When you configure service policies at the interface-level and system-level, the interface-level policy takes precedence over the system-level policy.

Example

```
OS10(conf-if-eth1/1/7)# service-policy input type qos pl
```

Supported Releases 10.2.0E or later

set cos

Sets a cost of service (CoS) value to mark L2 802.1p (dot1p) packets.

Syntax `set cos cos-value`

Parameters `cos-value` — Enter a CoS value (0 to 7).

Default Not configured

Command Mode POLICY-MAP-CLASS-MAP

Usage Information You cannot enter two set statements with the same action-type. If you enter two set statements with the same action-type, the second statement overwrites the first. When class-map type is `qos`, the `qos-group` corresponds to data queues 0 to 7.

Example

```
OS10(conf-pmap-c-qos)# set cos 6
```

Supported Releases 10.2.0E or later

set dscp

Sets the drop precedence for incoming packets based on their DSCP value and color map profile.

Syntax `set dscp dscp-value`

Parameters `dscp-value` — Enter a DSCP value (0 to 63).

Default Not configured

Command Mode	POLICY-MAP-CLASS-MAP
Usage Information	When class-map type is <code>qos</code> , the qos-group corresponds to data queues 0 to 7.
Example	<pre>OS10(conf-pmap-c-qos)# set dscp 10</pre>
Supported Releases	10.2.0E or later

set qos-group

Configures marking for the QoS-group queues.

Syntax	<code>set qos-group queue-number</code>
Parameters	<code>queue-number</code> — Enter a queue number (0 to 7).
Default	Not configured
Command Mode	POLICY-MAP-CLASS-MAP
Usage Information	The <code>qos</code> or <code>control-plane</code> ingress QoS policy type only supports this command. When class-map type is <code>control-plane</code> , the qos-group corresponds to CPU queues 0 to 11, and when the class-map type is <code>qos</code> , the qos-group corresponds to data queues 0 to 7.
Example	<pre>OS10(conf-pmap-c-qos)# set qos-group 7</pre>
Supported Releases	10.2.0E or later

shape

Shapes the outgoing traffic rate.

Syntax	<code>shape {min {kbps mbps} min-value [burst-size]} {max {kbps mbps} max-value [max-burst-size]}</code>
Parameters	<ul style="list-style-type: none"> • <code>min</code> — Enter the minimum committed rate in unit (kbps, mbps). • <code>kbps</code> — Enter the committed rate unit in kilobits per second (0 to 40000000). • <code>mbps</code> — Enter the committed rate unit in megabits per second (0 to 40000). • <code>burst-size</code> — Enter the burst size in kilobytes per packet (0 to 10000 or 1 to 1073000). • <code>max</code> — Enter the maximum peak rate in kbps, mbps. • <code>max-burst-size</code> — Enter the burst size in kilobytes per packets (0 to 10000 or 1 to 1073000).
Default	Maximum burst size is 50 kb
Command Mode	POLICY-MAP-CLASS-MAP
Usage Information	Only the ingress QoS policy type supports this command. You must enter both the minimum and maximum values. If you enter the rate value in pps, the burst provided is in packets. If you enter the rate in kbps or mbps, the burst is provided in kb.
Example	<pre>OS10(conf-pmap-c-que)# shape min kbps 11 max kbps 44</pre>
Supported Releases	10.2.0E or later

show class-map

Displays configuration details of all existing class-maps.

Syntax `show class-map [type {control-plane | qos | queuing | network-qos} class-map-name]`

- Parameters**
- `type` — Enter the policy-map type (qos, queuing, or control-plane).
 - `qos` — Displays all policy-maps of qos type.
 - `queuing` — Displays all policy-maps of queuing type.
 - `network-qos` — Displays all policy-maps of network-qos type.
 - `control-plane` — Displays all policy-maps of control-plane type.
 - `class-map-name` — Displays the QoS class-map name.

Default Not configured

Command Mode EXEC

Usage Information This command displays all class-maps of qos, queuing, network-qos, or control-plane type. The `class-map-name` parameter displays all details of a configured class-map name.

Example

```
OS10# show class-map type qos c1
      Class-map (qos):  c1 (match-all)
      Match(not): ip-any dscp 10
```

Supported Releases 10.2.0E or later

show control-plane info

Displays control-plane queue mapping and rate limits.

Syntax `show control-plane info`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information Monitors statistics for the control-plane and to troubleshoot CoPP.

Example

```
OS10# show control-plane info
Queue Rate Limit(in pps)  Protocols
0      600
1      1000
2      300
3      1300                VLT NDS
4      2000                IPV6_ICMP IPV4_ICMP
5      400                  ARP_REQ ICMPV6_RS ICMPV6_NS ISCSI
6      600                  ARP_RESP ICMPV6_RA ICMPV6_NA SSH TELNET TACACS
NTP FTP
7      400                  RSTP PVST MSTP LACP
8      600                  DOT1X LLDP FCOE
9      600                  IPV6_OSPF BGP IPV4_OSPF
10     600                  IPV6_DHCP IPV4_DHCP SERVICEABILITY VRRP
11     300                  OPEN_FLOW OSPF_HELLO
```

Supported Releases 10.2.0E or later

show control-plane statistics

Displays counters of all the CPU queue statistics.

Syntax `show control-plane info`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show control-plane statistics
Queue Packets Bytes Dropped Packets Dropped Bytes
0 0 0 0 0
1 0 0 0 0
2 0 0 0 0
3 0 0 0 0
4 0 0 0 0
5 2 172 0 0
6 0 0 0 0
7 32048 2180484 0 0
8 14140 2569184 0 0
9 0 0 0 0
10 0 0 0 0
11 0 0 0 0
```

Supported Releases 10.2.0E or later

show interface priority-flow-control

Displays the priority flow-control, operational status, CoS bitmap, and statistics per port.

Syntax `show interface ethernet 1/1/1 priority-flow-control [details]`

Parameters `details` — (Optional) Displays all priority flow control information for an interface.

Default Not configured

Command Mode EXEC

Usage Information None

Example (Details)

```
OS10# show interface priority-flow-control details

TenGig 1/1:
Admin Mode: On
OperStatus: On
PFC Priorities: 0,4,7
Total Rx PFC Frames: 300
Total Tx PFC Frames: 200
Cos      Rx      Tx
-----
0         0        0
1         0        0
2         0        0
3        300      200
4         0        0
5         0        0
6         0        0
7         0        0
```

Supported Releases 10.3.0E or later

show qos interface

Displays the QoS configuration applied to a specific interface.

Syntax `show qos interface ethernet node/slot/port[:subport]`
Parameters `node/slot/port[:subport]` — Enter the Ethernet interface information.
Default Not configured
Command Mode EXEC
Usage Information None

Example

```
OS10# show qos interface ethernet 1/1/10
Ethernet 1/1/10
  unknown-unicast-storm-control : 100 pps
  multicast-storm-control : 200 pps
  broadcast-storm-control : Disabled
  flow-control-rx: Enabled
  flow-control-tx: Disabled
  Service-policy (Input)(qos): p1
```

Supported Releases 10.2.0E or later

show policy-map

Displays information on all existing policy-maps.

Syntax `show policy-map type {control-plane | qos | queuing | network-qos} [policy-map-name]`
Parameters

- `type` — Enter the policy-map type (qos, queuing, or control-plane).
- `qos` — Displays all policy-maps of qos type.
- `queuing` — Displays all policy-maps configured of queuing type.
- `network-qos` — Displays all policy-maps configured of network-qos type.
- `control-plane` — Displays all policy-maps of control-plane type.
- `policy-map-name` — Displays the QoS policy-map name details.

Default Not configured
Command Mode EXEC
Usage Information None

Example

```
OS10# show policy-map
Service-policy(qos) input: p1
Class-map (qos): c1
  set qos-group 1
Service-policy(qos) input: p2
Class-map (qos): c2
  set qos-group 2
```

Supported Releases 10.2.0E or later

show qos control-plane

Displays the QoS configuration applied to the control-plane.

Syntax	<code>show qos control-plane</code>
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	Monitors statistics for the control-plane and troubleshoots CoPP.

Example

```
OS10# show qos control-plane
      Service-policy (Input): p1
```

Supported Releases 10.2.0E or later

show qos egress buffers interface

Displays egress buffer configurations.

Syntax	<code>show qos egress buffers interface [interface node/slot/port[:subport]]</code>
Parameters	<ul style="list-style-type: none">• <i>interface</i> — (Optional) Enter the interface type.• <i>node/slot/port[:subport]</i> — (Optional) Enter the port information.
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show qos egress buffers interface ethernet 1/1/1
Interface : ethernet1/1/1
Speed : 0
queue-number      pool-type      rsvd-buf-size  threshold-mode  threshold-valu
-----
0                  lossy          1792           dynamic         8
1                  lossy          1792           dynamic         8
2                  lossy          1792           dynamic         8
3                  lossy          1792           dynamic         8
4                  lossless       0              dynamic         10
5                  lossy          1792           dynamic         8
6                  lossy          1792           dynamic         8
7                  lossy          1792           dynamic         8
OS10#
```

Supported Releases 10.3.0E or later

show egress buffer-stats interface

Displays the buffers statistics for the egress interface.

Syntax	<code>show egress buffer-stats interface [interface node/slot/port[:subport]]</code>
Parameters	<ul style="list-style-type: none">• <i>interface</i> — (Optional) Enter the interface type.• <i>node/slot/port[:subport]</i> — (Optional) Enter the port information.
Default	Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show qos egress buffer-stats interface ethernet 1/1/1
Interface : ethernet1/1/1
Speed : 0
Queue      TX          TX          Used Total      Used shared
           pckts      bytes      buffers         buffers
-----
0           0           0           0           0
1           0           0           0           0
2           0           0           0           0
3           0           0           0           0
4           0           0           0           0
5           0           0           0           0
6           0           0           0           0
7           0           0           0           0
```

Supported Releases 10.3.0E or later

show qos ingress buffers interface

Displays interface buffer configurations.

Syntax `show qos ingress buffers interface [interface node/slot/port[:subport]]`

- Parameters**
- *interface* — (Optional) Enter the interface type.
 - *node/slot/port[:subport]* — (Optional) Enter the port information.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show qos ingress buffers interface
Interface : ethernet1/1/1
Speed : 0
Priority-grp      Reserved      Shared-buffer      Shared-buffer      XOFF
no               buffer-size    mode               threshold          threshold
-----
0                -             -                 -                 -
1                -             -                 -                 -
2                -             -                 -                 -
3                -             -                 -                 -
4                145152        -                 -                 98304
5                -             -                 -                 -
6                -             -                 -                 -
7                -             -                 -                 -
```

Supported Releases 10.3.0E or later

show ingress buffer-stats interface

Displays the buffers statistics for the ingress interface.

Syntax `show ingress buffer-stats interface [interface node/slot/port[:subport]]`

- Parameters**
- *interface* — (Optional) Enter the interface type.
 - *node/slot/port[:subport]* — (Optional) Enter the port information.

Default Not configured
Command Mode EXEC
Usage Information None

Example

```
OS10# show qos ingress buffer-stats interface ethernet 1/1/1
Interface : ethernet1/1/1
Speed : 0
Priority  Used Total          Used HDRM
Group    buffers                    buffers
-----
0         0          0          0
1         0          0          0
2         0          0          0
3         0          0          0
4         0          0          0
5         0          0          0
6         0          0          0
7         0          0          0
```

Supported Releases 10.3.0E or later

show queuing statistics

Displays QoS queuing statistics information.

Syntax `show queuing statistics interface ethernet node/slot/port[:subport] [queue number]`

- Parameters**
- *node/slot/port[:subport]* — Enter the Ethernet interface information.
 - *queue number* — Enter the QoS queue number (0 to 7).

Default Not configured

Command Mode EXEC

Usage Information Use this command to view all queuing counters. WRED counters are available only at the port level.

Example

```
OS10# show queuing statistics interface ethernet 1/1/1
Interface ethernet1/1/1 (All queues)
Description Packets Bytes
Output          0      0
Dropped         0      0
Green Drop      0      0
Yellow Drop     0      0
Red drop        0      0
```

Example (Queue)

```
OS10# show queuing statistics interface ethernet 1/1/1 queue 3
Interface ethernet1/1/1 Queue 3
Description Packets Bytes
Output          0      0
Dropped         0      0
```

Supported Releases 10.2.0E or later

show qos system

Displays the QoS configuration applied to the system.

Syntax	show qos system
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	View and verify system-level service-policy configuration information.

Example

```
OS10# show qos system

ETS Mode : off
ECN Mode : off  shows whether the ECN is enabled globally or not
Service-policy (Input) (qos) : policy1
Service-policy (Output)(queuing) : policy2
```

Supported Releases	10.4.1.0 or later
---------------------------	-------------------

show qos system buffers

Displays the system buffer configurations and utilization.

Syntax	show qos system {ingress egress} buffers
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example

```
OS10# show qos system ingress buffer
All values are in kb
Total buffers - 16384
  Total PFC buffers - 6833
    Total shared PFC buffers - 29
    Total used PFC buffers - 17
  Total lossy buffers - 9550
    Total shared lossy buffers - 9550
```

```
OS10# show qos system egress buffer
All values are in kb
Total buffers - 16384
  Total PFC buffers - 6833
    Total shared PFC buffers - 6833
    Total used PFC buffers - 0
  Total lossy buffers - 9550
    Total shared lossy buffers - 7651
    Total used lossy buffers - 0
```

Supported Releases	10.3.0E or later
---------------------------	------------------

show qos maps

Displays the active system trust map.

Syntax `show qos maps type {tc-queue | trust-map-dot1p | trust-map dscp} trust-map-name`

- Parameters**
- `dot1p` — Enter to view the dot1p trust map.
 - `dscp` — Enter to view the dscp trust map.
 - `tc-queue`—Enter to view the traffic class to queue map.
 - `trust-map` — Enter the name of the trust map.

Default Not configured

Command Mode EXEC

Usage Information None

Example (dot1p)

```
OS10# show qos maps type tc-queue queue-map1
Traffic-Class to Queue Map: queue-map1
Queue          Traffic-Class
-----
1              5
2              6
3              7
OS10# show qos maps type trust-map-dot1p dot1p-trustmap1
DOT1P Priority to Traffic-Class Map : dot1p-trustmap1
Traffic-Class  DOT1P Priority
-----
0              2
1              3
2              4
3              5
4              6
5              7
6              1
OS10# show qos maps type trust-map-dscp dscp-trustmap1
DSCP Priority to Traffic-Class Map : dscp-trustmap1
Traffic-Class  DSCP Priority
-----
0              8-15
2              16-23
1              0-7
OS10# show qos maps
Traffic-Class to Queue Map: queue-map1
Queue          Traffic-Class
-----
1              5
2              6
3              7
DOT1P Priority to Traffic-Class Map : map1
Traffic-Class  DOT1P Priority
-----
DOT1P Priority to Traffic-Class Map : dot1p-trustmap1
Traffic-Class  DOT1P Priority
-----
0              2
1              3
2              4
3              5
4              6
5              7
6              1
DSCP Priority to Traffic-Class Map : dscp-trustmap1
Traffic-Class  DSCP Priority
-----
0              8-15
2              16-23
1              0-7
```

```

Default Dot1p Priority to Traffic-Class Map
Traffic-Class      DOT1P Priority
-----
0                   1
1                   0
2                   2
3                   3
4                   4
5                   5
6                   6
7                   7
Default Dscp Priority to Traffic-Class Map
Traffic-Class      DSCP Priority
-----
0                   0-7
1                   8-15
2                   16-23
3                   24-31
4                   32-39
5                   40-47
6                   48-55
7                   56-63
Default Traffic-Class to Queue Map
Traffic-Class      Queue number
-----
0                   0
1                   1
2                   2
3                   3
4                   4
5                   5
6                   6
7                   7
OS10#

```

Example (dscp)

```

OS10# show qos trust-map dscp new-dscp-map

new-dscp-map
qos-group      Dscp
  Id
-----
0              0-7
1              8-15
2              16-23
3              24-31
4              32-39
5              40-47
6              48-55
7              56-63

```

Supported Releases 10.3.0E or later

show qos wred-profile

Displays the details of WRED profile configuration.

Syntax `show qos wred-profile [wred-profile-name]`

Parameters `wred-profile-name` — (Optional) Enter the Ethernet interface information.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show qos wred-profile
Profile Name          |           Green           |           Yellow           |
      MIN      MAX   DROP-RATE |      MIN      MAX   DROP-RATE |      MIN      MAX   DROP-RATE |
      KB        KB        %    |      KB        KB        %    |      KB        KB        %    |
-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
```

Example (S4200) — When ECN is enabled globally.

```
OS10#show qos wred-profile wred_prof1
Wred-profile-name gmin-thd gmax-thd gmax-drop-rate ymin-thd ymax-thd ymax-drop-rate
-----|-----|-----|-----|-----|-----|-----|
wred_prof1 0 0 0 1 10 40 0 0 0

S4200 o/p
```

```
OS10# show qos wred-profile

Profile Name          |           Green           |           Yellow           |
-----|-----|-----|-----|-----|-----|-----|
      MIN      MAX   DROP-RATE |      MIN      MAX   DROP-RATE |      MIN      MAX   DROP-RATE |
      KB        KB        %    |      KB        KB        %    |      KB        KB        %    |
-----|-----|-----|-----|-----|-----|-----|
profile1              |           10           100           100 |                               |
-----|-----|-----|-----|-----|-----|
profile2              |                               |                               |
-----|-----|-----|-----|-----|-----|
Color Blind ECN Thd  |           100           1000           100 |                               |
-----|-----|-----|-----|-----|-----|
```

Supported Releases

system qos

Enters SYSTEM-QOS mode to configure system-level service policies.

Syntax	system qos
Parameters	None
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	None
Example	

```
OS10(config)# system qos
OS10(config-sys-qos)#
```

Supported Releases	10.2.0E or later
---------------------------	------------------

trust-map

Configures trust map on an interface or on system QoS.

Syntax	<code>trust-map {dot1p dscp} {default <i>trust-map-name</i>}</code>
Parameters	<ul style="list-style-type: none">• <code>dot1p</code> — Apply dot1p trust map.• <code>dscp</code> — Apply dscp trust map.• <code>default</code> — Apply default dot1p or dscp trust map.• <code><i>trust-map-name</i></code> — Enter the name of trust map.
Default	Disabled
Command Mode	INTERFACE SYSTEM-QoS
Usage Information	Use this command to apply the trust map on interface or System QoS. The <code>no</code> version of this command removes the applied trust map from the interface or System QoS.
Example	<pre>OS10(config)# interface ethernet 1/1/10 OS10(conf-if-eth1/1/10)# trust-map dot1p default OS10(conf-if-eth1/1/10)# trust-map dot1p d1 OS10(config)# interface ethernet 1/1/2 OS10(conf-if-eth1/1/2)# trust-map dscp default OS10(conf-if-eth1/1/2)# trust-map dscp d2 OS10(config)# system qos OS10(config-sys-qos)# trust-map dot1p default OS10(config-sys-qos)# trust-map dscp d2</pre>
Supported Releases	10.4.1.0 or later

trust dot1p-map

Creates user-defined trust map for dot1p flows.

Syntax	<code>trust dot1p-map <i>map-name</i></code>
Parameters	<code><i>map-name</i></code> — Enter the name of the dot1p trust map (up to 32 characters).
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	If trust is enabled, traffic obeys the dot1p map. <code>default-dot1p-trust</code> is a reserved trust-map name. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(config)# trust dot1p-map map1 OS10(config-tmap-dot1p-map)# qos-group 4 dot1p 5</pre>
Supported Releases	10.3.0E or later

trust dscp-map

Creates user-defined trust map for dscp flows.

Syntax	<code>trust dscp-map <i>map-name</i></code>
Parameters	<code><i>map-name</i></code> — Enter the name of the dscp trust map (up to 32 characters).

Default	Not configured
Command Mode	CONFIGURATION
Usage Information	<code>default-dscp-trust</code> is a reserved trust-map name. If <code>trust</code> is enabled, traffic obeys this trust map. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(config)# trust dscp-map dscp-trust1</pre>
Supported Releases	10.3.0E or later

qos-map traffic-class

Creates user-defined trust map for queue mapping. In S5148F-ON, apply the traffic class only on the egress traffic.

Syntax	<code>qos-map traffic-class map-name</code>
Parameters	<i>map-name</i> — Enter the name of the queue trust map (up to 32 characters).
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The traffic class will route all traffic to the mapped queue if applied on the interface- or system-level. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(config)# qos-map traffic-class queue-map1 OS10(config-qos-map)# queue 1 qos-group 5 OS10(config-qos-map)# queue 2 qos-group 6 OS10(config-qos-map)# queue 3 qos-group 7 OS10(config-qos-map)#</pre>
Supported Releases	10.3.0E or later

trust-map

Applies a dot1p or dscp traffic class to a queue trust map.

Syntax	<code>trust {dot1p dscp} {default trust-map-name}</code>
Parameters	<ul style="list-style-type: none"> <code>dot1p</code>— Applies a dot1p trust map. <code>dscp</code>— Applies a dscp trust map. <code>default</code>— Applies a default trust map.
Default	Disabled
Command Mode	SYSTEM-QOS INTERFACE
Usage Information	Use the <code>show qos maps type [tc-queue trust-map-dot1p trust-map-dscp] [string]</code> command to view the current trust mapping. You should change the trust map only during no traffic flow, and verify the correct policy maps are applied. The <code>no</code> version of this command returns the value to the default.
Example	<pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# trust-map dscp dscp-trustmap1</pre>
Supported Releases	10.4.1.0 or later

wred

Configures a weighted random early detection (WRED) profile.

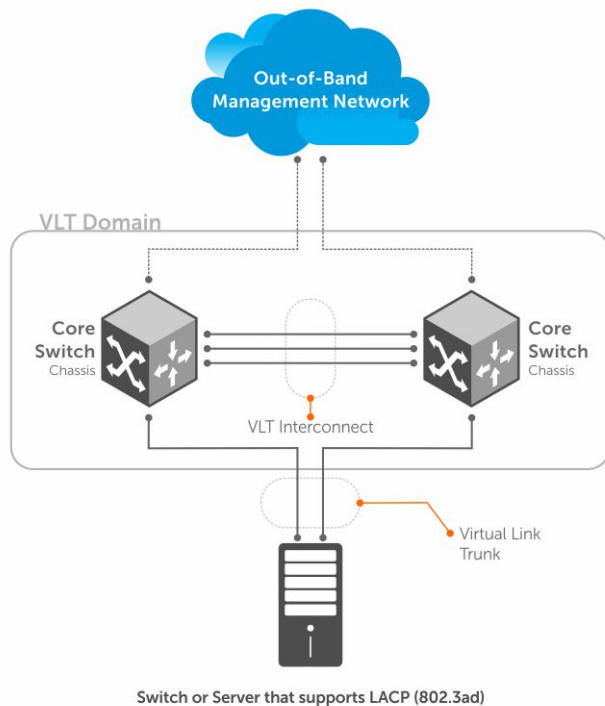
Syntax	<code>wred wred-profile-name</code>
Parameters	<code>wred-profile-name</code> — Enter a name for the WRED profile.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	The <code>no</code> version of this command removes the WRED profile.
Example	<pre>OS10(config)# wred test_wred OS10(config-wred)#</pre>
Supported Releases	10.4.0E(R1) or later

Virtual Link Trunking

Virtual Link Trunking (VLT) is a Layer 2 (L2) aggregate protocol between end devices (servers) connected to different network devices. VLT reduces the role of Spanning Tree Protocols (STPs) by allowing link aggregation group (LAG) terminations on two separate distribution or core switches and supporting a loop-free topology.

- Allows a single device to use a LAG across two upstream devices
- Provides a loop-free topology
- Eliminates STP-blocked ports
- Optimizes the use of all available uplink bandwidth
- Guarantees fast convergence if either a link or a device fails
- Enhances optimized forwarding with Virtual Router Redundancy Protocol (VRRP)
- Provides link-level resiliency
- Assures high availability

VLT provides L2 multipathing, creating redundancy through increased bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.



VLT presents a single logical L2 domain from the perspective of attached devices that have a virtual link trunk terminating on a separate node in the VLT domain. The two VLT nodes are independent Layer2 or Layer3 (L2/L3) switches for devices in the upstream network. L2/L3 control plane protocols and system management features function normally in VLT mode.

To ensure the same behavior on both sides of the VLT nodes, VRRP requires state information coordination. VLT configurations must be identical on both sides of a trunk. External switches or servers with LACP see the VLT switches as a single virtual switch.

VLT physical ports

802.1p, 802.1q, LLDP, flow control, port monitoring, and jumbo frames are supported on VLT physical ports.

System management protocols

All system management protocols are supported on VLT ports — SNMP, RMON, AAA, ACL, DNS, FTP, SSH, syslog, NTP, RADIUS, SCP, and LLDP.

L3 VLAN connectivity	Enable L3 VLAN connectivity (VLANs assigned with an IP address) on VLT peers by configuring a VLAN interface for the same VLAN on both devices.
Optimized forwarding with VRRP	To enable optimized L3 forwarding over VLT, use VRRP Active-Active mode. VRRP Active-Active mode enables each peer to locally forward L3, resulting in reduced traffic flow between peers over the VLTi.
Spanning-Tree Protocol	RSTP and RPVST+ are supported on VLT ports.

NOTE: 802.1x, DHCP snooping, MSTP, IGMP snooping, MLD snooping, ingress and egress QoS are not supported on VLT ports.

Terminology

Discovery interface	Port interfaces on VLT peers in the VLT interconnect (VLTi) link.
Virtual-link trunk (VLT port-channel)	A combined port-channel between an attached device and VLT peer switches.
VLT domain	The domain includes VLT peer devices, VLT interconnect, and all port-channels in the VLT connected to the attached devices. It is also associated with the configuration mode that you must use to assign VLT global parameters.
VLT interconnect (VLTi)	The link between VLT peer switches used to synchronize operating states.
VLT MAC address	(Optional) Unique MAC address that you assign to the VLT domain. A VLT MAC address is the common address used for all VLT peers. If you do not configure a VLT MAC address, the MAC address of the primary peer is used as the VLT MAC address across all peers.
VLT peer device	A pair of devices connected using a dedicated port-channel — the VLTi.
VLT port-channel ID	Groups port-channel interfaces on VLT peers into a single virtual-link trunk connected to an attached device. Assign the same port-channel ID to interfaces on different peers that you bundle together.
VLT Node Priority	The priority based on which the primary and secondary VLT nodes are determined. If priority is not configured, the VLT node with the lowest MAC address is elected as the primary VLT node.

VLT peer switches have independent management planes. A VLTi between the VLT chassis maintains synchronization of L2/L3 control planes across the two peer switches.

VLT domain

A VLT domain includes the VLT peer devices, VLT interconnect, and all port-channels in the VLT that connect to the attached devices. It is also associated with the configuration mode that you must use to assign VLT global parameters.

- A VLT domain supports two node members. These peer devices appear as a single logical device to network access devices that connect to VLT ports through a port-channel.
- A VLT domain consists of the two core nodes, interconnect trunk, and LAG members that connect to attached devices.
- Each VLT domain must have a unique MAC address that you create or that VLT creates automatically.
- VLAN ID 4094 is reserved as an internal control VLAN for the VLT domain.
- ARP, IPv6 neighbors, and MAC tables synchronize between the VLT peer nodes.
- VLT peer devices operate as a separate node with independent control and data planes for devices that attach to non-VLT ports.
- One node in the VLT domain takes a primary role and the other node takes the secondary role. In a VLT domain with two nodes, the VLT assigns the primary node role to the node with the lowest MAC address. By default, VLT assigns the primary node role to the node with the lowest system MAC address. You can override the default primary election mechanism by assigning priorities to each node using the `primary-priority` command.
- If the primary peer fails, the secondary peer (with the higher priority) takes the primary role. If the primary peer (with the lower priority) later comes back online, it is assigned the secondary role (there is no preemption).
- In a VLT domain, the peer network devices must run the same OS10 software version.

- Configure the same VLT domain ID on peer devices. If a VLT domain ID mismatch occurs on VLT peers, the VLTi does not activate.
- In a VLT domain, VLT peers support connections to network devices that connect to only one peer.

VLT interconnect

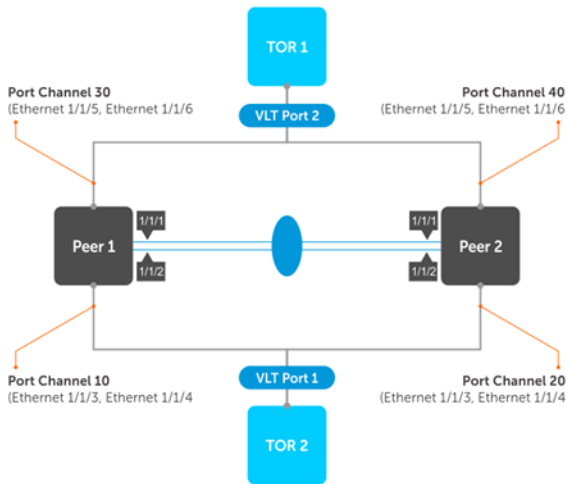
A VLTi is the link that synchronizes states between VLT peers. OS10 automatically adds VLTi ports to VLANs spanned across VLT peers. VLTi ports are not supported as members of VLANs configured on only one peer.

- The system automatically provisions the required VLANs.
- VLAN ID 4094 is reserved as an internal control VLAN for the VLT domain, and it is not user configurable.
- VLT peer switches operate as separate nodes with independent control and data planes for devices attached to non-VLT ports.
- The VLTi synchronizes L2 and L3 control-plane information across the two nodes. The VLTi is used for data traffic only when there is a link failure that requires using VLTi for data packets to reach their final destination.
- Traffic with an unknown destination MAC address, multicast, or broadcast traffic can cause flooding across the VLTi.
- MAC, ARP, IPv6 neighbors that are learned over VLANs across VLT peer nodes are synchronized across the nodes.
- In a VLT domain, LLDP, flow control, port monitoring, and jumbo frame features are supported on a VLTi.

Configure VLT

Verify that both VLT peer devices are running the same software version. For VRRP operation, configure VRRP groups and L3 routing on each VLT peer. To configure VLT and create a VLT domain where two devices are physically connected and provide a single port-channel connection to access devices, configure settings on each VLT peer device.

1. To prevent loops in VLT domain, enable the STP globally (`spanning-tree mode {rstp | rapid-pvst}` command). RSTP and RPVST+ modes are supported on VLT ports.
2. Create a VLT domain by configuring the same domain ID on each peer (`vlt-domain` command).
3. (Optional) To override the default VLT primary election mechanism based on the system MAC addresses of the VLT nodes, configure a VLT node priority for each of the VLT nodes using the `primary-priority` command. Enter a lower priority value for the desired primary VLT peer and a higher priority value for the desired secondary VLT peer.
4. Configure the VLT interconnect interfaces on each peer (`discovery-interface` command). After you configure both sides of the VLTi, the primary and secondary roles in the VLT domain are automatically assigned if primary priority is not configured.
5. (Optional) Manually reconfigure the default VLT MAC address. Configure the VLT MAC address in both the VLT peers.
6. (Optional) Configure a time interval to delay bringing up VLT ports after reload or peer-link restoration between the VLT peer switches.
7. Configure the VLT backup link used for heartbeat timers (`backup destination {ip-address | ipv6 ipv6-address} [vrf management] [interval interval-time]` command).
8. Configure VLT port-channels between VLT peers and an attached device (`vlt-port-channel` command). Assign the same VLT port-channel ID from 1 to 1024 to interfaces on different peers that you bundle together so that peer interfaces appear as a single VLT LAG to downstream devices.
9. Connect peer devices in a VLT domain to an attached access device or server.



RSTP configuration

RSTP mode is supported on VLT ports. Before you configure VLT on peer switches, configure RSTP in the network. RSTP prevents loops during the VLT startup phase.

- Enable RSTP on each peer node in CONFIGURATION mode.

```
spanning-tree mode rstp
```

Configure RSTP — peer 1

```
OS10(config)# spanning-tree mode rstp
```

Configure RSTP — peer 2

```
OS10(config)# spanning-tree mode rstp
```

View VLT-specific STP information

```
OS10# show spanning-tree virtual-interface
VFP(VirtualFabricPort) of RSTP 1 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-
violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 11, Received: 7
Interface
Name          PortID  Prio  Cost  Sts  Cost  Bridge ID          Designated
-----
VFP(VirtualFabricPort)  0.1    0    1    FWD  0    32768  0078.7614.6062  0.1
```

View STP virtual interface detail

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of RSTP 1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 32768, address: 00:78:76:14:60:62
Designated bridge priority: 32768, address: 00:78:76:14:60:62
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 15, Received: 5
```


RPVST+ configuration

RPVST+ mode is supported on VLT ports. Before you configure VLT on peer switches, configure RPVST+ in the network. You can use RPVST+ for initial loop prevention during the VLT startup phase.

Configure RPVST+ on both the VLT peers. This creates an RPVST+ instance for every VLAN configured in the system. The RPVST+ instances in the primary VLT peer control the VLT LAGs on both the primary and secondary peers.

- Enable RPVST+ on each peer node in CONFIGURATION mode.

```
spanning-tree mode rapid-pvst
```

Configure RPVST+ — peer 1

```
OS10(config)# spanning-tree mode rapid-pvst
```

Configure RPVST+ — peer 2

```
OS10(config)# spanning-tree mode rapid-pvst
```

View RPVST+ information on VLT

```
OS10# show spanning-tree virtual-interface
```

```
VFP(VirtualFabricPort) of vlan 100 is Designated Blocking
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-
violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 7, Received: 9
Interface
Designated
Name          PortID      Prio      Cost      Sts      Cost
Bridge ID      PortID
-----
VFP(VirtualFabricPort)      0.1      0      1      BLK      0
4196      90b1.1cf4.a602  0.1
```

View RPVST+ information on VLT in detail

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of vlan1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4097, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4097, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 202, Received: 42
Port 1 (VFP(VirtualFabricPort)) of vlan100 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4196, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4196, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 101, Received: 21
```

Create VLT domain

A VLT domain requires an ID number. Configure the same VLT domain ID on both peers, see [VLT domain](#). The `no vlt-domain` command disables VLT.

1. Configure a VLT domain and enter VLT-DOMAIN mode. Configure the same VLT domain ID on each peer, from 1 to 255.

```
vlt-domain domain-id
```

2. Repeat the steps on the VLT peer to create the VLT domain.

Peer 1

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)#
```

Peer 2

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)#
```

VLTi configuration

Before you configure VLTi on peer interfaces, remove each interface from L2 mode with the `no switchport` command, see [VLT interconnect](#).

1. Enter the VLT domain ID to enter from CONFIGURATION mode.

```
vlt-domain domain-id
```

2. Configure one or a hyphen-separated range of VLT peer interfaces to become a member of the VLTi in INTERFACE mode.

```
discovery-interface {ethernet node/slot/port[:subport] | ethernet node/slot/
port[:subport] -node/slot/port[:subport]}
```

3. Repeat the steps on the VLT peer.

Peer 1

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# exit
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/2
```

Peer 2

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# exit
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/2
```

Configure the VLT MAC address

You can manually configure the VLT MAC address.

Configure the same VLT MAC address on both the VLT peer switches to avoid any unpredictable behavior during a VLT failover. For example, when a unit is down or when the VLTi is reset. If you do not configure a VLT MAC address, the MAC address of the primary peer is used as the VLT MAC address across all peers.

Use the `vlt-mac mac-address` to configure the MAC address in both the VLT peers.

Example configuration:

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# vlt-mac 00:00:00:00:00:02
```

NOTE: Dell EMC Networking recommends configuring the VLT MAC address manually on both the VLT peer switches. Use the same MAC address on both peers.

Configure the delay restore timer

When the secondary VLT node boots, it waits for a pre-configured amount of time (delay restore) to restore the VLT port status. This delay enables VLT peers to complete the control data information exchange.

If the peer VLT device was up at the time the VLTi link failed, the system delays bringing up the VLT ports after reload or peer-link restoration between the VLT peer switches.

When both the VLT peers are up and running, and if the VLTi fails with the VLT heartbeat up, the secondary peer brings down the VLT ports. When the VLTi comes up, the secondary peer does not bring up its VLT ports immediately. The VLT ports are brought up only after the VLT port restoration timer expires. The delay restore timer enables both VLT peers to synchronize the control information with each other.

The default timer is 90 seconds. You can use the `delay-restore seconds` command to modify the duration of the timer.

Example:

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# delay-restore 100
```

Configure the VLT peer liveliness check

The VLT peer liveliness mechanism checks for the availability of the peer node. The system sends periodic keep-alive messages to detect the liveliness of the peer node. You must use a different link other than the VLTi for the peer liveliness check. This link is referred to as the VLT backup link.

NOTE: Dell EMC Networking recommends using the OOB management network connection for the VLT backup link.

If the VLTi goes down, the backup link helps to differentiate the VLTi link failure from a peer node failure. If all links in the VLTi fail, the VLT nodes exchange node liveliness information through the backup link.

Based on the node liveliness information:

- If only the VLTi link fails, but the peer is alive, the secondary VLT peer shuts down its VLT ports.
- If the primary VLT node fails, both the VLTi and heartbeat fail, and the current secondary peer takes over the primary role.

Configure the VLT backup link using the `backup destination {ip-address | ipv6 ipv6-address} [vrf management] [interval interval-time]`. The `interval` range is from 1 to 30 seconds. The default interval is 30 seconds. Irrespective of the interval that is configured, when the VLTi link fails, the system checks for the heartbeat connection without waiting for the timed intervals, thus allowing faster convergence.

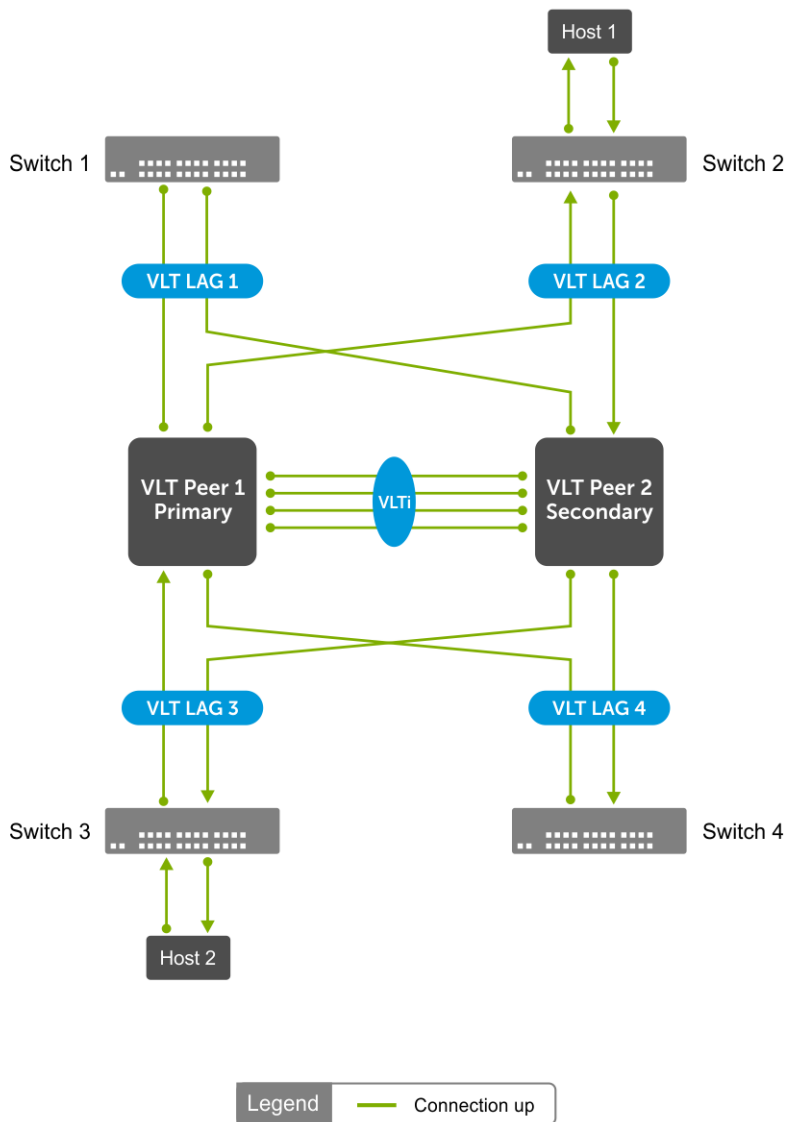
Example configuration:

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.151.110 vrf management interval 20

OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination ipv6 1::1 vrf management interval 20
```

The following examples describe different cases where the VLT backup link is used:

In the following figure, the backup link is not configured:

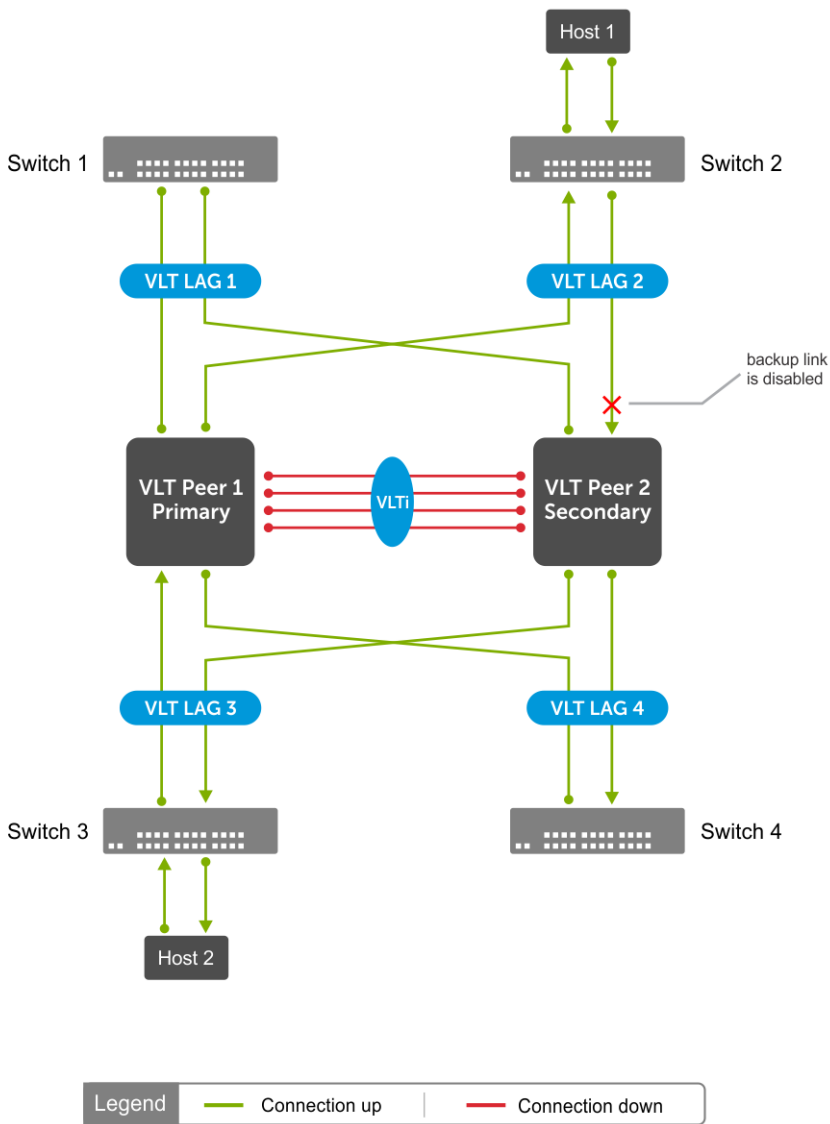


Support for new streams during VLTi failure

If the VLTi fails, MAC addresses that are learned after the failure are not synchronized with VLT peers. Thus, instead of unicast, the VLTi failure causes a continuous traffic flood.

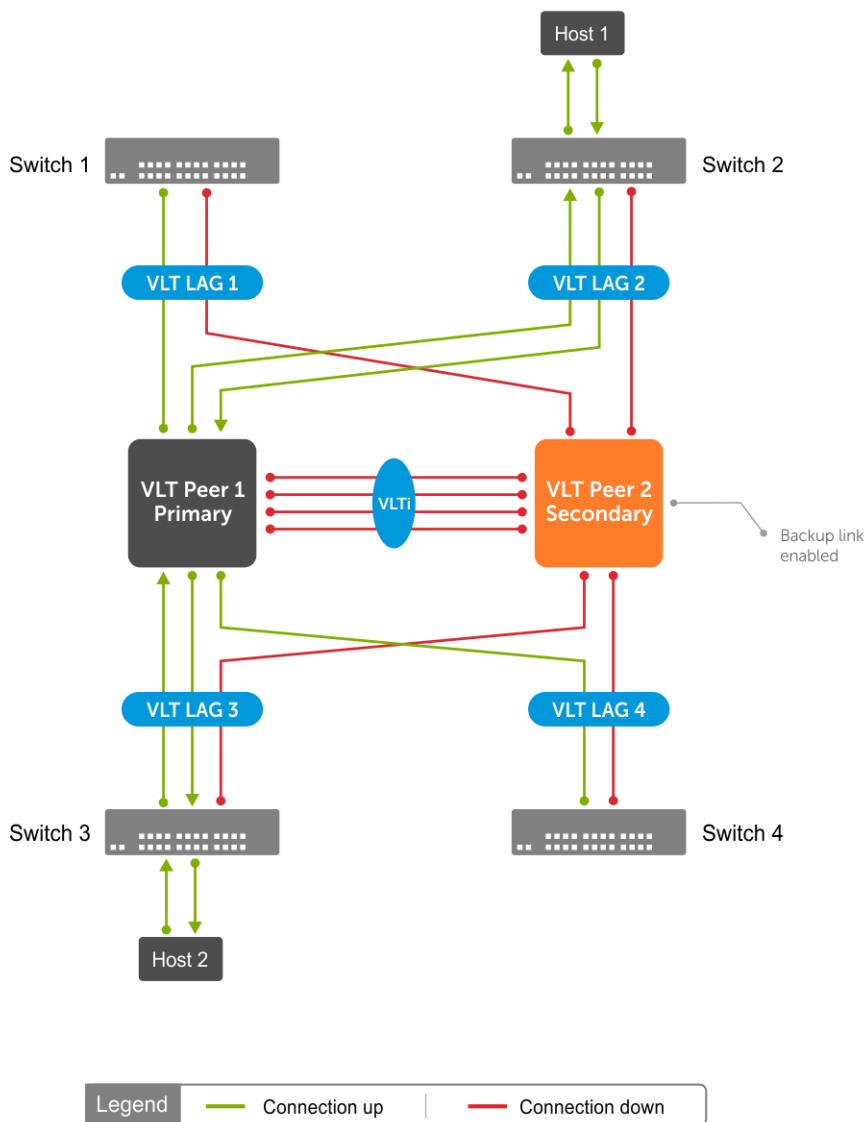
If the VLTi links fail, MAC and ARP synchronization does not happen, and it causes the system to flood L2 packets and drop L3 packets.

For example, as shown, after the VLTi is down, VLT peer1 learns the MAC address of Host 2:



VLT Peer 2 is not synchronized with the MAC address of Host 2 because the VLTi link is down. When traffic from Host 1 is sent to VLT Peer 2, VLT Peer 2 floods the traffic.

When the VLT backup link is enabled, the secondary VLT Peer 2 identifies the node liveliness through the backup link. If the primary is up, the secondary peer brings down VLT port channels. The traffic from Host 1 reaches VLT Peer 1 and then reaches the destination, Host 2. In this case, the traffic is unicasted instead of flooding, as shown:

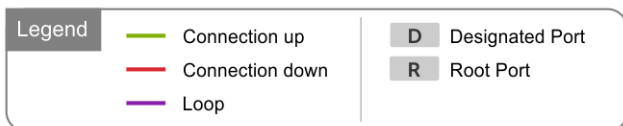
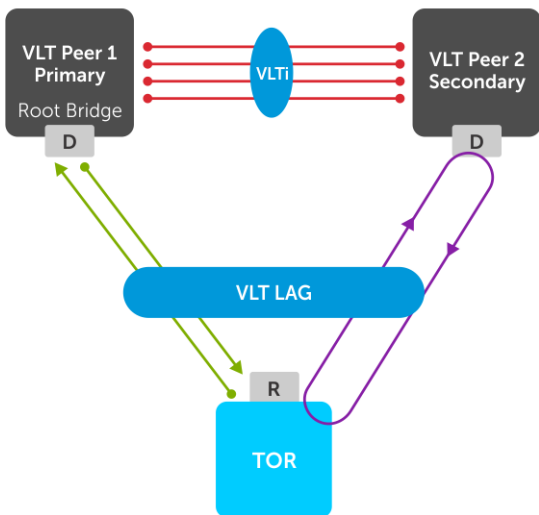


Role of VLT backup link in the prevention of loops during VLTi failure

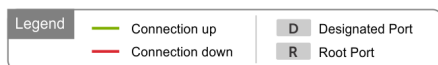
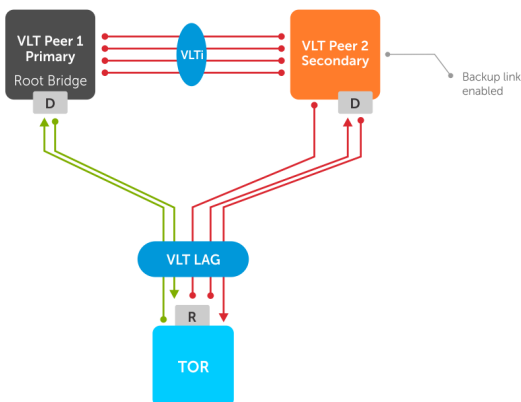
When the VLTi is down, STP may fail to detect any loops in the system. This failure creates a data loop in an L2 network.

As shown, STP is running in all three switches:

In the steady state, VLT Peer 1 is elected as the root bridge. When the VLTi is down, both the VLT nodes become primary. In this state, VLT Peer 2 sends STP BPDU to TOR assuming that TOR sends BPDU to VLT Peer 1. Due to this, VLT Peer 2 does not receive BPDU on the VLT port, but receives TOR BPDU from the orphan port. The STP in VLT Peer 2 assumes that there is no loop in the system and opens up both the VLT and the orphan ports. Opening up both the VLT and orphan ports creates a data loop and brings down the system.



When the VLT backup link is enabled, the secondary VLT peer identifies the node liveliness of primary through the backup link. If the primary VLT peer is up, the secondary VLT peer brings down the VLT port channels. In this scenario, the STP opens up the orphan port and there is no loop in the system, as shown:



Configure VLT port-channel

A VLT port-channel links an attached device and VLT peer switches, also known as a virtual link trunk.

1. Enter the port-channel ID number on the VLT peer in INTERFACE mode, from 1 to 1024.

```
interface port-channel id-number
```

2. Assign the same ID to a VLT port-channel on each VLT peer — peers are seen as a single VLT LAG to downstream devices.

```
vlt-port-channel vlt-lag-id
```

3. Repeat the steps on the VLT peer.

Configure VLT LAG — peer 1

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# vlt-port-channel 1
```

Configure VLT LAG — peer 2

```
OS10(config)# interface port-channel 20
OS10(conf-if-po-20)# vlt-port-channel 1
```

VLT unicast routing

VLT unicast routing enables optimized routing where packets destined for the L3 endpoint of the VLT peer are locally routed. VLT unicast routing is supported for IPv4 and IPv6.

To enable VLT unicast routing, both VLT peers must be in L3 mode. The VLAN configuration must be symmetrical on both peers. You cannot configure the same VLAN as L2 on one node and as L3 on the other node.

1. Enter the VLT domain ID in CONFIGURATION mode, from 1 to 1024.

```
vlt-domain domain-id
```

2. Enable peer-routing in VLT-DOMAIN mode.

```
peer-routing
```

3. Repeat the steps on the VLT peer.

Configure unicast routing — peer 1

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# peer-routing
```

View unicast routing — peer 1

```
do show running-configuration vlt
!
vlt-domain 1
  discovery-interface ethernet1/1/3-1/1/6,1/1/53:1-1/1/53:4,1/1/54:1-1/1/54:4
  peer-routing
```

Configure unicast routing — peer 2

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# peer-routing
```

View unicast routing — peer 2

```
do show running-configuration vlt
!
vlt-domain 1
  discovery-interface ethernet1/1/3-1/1/6,1/1/53:1-1/1/53:4,1/1/54:1-1/1/54:4
  peer-routing
```

VRRP Optimized Forwarding

To enable optimized L3 forwarding over VLT, use VRRP Active-Active mode. By default, VRRP Active-Active mode is enabled on the VLAN interfaces. In Active-Active mode, each peer locally forwards L3 traffic, resulting in reduced traffic flow over the VLTi. Configure the same L3 static and dynamic routing on each peer so that L3 reachability and routing tables are the same on both peers.

1. Enable VRRP Active-Active mode in VLAN-INTERFACE mode.

```
vrrp mode active-active
```


2. Configure VRRP on the L3 VLAN that spans both peers.
3. Repeat the steps on the VLT peer.

Configure VRRP active-active mode — peer 1

```
OS10(conf-if-vl-10)# vrrp mode active-active
```

Configure VRRP active-active mode — peer 2

```
OS10(conf-if-vl-10)# vrrp mode active-active
```

View VRRP configuration

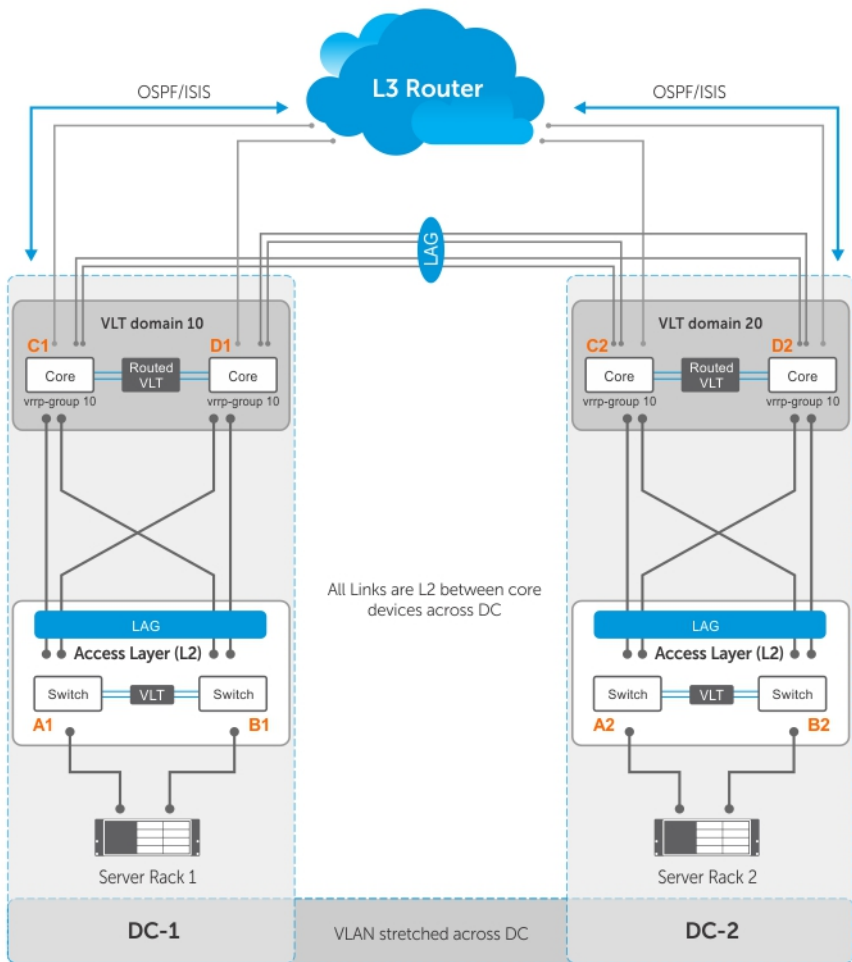
```
OS10# show running-configuration interface vlan 10
!
interface vlan10
  no shutdown
  no vrrp mode active-active
OS10#
```

Migrate VMs across data centers

OS10 does not support proxy gateway. Instead of proxy gateway, you can use VRRP in VLANs to migrate virtual machines across data centers.

You must assign same VRRP group IDs to the VLANs in L3 mode, with VRRP in active-active mode.

The following illustration shows a sample configuration with two data centers:



- Server racks, Rack 1 and Rack 2, are part of data centers DC1 and DC2, respectively.
- Rack 1 is connected to devices A1 and B1 in a Layer 2 network segment.
- Rack 2 is connected to devices A2 and B2 in a Layer 2 network segment.
- A VLT link aggregation group (LAG) is present between A1 and B1 as well as A2 and B2.
- A1 and B1 are connected to core routers, C1 and D1 with VLT routing enabled.
- A2 and B2 are connected to core routers, C2 and D2, with VLT routing enabled.
- The core routers C1 and D1 in the local VLT domain are connected to the core routers C2 and D2 in the remote VLT Domain using VLT links.
- The core routers C1 and D1 in local VLT Domain along with C2 and D2 in the remote VLT Domain are part of a Layer 3 cloud.
- The core routers C1, D1, C2, D2 are in a VRRP group with the same vrrp-group ID.

When a virtual machine running in Server Rack 1 migrates to Server Rack 2, L3 packets for that VM are routed through the default gateway.

The following examples show sample configurations of the core routers.

Sample configuration of C1:

- **Configure VRRP on L2 links between core routers:**

```
C1(config)# interface vlan 100
C1(conf-if-vl-100)# ip address 10.10.100.1/24
C1(conf-if-vl-100)# vrrp-group 10
C1(conf-vlan100-vrid-10)# priority 250
C1(conf-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- **Configure VLT port channel for VLAN 100:**

```
C1(config)# interface port-channel 10
C1(conf-if-po-10)# vlt-port-channel 10
C1(conf-if-po-10)# switchport mode trunk
C1(conf-if-po-10)# switchport trunk allowed vlan 100
C1(conf-if-po-10)# exit
```

- **Add members to port channel 10:**

```
C1(config)# interface ethernet 1/1/3
C1(conf-if-eth1/1/3)# channel-group 10
C1(conf-if-eth1/1/3)# exit
C1(config)# interface ethernet 1/1/4
C1(conf-if-eth1/1/4)# channel-group 10
C1(conf-if-eth1/1/4)# exit
```

- **Configure OSPF on L3 side of core router:**

```
C1(config)# router ospf 100
C1(conf-router-ospf-100)# exit
C1(config)# interface vlan 200
C1(conf-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- **Configure VLT port channel for VLAN 200:**

```
C1(config)# interface port-channel 20
C1(conf-if-po-20)# vlt-port-channel 20
C1(conf-if-po-20)# switchport mode trunk
C1(conf-if-po-20)# switchport trunk allowed vlan 200
C1(conf-if-po-20)# exit
```

- **Add members to port channel 20:**

```
C1(config)# interface ethernet 1/1/5
C1(conf-if-eth1/1/5)# channel-group 20
C1(conf-if-eth1/1/5)# exit
C1(config)# interface ethernet 1/1/6
C1(conf-if-eth1/1/6)# channel-group 20
C1(conf-if-eth1/1/6)# exit
```

Sample configuration of D1:

- **Configure VRRP on L2 links between core routers:**

```
D1(config)# interface vlan 100
D1(conf-if-vl-100)# ip address 10.10.100.2/24
D1(conf-if-vl-100)# vrrp-group 10
D1(conf-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- **Configure VLT port channel for VLAN 100:**

```
D1(config)# interface port-channel 10
D1(conf-if-po-10)# vlt-port-channel 10
D1(conf-if-po-10)# switchport mode trunk
D1(conf-if-po-10)# switchport trunk allowed vlan 100
D1(conf-if-po-10)# exit
```

- **Add members to port channel 10:**

```
D1(config)# interface ethernet 1/1/3
D1(conf-if-eth1/1/3)# channel-group 10
D1(conf-if-eth1/1/3)# exit
D1(config)# interface ethernet 1/1/4
D1(conf-if-eth1/1/4)# channel-group 10
D1(conf-if-eth1/1/4)# exit
```

- **Configure OSPF on L3 side of core router:**

```
D1(config)# router ospf 100
D1(conf-router-ospf-100)# exit
```

```
D1(config)# interface vlan 200
D1(conf-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- **Configure VLT port channel for VLAN 200:**

```
D1(config)# interface port-channel 20
D1(conf-if-po-20)# vlt-port-channel 20
D1(conf-if-po-20)# switchport mode trunk
D1(conf-if-po-20)# switchport trunk allowed vlan 200
D1(conf-if-po-20)# exit
```

- **Add members to port channel 20:**

```
D1(config)# interface ethernet 1/1/5
D1(conf-if-eth1/1/5)# channel-group 20
D1(conf-if-eth1/1/5)# exit
D1(config)# interface ethernet 1/1/6
D1(conf-if-eth1/1/6)# channel-group 20
D1(conf-if-eth1/1/6)# exit
```

Sample configuration of C2:

- **Configure VRRP on L2 links between core routers:**

```
C2(config)# interface vlan 100
C2(conf-if-vl-100)# ip address 10.10.100.3/24
C2(conf-if-vl-100)# vrrp-group 10
C2(conf-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- **Configure VLT port channel for VLAN 100:**

```
C2(config)# interface port-channel 10
C2(conf-if-po-10)# vlt-port-channel 10
C2(conf-if-po-10)# switchport mode trunk
C2(conf-if-po-10)# switchport trunk allowed vlan 100
C2(conf-if-po-10)# exit
```

- **Add members to port channel 10:**

```
C2(config)# interface ethernet 1/1/3
C2(conf-if-eth1/1/3)# channel-group 10
C2(conf-if-eth1/1/3)# exit
C2(config)# interface ethernet 1/1/4
C2(conf-if-eth1/1/4)# channel-group 10
C2(conf-if-eth1/1/4)# exit
```

- **Configure OSPF on L3 side of core router:**

```
C2(config)# router ospf 100
C2(conf-router-ospf-100)# exit
C2(config)# interface vlan 200
C2(conf-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- **Configure VLT port channel for VLAN 200:**

```
C2(config)# interface port-channel 20
C2(conf-if-po-20)# vlt-port-channel 20
C2(conf-if-po-20)# switchport mode trunk
C2(conf-if-po-20)# switchport trunk allowed vlan 200
C2(conf-if-po-20)# exit
```

- **Add members to port channel 20:**

```
C2(config)# interface ethernet 1/1/5
C2(conf-if-eth1/1/5)# channel-group 20
C2(conf-if-eth1/1/5)# exit
C2(config)# interface ethernet 1/1/6
C2(conf-if-eth1/1/6)# channel-group 20
C2(conf-if-eth1/1/6)# exit
```

Sample configuration of D2:

- **Configure VRRP on L2 links between core routers:**

```
D2(config)# interface vlan 100
D2(conf-if-vl-100)# ip address 10.10.100.4/24
D2(conf-if-vl-100)# vrrp-group 10
D2(conf-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- **Configure VLT port channel for VLAN 100:**

```
D2(config)# interface port-channel 10
D2(conf-if-po-10)# vlt-port-channel 10
D2(conf-if-po-10)# switchport mode trunk
D2(conf-if-po-10)# switchport trunk allowed vlan 100
D2(conf-if-po-10)# exit
```

- **Add members to port channel 10:**

```
D2(config)# interface ethernet 1/1/3
D2(conf-if-eth1/1/3)# channel-group 10
D2(conf-if-eth1/1/3)# exit
D2(config)# interface ethernet 1/1/4
D2(conf-if-eth1/1/4)# channel-group 10
D2(conf-if-eth1/1/4)# exit
```

- **Configure OSPF on L3 side of core router:**

```
D2(config)# router ospf 100
D2(conf-router-ospf-100)# exit
D2(config)# interface vlan 200
D2(conf-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- **Configure VLT port channel for VLAN 200:**

```
D2(config)# interface port-channel 20
D2(conf-if-po-20)# vlt-port-channel 20
D2(conf-if-po-20)# switchport mode trunk
D2(conf-if-po-20)# switchport trunk allowed vlan 200
D2(conf-if-po-20)# exit
```

- **Add members to port channel 20:**

```
D2(config)# interface ethernet 1/1/5
D2(conf-if-eth1/1/5)# channel-group 20
D2(conf-if-eth1/1/5)# exit
D2(config)# interface ethernet 1/1/6
D2(conf-if-eth1/1/6)# channel-group 20
D2(conf-if-eth1/1/6)# exit
```

View VLT information

To monitor the operation or verify the configuration of a VLT domain, use a VLT `show` command on primary and secondary peers.

- View detailed information about the VLT domain configuration in EXEC mode, including VLTi status, local and peer MAC addresses, peer-routing status, and VLT peer parameters.

```
show vlt domain-id
```

- View the role of the local and remote VLT peer in EXEC mode.

```
show vlt domain-id role
```

- View any mismatches in the VLT configuration in EXEC mode.

```
show vlt domain-id mismatch
```

- View detailed information about VLT ports in EXEC mode.

```
show vlt domain-id vlt-port-detail
```

- View the current configuration of all VLT domains in EXEC mode.

```
show running-configuration vlt
```

View peer-routing information

```
OS10# show vlt 255
Domain ID           : 255
Unit ID            : 1
Role               : primary
Version           : 2.0
Local System MAC address : 34:17:eb:3a:bd:80
Role priority      : 1
VLT MAC address    : aa:bb:cc:dd:ee:ff
IP address         : fda5:74c8:b79e:1::1
Delay-Restore timer : 100 seconds
Peer-Routing       : Enabled
Peer-Routing-Timeout timer : 9999 seconds
VLTi Link Status
  port-channel1000 : up
```

VLT Peer Unit ID	System MAC Address	Status	IP Address	Version
2	34:17:eb:3a:c2:80	up	fda5:74c8:b79e:1::2	2.0

View VLT role

* indicates the local peer

```
OS10# show vlt 1 role
VLT Unit ID  Role
-----
* 1          primary
  2          secondary
```

View VLT mismatch — no mismatch

```
OS10# show vlt 1 mismatch
Peer-routing mismatch:
No mismatch

VLAN mismatch:
No mismatch

VLT VLAN mismatch:
No mismatch
```

View VLT mismatch — mismatch in VLT configuration

```
OS10# show vlt 1 mismatch peer-routing
Peer-routing mismatch:
VLT Unit ID  Peer-routing
-----
* 1          Enabled
  2          Disabled

OS10# show vlt 1 mismatch
Peer-routing mismatch:
VLT Unit ID  Peer-routing
-----
* 1          Enabled
  2          Disabled

VLAN mismatch:
VLT Unit ID  Mismatch VLAN List
```

```

-----
* 1          -
  2          4

VLT VLAN mismatch:
VLT ID : 1
VLT Unit ID      Mismatch VLAN List
-----
* 1          1
  2          2
VLT ID : 2
VLT Unit ID      Mismatch VLAN List
-----
* 1          1
  2          2

```

View VLT port details

* indicates the local peer

```

OS10# show vlt 1 vlt-port-detail
VLT port channel ID : 1
VLT Unit ID      Port-Channel      Status      Configured ports  Active ports
-----
* 1              port-channel11    down        2                 0
  2              port-channel11    down        2                 0
VLT port channel ID : 2
VLT Unit ID      Port-Channel      Status      Configured ports  Active ports
-----
* 1              port-channel12    down        1                 0
  2              port-channel12    down        1                 0
VLT port channel ID : 3
VLT Unit ID      Port-Channel      Status      Configured ports  Active ports
-----
  2              port-channel13    down        1                 0

```

View VLT running configuration

```

OS10# show running-configuration vlt
!
vlt domain 1
  peer-routing
  discovery-interface ethernet1/1/17
!
interface port-channel1
  vlt-port-channel 10
!
interface port-channel10
  vlt-port-channel 20
!
interface port-channel20
  vlt-port-channel 20

```

VLT commands

backup destination

Configures the VLT backup link for heartbeat timers.

Syntax `backup destination {ip-address | ipv6 ipv6-address} [vrf management] [interval interval-time]`

- Parameters**
- *ip-address* — Enter the IPv4 address of the backup link.
 - *ipv6-address* — Enter the IPv6 address of the backup link.
 - *vrf management* — (Optional) Configures the management VRF instance for the backup IPv4 or IPv6 address.

- `interval interval-time` — (Optional) Enter the time in seconds to configure the heartbeat interval.

Default Not configured

Command Mode VLT-DOMAIN

Usage Information The `no` version of this command removes the IP address from the backup link.

Example

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.151.110 vrf management
interval 30
```

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination ipv6 1::1 vrf management interval 30
```

Supported Releases 10.3.1E or later

delay-restore

Configures a time interval to delay the bringing up of VLT ports after reload or peer-link restoration between the VLT peer switches.

Syntax `delay-restore seconds`

Parameters `seconds` — Enter a delay time, in seconds, to delay bringing up VLT ports after the VLTi device is reloaded, from 1 to 1200.

Default 90 seconds

Command Mode VLT-DOMAIN

Usage Information Use this command to delay the system from bringing up the VLT port for a brief period to allow L3 routing protocols to converge. If the peer VLT device was up at the time the VLTi link failed, use this command after a VLT device is reloaded. The `no` version of this command resets the delay time to the default value.

Example

```
OS10(conf-vlt-1)# delay-restore 100
```

Supported Releases 10.3.0E or later

discovery-interface

Configures the interface to discover and connect to a VLT peer in the VLT interconnect (VLTi) link between peers.

Syntax `discovery-interface {ethernet node/slot/port[:subport]}`

Parameters `ethernet` — Enter the Ethernet interface information for the port on a VLT peer. You can also enter a range of interfaces separated by hyphens.

Default None

Command Mode VLT-DOMAIN

Usage Information The VLT node discovery service auto-LAGs the discovery ports and creates VLTi interfaces. The `no` version of this command disables the discovery-interface configuration.

Example

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# discovery-interface ethernet 1/1/15
```


Example (range)

```
OS10(config)# vlt-domain 2
OS10(config-vlt-2)# discovery-interface ethernet 1/1/1-1/1/12
```

Supported Releases 10.2.0E or later

peer-routing

Enables or disables L3 routing to peers.

Syntax `peer-routing`

Parameters None

Default Disabled

Command Mode VLT-DOMAIN

Usage Information The no version of this command disables L3 routing.

Example

```
OS10(config-vlt-1)# peer-routing
```

Supported Releases 10.2.0E or later

peer-routing-timeout

Configures the delay after which peer routing is disabled when the peer is not available. This command is applicable for both IPv6 and IPv4.

Syntax `peer-routing-timeout value`

Parameters *value* — Enter the timeout value in seconds, from 0 to 65535.

Default 0

Command Mode VLT-DOMAIN

Usage Information Use this command to configure a timer to disable the peer-routing when the peer is not available. When the timer expires, the software checks to see if the VLT peer is available. If the VLT peer is not available, peer-routing is disabled on the peer. If you do not configure the timer, peer-routing is not disabled even when the peer is unavailable.

Example

```
OS10(config-vlt-1)# peer-routing-timeout 120
```

Supported Releases 10.3.0E or later

primary-priority

Configures the priority to be used for selecting the primary and secondary VLT peers during election.

Syntax `primary-priority value`

Parameters *value* — To configure the primary role on a VLT peer, enter a lower value than the priority value of the remote peer. The range is from 1 to 65535. The default value is 32768.

Default 32768.

Command Mode VLT-DOMAIN

Usage Information

- After you configure a VLT domain on each peer switch and connect (cable) the two VLT peers on each side of the VLT interconnect, the system elects a primary and secondary VLT peer device. To configure the primary and secondary roles before the election process, use the `primary-priority` command. Enter a lower value on the primary peer and a higher value on the secondary peer. If the primary peer fails, the secondary peer (with the higher priority) takes the primary role. If the primary peer (with the lower priority) later comes back online, it is assigned the secondary role (there is no preemption).
- If the priority values configured on the two VLT peers are equal, VLT uses the default primary election mechanism based on the values of the system MAC addresses of the two nodes. The VLT peer with the lowest system MAC address assumes the primary role.
- In a scenario where the heartbeat is up and the VLTi link goes down between the VLT peers, both the VLT peers retain their primary and secondary roles. However, the VLT LAG on the secondary VLT peer is shutdown.

NOTE: When you configure priority for VLT peers using this command, the configuration is not effective immediately. This primary priority configuration comes into effect the next time election is triggered.

Example

```
OS10(conf-vlt-1)#primary-priority 2
```

Supported Releases

10.4.1.0 or later

show spanning-tree virtual-interface

Displays details of STP and RPVST+ information specific to VLT.

Syntax `show spanning-tree virtual-interface [detail]`

Parameters `detail` — (Optional) Displays detailed output.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show spanning-tree virtual-interface
VFP(VirtualFabricPort) of RSTP 1 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 11, Received: 7
Interface
Name          PortID  Prio  Cost  Sts  Cost  Bridge ID          Designated
-----
VFP(VirtualFabricPort) 0.1    0    1    FWD  0    32768  0078.7614.6062  0.1
```

```
OS10# show spanning-tree virtual-interface
VFP(VirtualFabricPort) of vlan 100 is Designated Blocking
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 7, Received: 9
Interface
Name          PortID  Prio  Cost  Sts  Cost  Bridge ID          Designated
-----
VFP(VirtualFabricPort) 0.1    0    1    BLK  0    4196  90b1.1cf4.a602  0.1
```

Example (detail)

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of RSTP 1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 32768, address: 00:78:76:14:60:62
Designated bridge priority: 32768, address: 00:78:76:14:60:62
```

```
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 15, Received: 5
```

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of vlan1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4097, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4097, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 202, Received: 42
Port 1 (VFP(VirtualFabricPort)) of vlan100 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4196, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4196, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 101, Received: 21
```

Supported Releases 10.3.0E or later

show vlt

Displays information on a VLT domain.

Syntax `show vlt id`

Parameter `id` — Enter a VLT domain ID, from 1 to 255.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show vlt 255
Domain ID           : 255
Unit ID            : 1
Role               : primary
Version           : 2.0
Local System MAC address : 34:17:eb:3a:bd:80
Role priority      : 1
VLT MAC address    : aa:bb:cc:dd:ee:ff
IP address         : fda5:74c8:b79e:1::1
Delay-Restore timer : 100 seconds
Peer-Routing       : Enabled
Peer-Routing-Timeout timer : 9999 seconds
VLTi Link Status
  port-channel1000 : up
```

VLT Peer	Unit ID	System MAC Address	Status	IP Address	Version
2		34:17:eb:3a:c2:80	up	fda5:74c8:b79e:1::2	2.0

Supported Releases 10.2.0E or later

show vlt backup-link

Displays the details of heartbeat status.

Syntax `show vlt domain-id backup-link`

Parameters `domain-id` — Enter the VLT domain ID.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show vlt 255 backup-link
VLT Backup Link
-----
Destination                : 10.16.208.164
Peer Heartbeat status      : Up
Heartbeat interval         : 1
Heartbeat timeout          : 3
```

Supported Releases 10.3.1E or later

show vlt mac-inconsistency

Displays inconsistencies in dynamic MAC addresses learnt between VLT peers across spanned-vlans.

Syntax `show vlt mac-inconsistency`

Parameters None

Default Not configured

Command Mode EXEC

Usage Information Use this command to check mismatch of MAC address table entries between VLT peers. To verify VLT configuration mismatch issues on peer switches, use the `show vlt domain-name mismatch` command.

Example

```
OS10# show vlt-mac-inconsistency
Checking Vlan 228 .. Found 7 inconsistencies .. Progress 100%
VLAN 128
-----
MAC 00:00:00:00:00:02 is missing from Node(s) 2
VLAN 1
-----
MAC 00:a0:c9:00:00:18 is missing from Node(s) 2
MAC 00:a0:c9:00:00:20 is missing from Node(s) 2
VLAN 131
-----
MAC 00:00:00:00:00:02 is missing from Node(s) 2
VLAN 132
-----
MAC 00:00:00:00:00:02 is missing from Node(s) 2
VLAN 135
-----
MAC 00:00:00:00:00:02 is missing from Node(s) 2
VLAN 137
-----
MAC 00:00:00:00:00:02 is missing from Node(s) 2

Run "show vlt d1 mismatch ..." commands to identify configuration issues
```

Supported Releases 10.2.0E or later

show vlt mismatch

Displays mismatches in a VLT domain configuration.

Syntax `show vlt id mismatch [peer-routing | vlan | vlt-vlan vlt-port-id]`

- Parameters**
- `id` — Enter the VLT domain ID, from 1 to 255.
 - `peer-routing` — Display mismatches in peer-routing configuration.
 - `vlan` — Display mismatches in VLAN configuration in the VLT domain.
 - `vlt-vlan vlt-port-id` — Display mismatches in VLT port configuration, from 1 to 4095.

Default Not configured

Command Mode EXEC

Usage Information The * in the mismatch output indicates a local node entry.

Example (no mismatch)

```
OS10# show vlt 1 mismatch
Peer-routing mismatch:
No mismatch

VLAN mismatch:
No mismatch

VLT VLAN mismatch:
No mismatch
```

Example (mismatch)

```
OS10# show vlt 1 mismatch
Peer-routing mismatch:
VLT Unit ID      Peer-routing
-----
* 1              Enabled
  2              Disabled

VLAN mismatch:
No mismatch

VLT VLAN mismatch:
VLT ID : 1
VLT Unit ID      Mismatch VLAN List
-----
* 1              1
  2              2
VLT ID : 2
VLT Unit ID      Mismatch VLAN List
-----
* 1              1
  2              2
```

Example (mismatch peer routing)

```
OS10# show vlt 1 mismatch peer-routing
Peer-routing mismatch:
VLT Unit ID      Peer-routing
-----
* 1              Enabled
  2              Disabled
```

Example (mismatch VLAN)

```
OS10# show vlt 1 mismatch vlan
VLT Unit ID      Mismatch VLAN List
-----
* 1              -
  2              4
```

Example (mismatch VLT VLAN)

```
OS10# show vlt 1 mismatch vlt-vlan
VLT ID : 1
VLT Unit ID      Mismatch VLAN List
-----
* 1              1
  2              2
VLT ID : 2
VLT Unit ID      Mismatch VLAN List
-----
* 1              1
  2              2
```

Supported Releases 10.2.0E or later

show vlt role

Displays the VLT role of the local peer.

Syntax `show vlt id role`

Parameters *id* — Enter the VLT domain ID, from 1 to 255.

Default Not configured

Command Mode EXEC

Usage Information The * in the mismatch output indicates a local node entry.

Example

```
OS10# show vlt 1 role
VLT Unit ID      Role
-----
* 1              primary
  2              secondary
```

Supported Releases 10.2.0E or later

show vlt vlt-port-detail

Displays detailed status information about VLT ports.

Syntax `show vlt id vlt-port-detail`

Parameters *id* — Enter a VLT domain ID, from 1 to 255.

Default Not configured

Command Mode EXEC

Usage Information The * in the mismatch output indicates a local node entry.

Example

```
OS10# show vlt 1 vlt-port-detail
Vlt-port-channel ID : 1
VLT Unit ID      Port-Channel      Status      Configured ports      Active ports
-----
* 1              port-channel1      down        2                      0
  2              port-channel1      down        2                      0
VLT ID : 2
VLT Unit ID      Port-Channel      Status      Configured ports      Active ports
-----
* 1              port-channel2      down        1                      0
  2              port-channel2      down        1                      0
```

VLT ID : 3				
VLT Unit ID	Port-Channel	Status	Configured ports	Active ports
2	port-channel3	down	1	0

Supported Releases 10.2.0E or later

vlt-domain

Creates a VLT domain.

Syntax `vlt-domain domain-id`

Parameter `domain-id` — Enter a VLT domain ID on each peer, from 1 to 255.

Default None

Command Mode CONFIGURATION

Usage Information Configure the same VLT domain ID on each peer. If a VLT domain ID mismatch occurs on VLT peers, the VLTi link between peers does not activate. The no version of this command disables VLT.

Example

```
OS10(config)# vlt-domain 1
```

Supported Releases 10.2.0E or later

vlt-port-channel

Configures the ID used to map interfaces on VLT peers into a single VLT port-channel.

Syntax `vlt-port-channel vlt-lag-id`

Parameters `vlt-lag-id` — Enter a VLT port-channel ID, from 1 to 1024.

Default Not configured

Command Mode PORT-CHANNEL INTERFACE

Usage Information Assign the same VLT port-channel ID to interfaces on VLT peers to create a VLT port-channel. The no version of this command removes the VLT port-channel ID configuration.

Example (peer 1)

```
OS10(conf-if-po-10)# vlt-port-channel 1
```

Example (peer 2)

```
OS10(conf-if-po-20)# vlt-port-channel 1
```

Supported Releases 10.2.0E or later

vlt-mac

Configures a MAC address for all peer switches in a VLT domain.

Syntax `vlt-mac mac-address`

Parameters `mac-address` — Enter a MAC address for the topology in nn:nn:nn:nn:nn:nn format.

Default Not configured

Command Mode VLT-DOMAIN

Usage Information

Use this command to minimize the time required to synchronize the default MAC address of the VLT domain on both peer devices when one peer switch reboots. If you do not configure a VLT MAC address, the MAC address of the primary peer is used as the VLT MAC address across all peers. This configuration must be symmetrical in all the peer switches to avoid any unpredictable behavior. For example, unit down or VLTi reset. The `no` version of this command disables the VLT MAC address configuration.

NOTE: Configure the VLT MAC address as symmetrical in all the VLT peer switches to avoid any unpredictable behavior when any unit is down or when VLTi is reset.

Example

```
OS10(conf-vlt-1)# vlt-mac 00:00:00:00:00:02
```

Supported Releases

10.2.0E or later

vrrp mode active-active

Enables the VRRP peers to locally forward L3 traffic in a VLAN interface.

Syntax `vrrp mode active-active`

Parameters None

Default Enabled

Command Mode VLAN INTERFACE

Usage Information The `no` version of this command disables the configuration. This command is applicable only for VLAN interfaces.

Example

```
OS10(conf-if-vl-10)# vrrp mode active-active
```

Supported Releases

10.2.0E or later

Converged data center services

OS10 supports converged data center services, including IEEE 802.1 data center bridging (DCB) extensions to classic Ethernet. DCB provides I/O consolidation in a data center network. Each network device carries multiple traffic classes while ensuring lossless delivery of storage traffic with best-effort for LAN traffic and latency-sensitive scheduling of service traffic.

- 802.1Qbb — Priority flow control
- 802.1Qaz — Enhanced transmission selection
- 802.1Qau — Congestion notification
- Data Center Bridging Exchange (DCBX) protocol

DCB enables the convergence of LAN and SAN traffic over a shared physical network in end-to-end links from servers to storage devices. In a converged network, all server, storage, and networking devices are DCB-enabled. DCB supports fibre channel over Ethernet (FCoE) and iSCSI transmission of storage data. DCB is not supported on interfaces with link-level flow control (LLFC) enabled.

Priority flow control (PFC)	Use priority-based flow control to ensure lossless transmission of storage traffic, while transmitting other traffic classes that perform better without flow control (see Priority flow control).
Enhanced transmission selection (ETS)	Assign bandwidth to 802.1p CoS-based traffic classes. Use ETS to increase preferred traffic-class throughput during network congestion (see Enhanced transmission selection).
Data Center Bridging Exchange protocol (DCBX)	Configure the DCBX protocol used by DCB neighbors to discover and exchange configuration information for plug-and-play capability (see Data center bridging eXchange).
Internet small computer system interface (iSCSI)	Use iSCSI auto-configuration and detection of storage devices, monitor iSCSI sessions, and apply QoS policies on iSCSI traffic (see Internet small computer system interface).

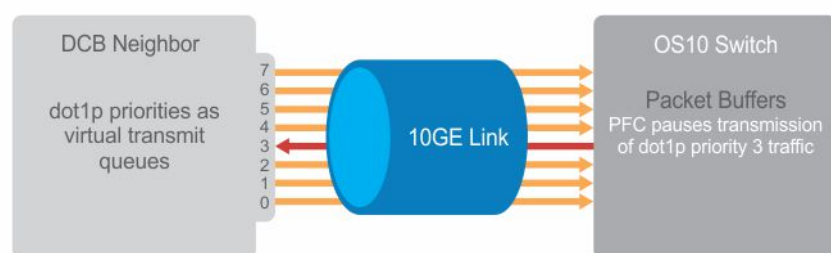
Priority flow control

In a converged data-center network, to ensure that no frames are lost due to congestion, use priority flow control (PFC). PFC uses the 802.1p priority in the Ethernet header to pause priority-specific traffic sent from a transmitting device. The 802.1p priority is also known as the class of service (CoS) or dot1p priority value.

When PFC detects congestion of a dot1p traffic class, it sends a pause frame for the priority traffic to the transmitting device. In this way, PFC ensures that specified priority traffic is not dropped by the switch.

PFC enhances the existing 802.3x pause capability to enable flow control based on 802.1p priorities. Instead of stopping all traffic on a link, as performed by the 802.3x pause mechanism, PFC pauses traffic for 802.1p traffic types. For example, when LAN traffic congestion occurs on an interface, PFC ensures lossless flows of storage and server traffic while allowing for lossy best-effort transmission of other traffic.

PFC handles traffic congestion by pausing prioritized dot1p traffic on an ingress interface and allowing other dot1p traffic best-effort, lossy data transmission.



PFC configuration notes

- PFC is supported for 802.1p priority traffic (dot1p 0 to 7). FCoE traffic traditionally uses dot1p priority 3 — iSCSI storage traffic uses dot1p priority 4.
- Configure PFC for ingress traffic by using network-qos class and policy maps (see *Quality of Service*). The queues used for PFC-enabled traffic are treated as lossless queues. Configure the same network-qos policy map on all PFC-enabled ports. Configure required bandwidth for lossless traffic using ETS queuing (output) policies on egress interfaces.
- In a network-qos policy-class map, use commands to generate PFC pause frames for matching class-map priorities:
 - Send pause frames for matching class-map traffic during congestion (`pause` command).
 - (Optional) Enter user-defined values for the reserved ingress buffer-size of PFC class-map traffic, and the thresholds used to send XOFF and XON pause frames (`pause [buffer-size kilobytes pause-threshold kilobytes resume-threshold kilobytes]command`).
 - Configure the matching dot1p values used to send pause frames (`pfc-cos` command).
 - (Optional) Set the static and dynamic thresholds that determine the shared buffers available for PFC class-map traffic queues (`queue-limit thresh-mode` command).
- By default, all ingress traffic is handled by the lossy ingress buffer. When you enable PFC, dot1p ingress traffic competes for shared buffers in the lossless pool instead of the shared lossy pool. The number of lossless queues supported on an interface depends on the amount of available free memory in the lossy pool.
- Use the `priority-flow-control mode on` command to enable PFC for FCoE and iSCSI traffic (example, priority 3 and 4).
- Enable DCBX on interfaces to detect and auto-configure PFC/ETS parameters from peers.
- PFC and 802.3x link-level flow control (LLFC) are disabled by default on an interface. You cannot enable PFC and LLFC at the same time. LLFC ensures lossy traffic in best-effort transmission. Enable PFC to enable guarantee lossless FCoE and iSCSI traffic. PFC manages buffer congestion by pausing specified ingress dot1p traffic; LLFC pauses all data transmission on an interface. To enable LLFC, enter the `flowcontrol [receive | transmit] [on | off]` command.
- SYSTEM-QOS mode applies a service policy globally on all interfaces:
 - Create and apply a 1-to-1 802.1p-priority-to-traffic-class mapping on an interface or all interfaces in INTERFACE or SYSTEM-QOS mode
 - Create and apply a 1-to-1 traffic-class-to-queue mapping on an interface or all interfaces in INTERFACE or SYSTEM-QOS mode

The S5148F-ON platform has the following limitations:

- You cannot configure PFC priority 0 as a lossless priority.
- You cannot map multiple priorities to same queue.
- Whenever LLFC is enabled on an interface, Rx PFC frames are honored. Also, whenever PFC is enabled on an interface, Rx Pause frames are honored. With respect to statistics, Rx Pause statistics in the hardware includes the Rx PFC frames too.

Configure dot1p priority to traffic class mapping

Decide if you want to use the default 802.1p priority-to-traffic class (`qos-group`) mapping or configure a new map. By default, the `qos class-trust` class map is applied to ingress traffic. The class-trust class instructs OS10 interfaces to honor dot1p or DSCP traffic.

```
Dot1p Priority : 0  1  2  3  4  5  6  7
Traffic Class : 1  0  2  3  4  5  6  7
```

- Apply the default trust map specifying that dot1p values are trusted in SYSTEM-QOS or INTERFACE mode.

```
trust-map dot1p default
```

Configure a non-default dot1p-priority-to-traffic class mapping

1. Configure a trust map of dot1p traffic classes in CONFIGURATION mode. A trust map does not modify ingress dot1p values in output flows.

Assign a `qos-group` to trusted dot1p values in TRUST mode using 1-to-1 mappings. Dot1p priorities are 0-7. For a PFC traffic class, map only one dot1p value to a `qos-group` number; for Broadcom-based NPU platforms, the `qos-group` number and the dot1p value must be the same. A `qos-group` number is used only internally to classify ingress traffic classes.

```
trust dot1p-map dot1p-map-name
  qos-group {0-7} dot1p {0-7}
exit
```

2. Apply the `trust dot1p-map` policy to ingress traffic in SYSTEM-QOS or INTERFACE mode.

```
trust-map dot1p trust-policy-map-name
```

Configure traffic-class-queue mapping

Decide if you want to use the default traffic-class-queue mapping or configure a non-default traffic-class-to-queue mapping.

```
Traffic Class : 0 1 2 3 4 5 6 7
Queue : 0 1 2 3 4 5 6 7
```

If you are using the default traffic-class-to-queue map, no further configuration steps are necessary.

1. Create a traffic-class-to-queue map in CONFIGURATION mode. Assign a traffic class (`qos-group`) to a queue in QOS-MAP mode using 1-to-1 mappings. For a PFC traffic class, map only one `qos-group` value to a `queue` number. A `qos-group` number is used only internally to classify ingress traffic.

```
qos-map traffic-class tc-queue-map-name
queue {0-7} qos-group {0-7}
exit
```

2. Apply the traffic-class-queue map in SYSTEM-QOS or INTERFACE mode.

```
qos-map traffic-class tc-queue-map-name
```

View interface PFC configuration

View PFC details on an interface.

```
OS10# show interface ethernet 1/1/1 priority-flow-control details
ethernet1/1/1
Admin Mode : true
Operstatus: true
PFC Priorities: 4
Total Rx PFC Frames: 0
Total Tx PFC frames: 0
Cos      Rx      Tx
-----
0        0        0
1        0        0
2        0        0
3        0        0
4        0        0
5        0        0
6        0        0
7        0        0
```

Configure PFC

Priority flow control (PFC) provides a pause mechanism based on the 802.1p priorities in ingress traffic. PFC prevents frame loss due to network congestion. Configure PFC lossless buffers, and enable pause frames for dot1p traffic on a per-interface basis. Repeat the PFC configuration on each PFC-enabled interface. PFC is disabled by default.

Decide if you want to use the default dot1p-priority-to-traffic class mapping and the default traffic-class-to-queue mapping. See [PFC configuration notes](#) to change the default settings.

Configuration steps:

1. Create PFC dot1p traffic classes.
2. Configure ingress buffers for PFC traffic.
3. Apply a service policy and enable PFC.
4. (Optional) Configure the PFC shared buffer for lossless traffic.

Create PFC dot1p traffic classes

1. Create a `network-qos` class map to classify PFC traffic classes in CONFIGURATION mode (1 to 7). Specify the traffic classes using the `match qos-group` command. Qos-groups map 1:1 to traffic classes 1 to 7 (`qos-group 1` corresponds

to traffic class 1). Enter a single value, a hyphen-separated range, or multiple `qos-group` values separated by commas in CLASS-MAP mode.

```
class-map type network-qos class-map-name
  match qos-group {1-7}
  exit
```

2. (Optional) Repeat Step 1 to configure additional PFC traffic-class class-maps.

NOTE: In the S5148F-ON, PFC is not supported on priority 0.

Configure pause and ingress buffers for PFC traffic

See [PFC configuration notes](#) for the default ingress queue settings and the default dot1p priority-queue mapping.

1. Create a `network-qos` policy map in CONFIGURATION mode.

```
policy-map type network-qos policy-map-name
```

2. Associate the policy-map with a `network-qos` class map in POLICY-MAP mode.

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

3. Configure default values for ingress buffers used for the `network-qos` class maps in POLICY-CLASS-MAP mode.

```
pause
```

(Optional) Change the default values for the ingress-buffer size reserved for the `network-qos` class-map traffic and the thresholds used to send XOFF and XON pause frames (in kilobytes).

```
pause [buffer-size kilobytes {pause-threshold kilobytes | resume-threshold kilobytes}]
```

4. Enable the PFC pause function for dot1p traffic in POLICY-CLASS-MAP mode. The dot1p values must be the same as the `qos-group` (traffic class) numbers in the class map in Step 2. Enter a single dot1p value (1-7), a hyphen-separated range, or multiple dot1p values separated by commas.

```
pfc-cos dot1p-priority
```

5. (Optional) Set the static and dynamic thresholds used to limit the shared buffers allocated to PFC traffic-class queues. Configure a static, fixed queue-limit (in kilobytes) or a dynamic threshold (weight 1-10; default 9) based on the available PFC shared buffers. This option is not available in S5148F-ON.

```
queue-limit thresh-mode {static kilobytes | dynamic weight}
```

6. (Optional) Repeat Steps 2–4 to configure PFC on additional traffic classes.

Apply service policy and enable PFC

1. Apply the PFC service policy on an ingress interface or interface range in INTERFACE mode.

```
interface ethernet node/slot/port[:subport]
  service-policy input type network-qos policy-map-name
```

```
interface range ethernet node/slot/port[:subport]-node/slot/port[:subport]
  service-policy input type network-qos policy-map-name
```

2. Enable PFC (without DCBX) for FCoE and iSCSI traffic in INTERFACE mode.

```
priority-flow-control mode on
```

Configure PFC

PFC is enabled on traffic classes with dot1p 3 and 4 traffic. The two traffic classes require different ingress queue processing. In the `network-qos pp1` policy map, class `cc1` uses customized PFC buffer size and pause frame settings; class `cc2` uses the default settings.

```
OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p default
```

```

OS10(config)# system qos
OS10(config-sys-qos)# service-policy input type qos pclass1
OS10(config-sys-qos)# exit

OS10(config)# class-map type network-qos cc1
OS10(config-cmap-nqos)# match qos-group 3
OS10(config-cmap-nqos)# exit

OS10(config)# class-map type network-qos cc2
OS10(config-cmap-nqos)# match qos-group 4
OS10(config-cmap-nqos)# exit

OS10(config)# policy-map type network-qos pp1
OS10(config-pmap-network-qos)# class cc1
OS10(config-pmap-c-nqos)# pause buffer-size 30 pause-threshold 20 resume-threshold 10
OS10(config-pmap-c-nqos)#pfc-cos 3
OS10(config-pmap-c-nqos)#exit
OS10(config-pmap-network-qos)# class cc2
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)#pfc-cos 4
OS10(config-pmap-c-nqos)#exit

OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# service-policy input type network-qos pp1

OS10(conf-if-eth1/1/1)# priority-flow-control mode on
OS10(conf-if-eth1/1/1)# no shutdown

```

View PFC configuration and operational status

```

OS10(conf-if-eth1/1/1)# do show interface ethernet 1/1/1 priority-flow-control details
ethernet1/1/1
Admin Mode : true
Operstatus: true
PFC Priorities: 3,4
Total Rx PFC Frames: 300
Total Tx PFC frames: 200
Cos      Rx      Tx
-----
0         0         0
1         0         0
2         0         0
3        300        200
4         0         0
5         0         0
6         0         0
7         0         0

```

View PFC ingress buffer configuration

```

OS10(config)# show qos ingress buffer interface
Interface ethernet 1/1/1
Speed 40G
-----
PG# PRIORITIES qos          ALLOTED (Kb)
   group          Reserved Shared buffer  XOFF      XON      shared
buffer          id            buffers  MODE      threshold threshold threshold
-----
0      4           4           35      DYNAMIC    9         9         8
1      3           3           35      DYNAMIC    9         9         8
2      -           -            0       STATIC     0         0         0
3      -           -            0       STATIC     0         0         0
4      -           -            0       STATIC     0         0         0
5      -           -            0       STATIC     0         0         0
6      -           -            0       STATIC     0         0         0
7      -           0-2,5-7    8       STATIC     0         0         0

```

View PFC system buffer configuration

```

OS10(config)# show qos system ingress buffer
All values are in kb

```

```
Total buffers - 12187
  Total PFC buffers - 877
    Total shared PFC buffers - 832
    Total used shared PFC buffers - 665
  Total lossy buffers - 11309
    Total shared lossy buffers - 10816
    Total used shared lossy buffers - 1534
```

```
OS10(config)# show qos system egress buffer
All values are in kb
Total buffers - 12187
  Total PFC buffers - 877
    Total shared PFC buffers - 877
    Total used shared PFC buffers - 0
  Total lossy buffers - 11309
    Total shared lossy buffers - 8983
    Total used shared lossy buffers - 2237
```

View PFC ingress buffer statistics

```
OS10(config)# show qos ingress buffer-stats interface ethernet 1/1/15
Interface : ethernet1/1/15
Speed : 10G
Priority Used reserved      Used shared  Used HDRM
Group  buffers             buffers      buffers
-----
0      9360                   681824     35984
1      0                       0           0
2      0                       0           0
3      0                       0           0
4      0                       0           0
5      0                       0           0
6      0                       0           0
7      0                       0           0
```

PFC commands

pause

Configures the ingress buffer and pause frame settings used for PFC traffic classes.

Syntax `pause [buffer-size kilobytes pause-threshold kilobytes resume-threshold kilobytes]`

- Parameters**
- `buffer-size kilobytes` — Enter the reserved (guaranteed) ingress-buffer size in kilobytes for PFC dot1p traffic (0 to 7787).
 - `pause-threshold kilobytes` — Enter the threshold used to send pause frames in kilobytes to a transmitting device (0 to 7787).
 - `resume-threshold kilobytes` — Enter the threshold used to request a transmitting device in kilobytes to resume sending traffic (0 to 7787).

Defaults The default ingress-buffer size reserved for PFC traffic classes, and the pause and resume thresholds vary according to the interface type. The default egress buffer reserved for PFC traffic classes is 0 on all interface types.

Table 41. Port defaults

Port Speed	10G Port	25G Port	40G Port	100G Port
PFC reserved ingress buffer	166 KB	195 KB	315.5 KB	512 KB
PFC pause threshold	96 KB	96 KB	192 KB	232 KB
PFC resume threshold	87 KB	87 KB	183 KB	223 KB

Command Mode	POLICY-CLASS NETWORK-QOS
Usage Information	Use the <code>pause</code> command without optional parameters to apply the default ingress-buffer size, and pause (XON) and resume (XOFF) thresholds. Default values for the <code>buffer-size</code> , <code>pause-threshold</code> , and <code>resume-threshold</code> parameters vary across interface types and port speeds. The default values are based on the default MTU size of 9216 bytes.
Example	<pre>OS10(config)# policy-map type network-qos pp1 OS10(conf-pmap-network-qos)# class cc1 OS10(conf-pmap-c-nqos)# pause buffer-size 30 pause-threshold 20 resume- threshold 10</pre>
Supported Releases	10.3.0E or later

pfc-cos

Configures the matching dot1p values used to send PFC pause frames.

Syntax	<code>pfc-cos dot1p-priority</code>
Parameters	<code>dot1p-priority</code> — Enter a single dot1p priority value for a PFC traffic class (1 to 7), a hyphen-separated range, or multiple dot1p values separated by commas.
Default	Not configured
Command Mode	POLICY-CLASS NETWORK-QOS
Usage Information	When you enter PFC-enabled dot1p priorities with <code>pfc-cos</code> , the dot1p values must be the same as the <code>match qos-group</code> (traffic class) numbers in the network-qos class map used to define the PFC traffic class (see <i>Configure PFC Example</i>). A <code>qos-group</code> number is used only internally to classify ingress traffic classes. See PFC configuration notes for the default dot1p-priority-to-traffic-class mapping and how to configure a non-default mapping. A PFC traffic class requires a 1-to-1 mapping — only one dot1p value is mapped to a <code>qos-group</code> number.
Example	<pre>OS10(config)# class-map type network-qos cc1 OS10(conf-cmap-nqos)# match qos-group 3 OS10(conf-cmap-nqos)# exit</pre>
Example (policy-map)	<pre>OS10(config)# policy-map type network-qos pp1 OS10(conf-pmap-network-qos)# class cc1 OS10(conf-pmap-c-nqos)# pfc-cos 3</pre>
Supported Releases	10.3.0E or later

pfc-shared-buffer-size

Configures the amount of shared buffers available for PFC-enabled traffic on the switch.

Syntax	<code>pfc-shared-buffer-size kilobytes</code>
Parameter	<code>kilobytes</code> — Enter the total amount of shared buffers available to PFC-enabled dot1p traffic in kilobytes (0 to 7787).
Default	832KB
Command Mode	SYSTEM-QOS
Usage Information	By default, all ingress traffic is handled by the lossy ingress buffer. When you enable PFC, dot1p ingress traffic competes for shared buffers in the lossless pool instead of the shared lossy pool. Use this command to increase or decrease the shared buffer allowed for PFC-enabled flows. The configured amount of shared buffers is reserved for PFC flows only after you enable PFC on an interface (<code>priority-flow-control</code> mode on command).

Example

```
OS10(config)# system qos
OS10(conf-sys-qos)# pause-shared-buffer-size 1024
```

Supported Releases 10.3.0E or later

priority-flow-control

Enables PFC on ingress interfaces.

Syntax `priority-flow-control {mode on}`

Parameter `mode on` — Enable PFC for FCoE and iSCSI traffic on an interface without enabling DCBX.

Default Disabled

Command Mode INTERFACE

Usage Information Before you enable PFC, apply a network-qos policy-class map with the specific PFC dot1p priority values to the interface. In the PFC network-qos policy-class map, use the default `buffer-size` values if you are not sure about the `pause-threshold`, and `resume-threshold` settings that you want to use. You cannot enable PFC and link-layer flow control (LLFC) at the same time on an interface. The `no` version of this command disables PFC on an interface. When you disable PFC, remove the PFC network-qos policy-class map applied to the interface.

Example

```
OS10(conf-if-eth1/1/1)# priority-flow-control mode on
```

Supported Releases 10.3.0E or later

queue-limit

Sets the static and dynamic thresholds used to limit the shared-buffer size of PFC traffic-class queues.

Syntax `queue-limit {thresh-mode [static kilobytes | dynamic weight]}`

Parameters

- `thresh-mode` — Buffer threshold mode.
- `static kilobytes` — Enter the fixed shared-buffer limit available for PFC traffic-class queues in kilobytes (0 to 7787; maximum amount tuned by the `pfc-shared-buffer-size` command).
- `dynamic weight` — Enter the weight value used to dynamically determine the shared-buffer limit available for PFC traffic-class queues (1 to 10).

Default Dynamic weight of 9 and static shared-buffer limit of 12479488 kilobytes

Command Mode POLICY-CLASS NETWORK-QOS

Usage Information To tune the amount of shared buffers available for the static limit of PFC traffic-class queues on the switch, use the `pfc-shared-buffer-size` command. The dynamic queue-limit is determined by the current amount of available shared buffers.

Example

```
OS10(config)# policy-map type network-qos pp1
OS10(conf-pmap-network-qos)# class ccl
OS10(conf-pmap-c-nqos)# queue-limit thresh-mode static 1024
```

Supported Releases 10.3.0E or later

show interface priority-flow-control

Displays PFC operational status, configuration, and statistics on an interface.

Syntax	<code>show interface [ethernet node/slot/port[:subport]] priority-flow-control [details]</code>
Parameters	None
Default	Not configured
Command Mode	EXEC
Usage Information	Use the <code>details</code> option to display PFC statistics on received/transmitted frames for each dot1p (CoS) value, and use the <code>clear qos statistics interface ethernet 1/1/1</code> command to delete PFC statistics and restart the counter.

Example (details)

```
OS10(config)# show interface ethernet 1/1/15 priority-flow-control
details

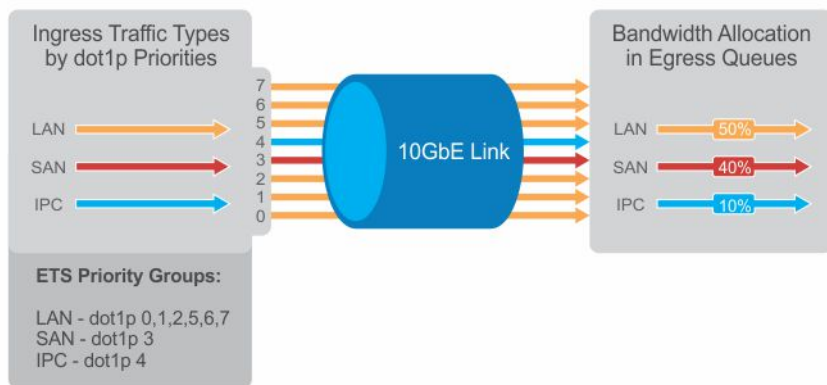
ethernet1/1/15
Admin Mode : true
Operstatus: true
PFC Priorities: 3
Total Rx PFC Frames: 0
Total Tx PFC frames: 587236
Cos      Rx      Tx
-----
0        0        0
1        0        0
2        0        0
3        0      587236
4        0        0
5        0        0
6        0        0
7        0        0
```

Supported Releases	10.3.0E or later
---------------------------	------------------

Enhanced transmission selection

Enhanced transmission selection (ETS) provides customized bandwidth allocation to 802.1p classes of traffic. Assign different amounts of bandwidth to traffic classes (Ethernet, FCoE, or iSCSI) that require different bandwidth, latency, and best-effort treatment during network congestion.

ETS divides traffic into different priority groups using their 802.1p priority value. To ensure that each traffic class is correctly prioritized and receives required bandwidth, configure bandwidth and queue scheduling for each priority group. You can allocate more bandwidth to a priority group to prioritize low-latency storage and server-cluster traffic. Allocate less bandwidth to a different priority group to rate-limit best-effort LAN traffic.



ETS configuration notes

- ETS is supported on L2 802.1p priority (dot1p 0 to 7) and L3 DSCP (0 to 63) traffic. FCoE traffic uses dot1p priority 3 — iSCSI storage traffic uses dot1p priority 4.
- Apply these maps and policies on interfaces:
 - Trust maps — OS10 interfaces do not honor the L2 and L3 priority fields in ingress traffic by default. Create a trust map to honor dot1p and DSCP classes of lossless traffic. A trust map does not change ingress dot1p and DSCP values in egress flows. In a trust map, assign a `qos-group` (traffic class) to trusted dot1p/DSCP values. A `qos-group` number is used only internally to schedule classes of ingress traffic.
 - QoS map — Create a QoS map to assign trusted dot1p and DSCP traffic classes to lossless queues.
 - Ingress trust policy — Configure a service policy to trust dot1p values in ingress traffic.
 - Egress queuing policy — Configure ETS for egress traffic by assigning bandwidth to matching lossless queues in queuing class and policy maps.
- Apply both PFC network-qos (input) and ETS queuing (output) policies on an interface to ensure lossless transmission.
- An ETS-enabled interface operates with dynamic weighted round robin (DWRR) or strict priority scheduling.
- OS10 control traffic is sent to control queues, which have a strict priority that is higher than data traffic queues. ETS-allocated bandwidth is not supported on a strict priority queue. A strict priority queue receives bandwidth only from DCBX TLVs.
- The CEE/IEEE2.5 versions of ETS TLVs are supported. ETS configurations are received in a TLV from a peer.

Configure ETS

ETS provides traffic prioritization for lossless storage, latency-sensitive, and best-effort data traffic on the same link.

- Configure classes of dot1p and DSCP traffic and assign them to lossless queues. Use the `class-trust` class map to honor ingress dot1p and DSCP traffic.
- Allocate guaranteed bandwidth to each lossless queue. An ETS queue can exceed the amount of allocated bandwidth if another queue does not use its share.

ETS is disabled by default on all interfaces.

- Configure trust maps of dot1p and DSCP values in CONFIGURATION mode. A trust map does not modify ingress values in output flows. Assign a `qos-group` (traffic class 0-7) to trusted dot1p/DSCP values in TRUST mode. A `qos-group` number is used only internally to schedule classes of ingress traffic. Enter multiple `dot1p` and `dscp` values in a hyphenated range or separated by commas.

```
trust dot1p-map dot1p-map-name
  qos-group {0-7} dot1p {0-7}
  exit
trust dscp-map dscp-map-name
  qos-group {0-7} dscp {0-63}
  exit
```

2. Configure a QoS map with trusted traffic-class (*qos-group*) to lossless-queue mapping in CONFIGURATION mode. Assign one or more qos-groups (0-7) to a specified queue in QOS-MAP mode. Enter multiple *qos-group* values in a hyphenated range or separated by commas. Enter multiple *queue qos-group* entries, if necessary.

```
qos-map traffic-class queue-map-name
  queue {0-7} qos-group {0-7}
exit
```

3. Apply the default trust map specifying that dot1p and dscp values are trusted in SYSTEM-QOS or INTERFACE mode.

```
trust-map {dot1p | dscp} default
```

4. Create a queuing class map for each ETS queue in CONFIGURATION mode. Enter *match queue* criteria in CLASS-MAP mode.

```
class-map type queuing class-map-name
  match queue {0-7}
exit
```

5. Create a queuing policy map in CONFIGURATION mode. Enter POLICY-CLASS-MAP mode and configure the percentage of bandwidth allocated to each traffic class-queue mapping. The sum of all DWRR-allocated bandwidth across ETS queues must be 100% (not including the strict priority queue). Otherwise, QoS automatically adjusts bandwidth percentages so that ETS queues always receive 100% bandwidth. The remaining non-ETS queues receive 1% bandwidth each.

```
policy-map type queuing policy-map-name
  class class-map-name
    bandwidth percent {1-100}
```

(Optional) To configure a queue as strict priority, use the *priority* command. Packets scheduled to a strict priority queue are transmitted before packets in non-priority queues.

```
policy-map type queuing policy-map-name
  class class-map-name
    priority
```

6. Apply the trust maps for dot1p and DSCP values, and the traffic class-queue mapping globally on the switch in SYSTEM-QOS mode or on an interface or interface range in INTERFACE mode.

```
system qos
  trust-map dot1p dot1p-map-name
  trust-map dscp dscp-map-name
  qos-map traffic-class queue-map-name
```

Or

```
interface {ethernet node/slot/port[:subport] | range ethernet node/slot/
port[:subport]-node/slot/port[:subport]}
  trust-map dot1p dot1p-map-name
  trust-map dscp dscp-map-name
  qos-map traffic-class queue-map-name
```

7. Apply the qos trust policy to ingress traffic in SYSTEM-QOS or INTERFACE mode.

```
service-policy input type qos trust-policy-map-name
```

8. Apply the queuing policy to egress traffic in SYSTEM-QOS or INTERFACE mode.

```
service-policy output type queuing policy-map-name
```

9. Enable ETS globally in SYSTEM-QOS mode or on an interface/interface range in INTERFACE mode.

```
ets mode on
```

Configure ETS

```
OS10(config)# trust dot1p-map dot1p_map1
OS10(config-trust-dot1pmap)# qos-group 0 dot1p 0-3
OS10(config-trust-dot1pmap)# qos-group 1 dot1p 4-7
OS10(config-trust-dot1pmap)# exit

OS10(config)# trust dscp-map dscp_map1
OS10(config-trust-dscpmap)# qos-group 0 dscp 0-31
OS10(config-trust-dscpmap)# qos-group 1 dscp 32-63
OS10(config-trust-dscpmap)# exit

OS10(config)# qos-map traffic-class tc-q-map1
OS10(config-qos-tcmap)# queue 0 qos-group 0
OS10(config-qos-tcmap)# queue 1 qos-group 1
OS10(config-qos-tcmap)# exit

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p default

OS10(config)# class-map type queuing c1
OS10(config-cmap-queuing)# match queue 0
OS10(config-cmap-queuing)# exit
OS10(config)# class-map type queuing c2
OS10(config-cmap-queuing)# match queue 1
OS10(config-cmap-queuing)# exit

OS10(config)# policy-map type queuing p1
OS10(config-pmap-queuing)# class c1
OS10(config-pmap-queuing)# bandwidth percent 30
OS10(config-pmap-queuing)# exit
OS10(config)# policy-map type queuing p2
OS10(config-pmap-queuing)# class c2
OS10(config-pmap-queuing)# bandwidth percent 70
OS10(config-pmap-queuing)# exit

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p dot1p_map1
OS10(config-sys-qos)# trust-map dscp dscp_map1
OS10(config-sys-qos)# qos-map traffic-class tc-q-map1
OS10(config-sys-qos)# ets mode on
OS10(config-sys-qos)# service-policy input type qos pclass1
OS10(config-sys-qos)# service-policy output type queuing p1
```

View ETS configuration

```
OS10# show qos interface ethernet 1/1/1
Interface
unknown-unicast-storm-control : Disabled
multicast-storm-control : Disabled
broadcast-storm-control : Disabled
flow-control-rx : Disabled
flow-control-tx : Disabled
ets mode : Disabled
Dot1p-tc-mapping : dot1p_map1
Dscp-tc-mapping : dscp_map1
tc-queue-mapping : tc-q-map1
```

View QoS maps: traffic-class to queue mapping

```
OS10# show qos maps
Traffic-Class to Queue Map: tc-q-map1
  queue 0 qos-group 0
  queue 1 qos-group 1
Traffic-Class to Queue Map: dot1p_map1
  qos-group 0 dot1p 0-3
  qos-group 1 dot1p 4-7
DSCP Priority to Traffic-Class Map : dscp_map1
  qos-group 0 dscp 0-31
  qos-group 1 dscp 32-63
```

ETS commands

ets mode on

Enables ETS on an interface.

Syntax ets mode on

Parameter None

Default Disabled

Command Mode INTERFACE

Usage Information Enable ETS on all switch interfaces in SYSTEM-QOS mode or on an interface or interface range in INTERFACE mode. The no version of this command disables ETS.

Example

```
OS10(config-sys-qos)# ets mode on
```

Supported Releases 10.3.0E or later

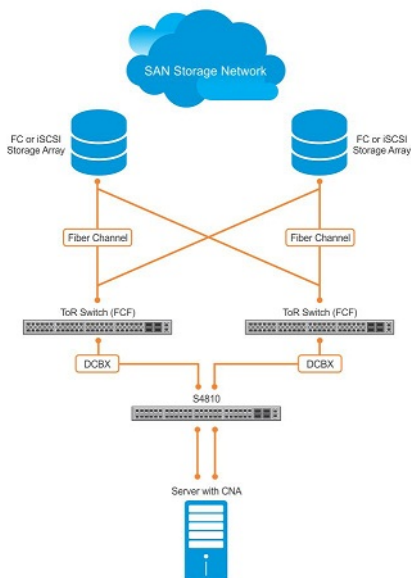
Data center bridging eXchange

DCBX allows a switch to automatically discover and set up DCBX-enabled peers configured with compatible settings. In a converged data center network, DCBX provides plug-and-play capability for server, storage, and networking devices in an end-to-end solution.

DCBX uses LLDP to mediate the automatic negotiation and exchange of device settings, such as PFC and ETS. DCBX uses LLDP TLVs to perform DCB parameter exchange:

- PFC configuration and application priority configuration
- ETS configuration and ETS recommendation

This sample DCBX topology shows two 40GbE ports on a switch that are configured as DCBX auto-upstream ports and used as uplinks to top-of-rack (ToR) switches. The top-of-rack (ToR) switches are part of a fibre channel storage network.



DCBX configuration notes

- To exchange link-level configurations in a converged network, DCBX is a prerequisite for using DCB features, such as PFC and ETS. DCBX is also deployed in topologies that support lossless operation for FCoE or iSCSI traffic. In these scenarios, all network devices must be DCBX-enabled so that DCBX is enabled end-to-end.
- DCBX uses LLDP to advertise and automatically negotiate the administrative state and PFC/ETS configuration with directly connected DCB peers. If you disable LLDP on an interface, DCBX cannot run. Enable LLDP on all DCBX ports.
- DCBX is disabled at a global level by default. Enable DCBX globally on a switch to activate the exchange of DCBX TLV messages with PFC, ETS, and iSCSI configurations.
- DCBX is enabled by default on OS10 interfaces. You can manually reconfigure DCBX settings on a per-interface basis. For example, you can disable DCBX on an interface (`no lldp tlv-select dcbxp` command) or change the DCBX version (`dcbx version` command).
- For DCBX to be operational, DCBX must be enabled at both the global and interface levels. If the `show lldp dcbx interface` command returns the message `DCBX feature not enabled`, DCBX is not enabled at both levels.
- OS10 supports DCBX versions: CEE and IEEE2.5.
- By default, DCBX advertises all TLVs—PFC, ETS Recommendation, ETS Configuration, DCBXP, and basic TLVs.
- A DCBX-enabled port operates in a manual role by default. The port operates only with user-configured settings and does not auto-configure with DCB settings received from a DCBX peer. When you enable DCBX, the port advertises its PFC and ETS configurations to peer devices but does not accept external, or propagate internal, DCB configurations.
- DCBX detects misconfiguration on a peer device when DCB features are not compatibly configured with the local switch. Misconfiguration detection is feature-specific because some DCB features support asymmetric (non-identical) configurations.

Configure DCBX

DCBX allows data center devices to advertise and exchange configuration settings with directly connected peers using LLDP. LLDP is enabled by default.

To ensure the consistent and efficient operation of a converged data center network, DCBX detects peer misconfiguration.

DCBX is disabled at a global level and enabled at an interface level by default. For DCBX to be operational, DCBX must be enabled at both the global and interface levels. You can manually reconfigure DCBX settings or disable DCBX on a per-interface basis.

1. Configure the DCBX version used on a port in INTERFACE mode.

```
dcbx version {auto | cee | ieee}
```

- `auto` — Automatically selects the DCBX version based on the peer response (default).
 - `cee` — Sets the DCBX version to CEE.
 - `ieee` — Sets the DCBX version to IEEE 802.1Qaz.
2. (Optional) A DCBX-enabled port advertises all TLVs by default. If PFC or ETS TLVs are disabled, enter the command in INTERFACE mode to re-enable PFC or ETS TLV advertisements.

```
dcbx tlv-select {ets-conf | ets-reco | pfc}
```

- `ets-conf` — Enables ETS configuration TLVs.
 - `ets-reco` — Enables ETS recommendation TLVs.
 - `pfc` — Enables PFC TLVs.
3. (Optional) DCBX is enabled on a port by default. If DCBX is disabled, enable it in INTERFACE mode.

```
lldp tlv-select dcbxp
```

4. Return to CONFIGURATION mode.

```
exit
```

5. Enable DCBX on all switch ports in CONFIGURATION mode to activate the exchange of DCBX TLV messages with PFC, ETS, and iSCSI configurations.

```
dcbx enable
```

Configure DCBX

View DCBX configuration

```
OS10# show lldp dcbx interface ethernet 1/1/15

E-ETS Configuration TLV enabled           e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled          r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled           p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled    f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled    i-Application Priority for iSCSI disabled
-----
-

Interface ethernet1/1/15
  Port Role is Manual
  DCBX Operational Status is Enabled
  Is Configuration Source? FALSE
  Local DCBX Compatibility mode is CEE
  Local DCBX Configured mode is CEE
  Peer Operating version is CEE
  Local DCBX TLVs Transmitted: ErPFI

Local DCBX Status
-----
DCBX Operational Version is 0
DCBX Max Version Supported is 0
Sequence Number: 14
Acknowledgment Number: 5
Protocol State: In-Sync

Peer DCBX Status
-----
DCBX Operational Version is 0
DCBX Max Version Supported is 255
Sequence Number: 5
Acknowledgment Number: 14
  220 Input PFC TLV pkts, 350 Output PFC TLV pkts, 0 Error PFC pkts
  220 Input PG TLV Pkts, 396 Output PG TLV Pkts, 0 Error PG TLV Pkts
  71 Input Appln Priority TLV pkts, 80 Output Appln Priority TLV pkts, 0 Error Appln
Priority TLV Pkts

Total DCBX Frames transmitted 538
Total DCBX Frames received 220
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0
```

View DCBX PFC TLV status

```
OS10# show lldp dcbx interface ethernet 1/1/15 pfc detail

Interface ethernet1/1/15
  Admin mode is on
  Admin is enabled, Priority list is 4,5,6,7
  Remote is enabled, Priority list is 4,5,6,7
  Remote Willing Status is disabled
  Local is enabled, Priority list is 4,5,6,7
  Oper status is init
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  PFC TLV Tx Status is enabled
  Application Priority TLV Parameters :
  -----
  ISCSI TLV Tx Status is enabled
  Local ISCSI PriorityMap is 0x10
  Remote ISCSI PriorityMap is 0x10

  220 Input TLV pkts, 350 Output TLV pkts, 0 Error pkts
  71 Input Appln Priority TLV pkts, 80 Output Appln Priority TLV pkts, 0 Error Appln
Priority TLV Pkts
```

View DCBX ETS TLV status

```
OS10# show lldp dcbx interface ethernet 1/1/15 ets detail
```

```
Interface ethernet1/1/15
Max Supported PG is 8
Number of Traffic Classes is 8
Admin mode is on
```

```
Admin Parameters :
```

```
-----
Admin is enabled
```

PG-grp	Priority#	Bandwidth	TSA
0	0,1,2,3	70%	ETS
1	4,5,6,7	30%	ETS
2		0%	SP
3		0%	SP
4		0%	SP
5		0%	SP
6		0%	SP
7		0%	SP
15		0%	SP

```
Remote Parameters :
```

```
-----
Remote is enabled
```

PG-grp	Priority#	Bandwidth	TSA
0	0,1,2,3	70%	ETS
1	4,5,6,7	30%	ETS
2		0%	SP
3		0%	SP
4		0%	SP
5		0%	SP
6		0%	SP
7		0%	SP
15		0%	SP

```
Remote Willing Status is disabled
```

```
Local Parameters :
```

```
-----
Local is enabled
```

PG-grp	Priority#	Bandwidth	TSA
0	0,1,2,3	70%	ETS
1	4,5,6,7	30%	ETS
2		0%	SP
3		0%	SP
4		0%	SP
5		0%	SP
6		0%	SP
7		0%	SP
15		0%	SP

```
Oper status is init
ETS DCBX Oper status is Up
State Machine Type is Feature
Conf TLV Tx Status is enabled
Reco TLV Tx Status is disabled
```

```
220 Input Conf TLV Pkts, 396 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
```


DCBX commands

dcbx enable

Enables DCBX globally on all port interfaces.

Syntax `dcbx enable`

Parameters None

Default Disabled

Command Mode CONFIGURATION

Usage Information DCBX is disabled at a global level and enabled at an interface level by default. For DCBX to be operational, DCBX must be enabled at both the global and interface levels. Enable DCBX globally with the `dcbx enable` command to activate the exchange of DCBX TLV messages with PFC, ETS, and iSCSI configurations. Use DCBX interface-level commands to configure the TLVs advertised by a DCBX-enabled port, change the DCBX version, or disable DCBX on an interface. DCBX allows peers to advertise DCB configuration using LLDP and self-configure with compatible settings. If you disable DCBX globally on a switch, you can re-enable it to ensure consistent operation of peers in a converged data center network.

Example

```
OS10(config)# dcbx enable
```

Supported Releases 10.3.0E or later

dcbx tlv-select

Configures the DCB TLVs advertised by a DCBX-enabled port.

Syntax `dcbx tlv-select {[ets-conf] [ets-reco] [pfc]}`

Parameters

- `ets-conf` — Advertise ETS configuration TLVs.
- `ets-reco` — Advertise ETS recommendation TLVs.
- `pfc` — Advertise PFC TLVs.

Default DCBX advertises PFC, ETS Recommendation, and ETS Configuration TLVs.

Command Mode INTERFACE

Usage Information A DCBX-enabled port advertises all TLVs to DCBX peers by default. If PFC or ETS TLVs are disabled, enter the command to re-enable PFC or ETS TLV advertisements. You can enable multiple TLV options (`ets-conf`, `ets-reco`, and `pfc`) with the same command.

Example

```
OS10(config-if-eth1/1/2)# dcbx tlv-select ets-conf pfc
```

Supported Releases 10.3.0E or later

dcbx version

Configures the DCBX version used on a port interface.

Syntax `dcbx version {auto | cee | ieee}`

Parameters

- `auto` — Automatically select the DCBX version based on the peer response.
- `cee` — Set the DCBX version to CEE.
- `ieee` — Set the DCBX version to IEEE 802.1Qaz.

Default Auto

Command Mode INTERFACE

Usage Information In auto mode, a DCBX-enabled port detects an incompatible DCBX version on a peer device port and automatically reconfigures a compatible version on the local port. The `no` version of this command disables the DCBX version.

Example

```
OS10(conf-if-eth1/1/2)# dcbx version cee
```

Supported Releases 10.3.0E or later

lldp tlv-select dcbxp

Enables and disables DCBX on a port interface.

Syntax `lldp tlv-select dcbxp`

Parameters None

Default Enabled interface level; disabled global level

Command Mode INTERFACE

Usage Information DCBX must be enabled at both the global and interface levels. Enable DCBX globally with the `dcbx enable` command to activate the exchange of DCBX TLV messages with PFC, ETS, and iSCSI configurations. Use DCBX interface-level commands to configure the TLVs advertised by a DCBX-enabled port, change the DCBX version, or disable DCBX on an interface. The `no` version of this command disables DCBX on an interface.

Example

```
OS10(conf-if-eth1/1/1)# lldp tlv-select dcbxp
```

Supported Releases 10.3.0E or later

show lldp dcbx interface

Displays DCBX configuration and PFC or ETS TLV status on an interface.

Syntax `show lldp dcbx interface ethernet node/slot/port[:subport] [ets detail | pfc detail]`


Parameters

- `interface ethernet node/slot/port[:subport]` — Enter interface information.
- `ets detail` — Display ETS TLV status and operation with DCBX peers.
- `pfc detail` — Display PFC TLV status and operation with DCBX peers.

Default Not configured

Command Mode EXEC

Usage Information DCBX must be enabled before using this command. DCBX advertises all TLVs — PFC, ETS Recommendation, ETS Configuration, DCBXP, and basic TLVs by default. Enter a port range to display DCBX configuration and TLV operation on multiple ports.

 **NOTE:** In the command output, the `Is configuration source` parameter always displays `False`.
Configuration source is type of port role that is not supported.

Example (interface)

```
OS10# show lldp dcbx interface ethernet 1/1/15
E-ETS Configuration TLV enabled          e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled         r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled          p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled   f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled  i-Application Priority for iSCSI disabled
-----
Interface ethernet1/1/15
Port Role is Manual
```

```

DCBX Operational Status is Enabled
Is Configuration Source? FALSE
Local DCBX Compatibility mode is IEEEv2.5
Local DCBX Configured mode is IEEEv2.5
Peer Operating version is IEEEv2.5
Local DCBX TLVs Transmitted: ERPFi
  5 Input PFC TLV pkts, 2 Output PFC TLV pkts, 0 Error PFC pkts
  5 Input ETS Conf TLV Pkts, 2 Output ETS Conf TLV Pkts, 0 Error ETS Conf TLV
Pkts
  5 Input ETS Reco TLV pkts, 2 Output ETS Reco TLV pkts, 0 Error ETS Reco TLV
Pkts
  5 Input Appln Priority TLV pkts, 2 Output Appln Priority TLV pkts, 0 Error
Appln Priority TLV Pkts

Total DCBX Frames transmitted 8
Total DCBX Frames received 20
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0

```

Example (ETS detail)

```

OS10# show lldp dcbx interface ethernet 1/1/15 ets detail
Interface ethernet1/1/15
Max Supported PG is 8
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :
-----
Admin is enabled

PG-grp      Priority#      Bandwidth      TSA
-----
0           0,1,2,3       70%            ETS
1           4,5,6,7       30%            ETS
2           0%            SP
3           0%            SP
4           0%            SP
5           0%            SP
6           0%            SP
7           0%            SP

Remote Parameters :
-----
Remote is enabled
PG-grp      Priority#      Bandwidth      TSA
-----
0           0,1,2,3       70%            ETS
1           4,5,6,7       30%            ETS
2           0%            SP
3           0%            SP
4           0%            SP
5           0%            SP
6           0%            SP
7           0%            SP

Remote Willing Status is disabled
Local Parameters :
-----
Local is enabled

PG-grp      Priority#      Bandwidth      TSA
-----
0           0,1,2,3       70%            ETS
1           4,5,6,7       30%            ETS
2           0%            SP
3           0%            SP
4           0%            SP
5           0%            SP
6           0%            SP
7           0%            SP

```

```

Oper status is init
ETS DCBX Oper status is Up
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled

5 Input Conf TLV Pkts, 2 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
5 Input Reco TLV Pkts, 2 Output Reco TLV Pkts, 0 Error Reco TLV Pkts

```

Example (PFC detail)

```

OS10# show lldp dcbx interface ethernet 1/1/15 pfc detail
Interface ethernet1/1/15
  Admin mode is on
  Admin is enabled, Priority list is 4,5,6,7
  Remote is enabled, Priority list is 4,5,6,7
  Remote Willing Status is disabled
  Local is enabled, Priority list is 4,5,6,7
  Oper status is init
  PFC DCBX Oper status is Up
  State Machine Type is Symmetric
  PFC TLV Tx Status is enabled
  Application Priority TLV Parameters :
  -----
  ISCSI TLV Tx Status is enabled
  Local ISCSI PriorityMap is 0x10
  Remote ISCSI PriorityMap is 0x10

  5 Input TLV pkts, 2 Output TLV pkts, 0 Error pkts
  5 Input Appln Priority TLV pkts, 2 Output Appln Priority TLV pkts, 0 Error
  Appln Priority TLV Pkts

```

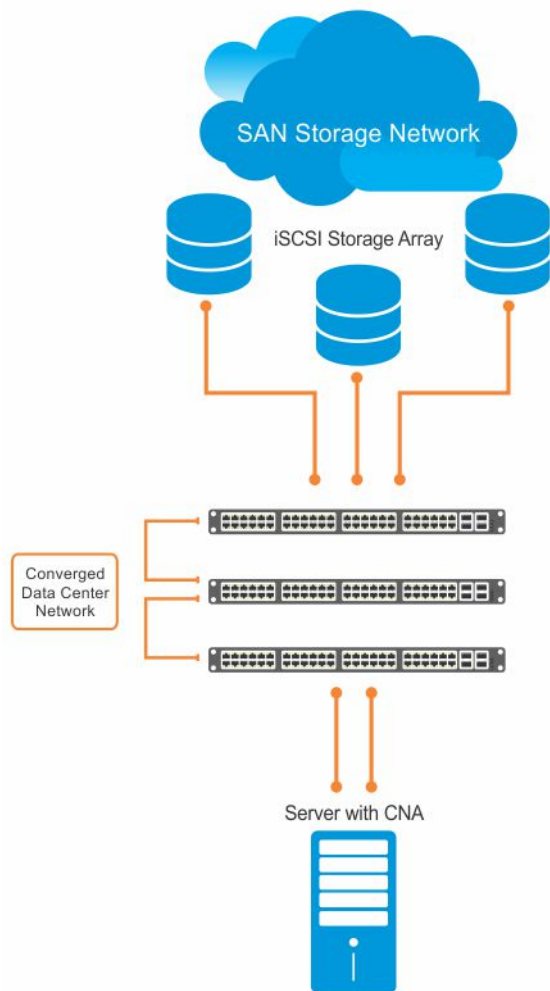
Supported Releases 10.3.0E or later

Internet small computer system interface

iSCSI is a TCP/IP-based protocol for establishing and managing connections between servers and storage devices in a data center network. After you enable iSCSI, iSCSI optimization automatically detects Dell EqualLogic storage arrays directly attached to switch ports. To support storage arrays where auto-detection is not supported, manually configure iSCSI optimization using the `iscsi profile-storage name` command.

iSCSI optimization enables a switch to auto-detect Dell's iSCSI storage arrays and auto-configure switch ports to improve storage traffic throughput. The switch monitors iSCSI sessions and applies QoS policies on iSCSI traffic. iSCSI optimization operates with or without DCBX over an Ethernet network.

- iSCSI uses the current flow-control configuration by default. If you do not configure flow-control, iSCSI auto-configures flow control settings so that receive-only is enabled and transmit-only is disabled.
- The switch monitors and tracks active iSCSI sessions, including port information and iSCSI session information.
- A user-configured iSCSI class of service (CoS) profile is applied to all iSCSI traffic. Classifier rules are used to direct the iSCSI data traffic to queues with preferential QoS treatment over other data passing through the switch. Preferential treatment helps to avoid session interruptions during times of congestion that would otherwise cause dropped iSCSI packets.



In an iSCSI session, a switch connects CNA servers (iSCSI initiators) to a storage array (iSCSI targets) in a storage area network (SAN) or TCP/IP network. iSCSI optimization running on the switch uses dot1p priority-queue assignments to ensure that iSCSI traffic receives priority treatment.

iSCSI configuration notes

- When you enable iSCSI optimization, the switch auto-detects and auto-configures for Dell EqualLogic storage arrays directly connected to an interface. iSCSI automatically configures switch parameters after connection to a storage device is verified. You must manually enable an interface to support a storage device that is directly connected to a port, but not automatically detected by iSCSI.
- By default, iSCSI monitoring sessions listen on TCP ports 860 and 3260. Enable iSCSI session monitoring and the aging time for iSCSI sessions.
- Configure the CoS/DSCP values applied to ingress iSCSI flows — create a `class-iscsi` class map in POLICY-CLASS-MAP mode.
- iSCSI operation requires LLDP to be enabled. The DCBX application TLV carries information about the dot1p priorities to use when sending iSCSI traffic. This informational TLV is packaged in LLDP PDUs. You can reconfigure the 802.1p priority bits advertised in the TLVs.

Configure iSCSI optimization

The iSCSI protocol provides TCP/IP transport of storage traffic between servers and storage arrays in a network using iSCSI commands.

1. Configure an interface or interface range to detect a connected storage device.

```
interface ethernet node/slot/port:[subport]
interface range ethernet node/slot/port:[subport]-node/slot/port[:subport]
```

2. Enable the interface to support a storage device that is directly connected to the port and not automatically detected by iSCSI. Use this command for storage devices that do not support LLDP. The switch auto-detects and auto-configures Dell EqualLogic storage arrays directly connected to an interface when you enable iSCSI optimization.

```
iscsi profile-storage storage-device-name
```

3. Configure DCBX to use LLDP to send iSCSI application TLVs with the dot1p priorities for iSCSI traffic in INTERFACE mode.

```
lldp tlv-select dcbxp-appln iscsi
```

4. Return to CONFIGURATION mode.

```
exit
```

5. (Optional) If necessary, re-configure the iSCSI TCP ports and IP addresses of target storage devices in CONFIGURATION mode. Separate TCP port numbers with a comma (0-65535; default 860 and 3260).

```
iscsi target port tcp-port1 [tcp-port2, ..., tcp-port16] [ip-address ip-address]
```

6. Configure the QoS policy applied to the ingress iSCSI flows. Apply the service policy to ingress interfaces in CONFIGURATION mode.

(Optional) Reset the default CoS dot1p priority (default 4) and/or the trusted DCSP value used for iSCSI traffic. Assign an internal qos-group queue (0 to 7) to dot1p (0 to 7) and DSCP (0 to 63) values in POLICY-CLASS-MAP mode.

```
class-map type application class-iscsi
policy-map type application policy-iscsi
  class class-iscsi
    set qos-group traffic-class-number
    set cos dot1p-priority
    set dscp dscp-value
  end
service-policy type application policy-iscsi
```

7. Enable iSCSI monitoring sessions on TCP ports in CONFIGURATION mode.

```
iscsi session-monitoring enable
```

8. (Optional) Set the aging time for the length of iSCSI monitoring sessions in CONFIGURATION mode (5 to 43,200 minutes; default 10).

```
iscsi aging time [minutes]
```

9. (Optional) Reconfigure the dot1p priority bits advertised in iSCSI application TLVs in CONFIGURATION mode. The default bitmap is 0x10 (dot1p 4). The default dot1p 4 value is sent in iSCSI application TLVs only if you enabled the PFC pause for dot1p 4 traffic (pfc-cos dot1p-priority command).

If you do not configure an `iscsi priority-bits dot1p` value and you configure a `set cos` value in Step 6, the `set cos` value is sent in iSCSI application TLVs. If you configure neither the `iscsi priority-bits` nor the `set cos` value, the default dot1p 4 is advertised.

```
iscsi priority-bits dot1p-bitmap
```

10. Enable iSCSI auto-detection and auto-configuration on the switch in CONFIGURATION mode.

```
iscsi enable
```

Configure iSCSI optimization

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# iscsi profile-storage compellent
OS10(conf-if-eth1/1/1)# lldp tlv-select dcbxp-appln iscsi
OS10(conf-if-eth1/1/1)# exit
```

```

OS10(config)# iscsi target port 3261 ip-address 10.1.1.1
OS10(config)# policy-map type application policy-iscsi
OS10(config-pmap-application)# class class-iscsi
OS10 (config-pmap-c-app)# set qos-group 4
OS10 (config-pmap-c-app)# set cos 4
OS10 (config-pmap-c-app)# exit
OS10(config-pmap-application)# exit

OS10(config)# system qos
OS10(config-sys-qos)# service-policy type application policy-iscsi
OS10(config-sys-qos)# exit

OS10(config)# iscsi session-monitoring enable
OS10(config)# iscsi aging time 15
OS10(config)# iscsi priority-bits 0x20
OS10(config)# iscsi enable

```

View iSCSI optimization

```

OS10# show iscsi
iSCSI Auto configuration is Enabled
iSCSI session monitoring is Enabled
iSCSI COS                qos-group 4 remark dot1p 4
Session aging time      15
Maximum number of connections is 100
Port      IP Address
-----
3260
860
3261      10.1.1.1

```

```

OS10# show iscsi session detailed
Session 1
-----
Target:iqn.2001-05.com.equallogic:0-8a0906-00851a00c-98326939fba510a1-517
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:18:12(DD:HH:MM:SS)
Time for aging out:29:23:59:35(DD:HH:MM:SS)
ISID:400001370000
Initiator      Initiator  Target      Target      Connection
IP Address     TCP Port   IP Address   TCP Port    ID
-----
10.10.10.210  54748     10.10.10.40  3260       1

Session 2
-----
Target:iqn.2001-05.com.equallogic:0-8a0906-01251a00c-8ab26939fbd510a1-518
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:16:02(DD:HH:MM:SS)
Time for aging out:29:23:59:35(DD:HH:MM:SS)
ISID:400001370000
Initiator      Initiator  Target      Target      Connection
IP Address     TCP Port   IP Address   TCP Port    ID
-----
10.10.10.210  54835     10.10.10.40  3260       1

```

```

OS10# show iscsi storage-devices
Interface Name  Storage Device Name  Auto Detected Status
-----
ethernet1/1/23  EQL-MEM              true

```

iSCSI synchronization on VLT

An iSCSI session is considered to be learnt on VLT LAG during the following scenarios:

- If the iSCSI session receives control packets, as login-request or login-response, on the VLT LAG.
- If the iSCSI session does not receive control packets, but receives data packets on the VLT LAG. This happens when iSCSI session monitoring is enabled after the iSCSI session has started.

The information learnt about iSCSI sessions on VLT LAGs are synchronized with the VLT peers.

The synchronization of the iSCSI sessions happens based on various scenarios:

- If the iSCSI login request is received on an interface that belongs to a VLT LAG, the information is synchronized with the VLT peer and the connection is associated with the interface.
- Any additional updates to connections, including aging updates, that are learnt on VLT LAG members are synchronized with the VLT peer.
- If the iSCSI login request is received on a non-VLT interface, followed by a response from a VLT interface, then the connection is associated with the VLT LAG interface and the information about the session is synchronized with the VLT peer.
- When VLT interconnect comes up, information about iSCSI sessions learnt on VLT LAG is exchanged between the VLT-peers.

iSCSI commands

iscsi aging

Sets the aging time for monitored iSCSI sessions.

Syntax	<code>iscsi aging [time minutes]</code>
Parameters	<code>time minutes</code> — Enter the aging time in minutes allowed for monitoring iSCSI sessions (5 to 43,200).
Default	10 minutes
Command Mode	CONFIGURATION
Usage Information	Configure the aging time allowed for monitored iSCSI sessions on TCP ports before the session closes. The <code>no</code> version of this command disables the aging time.
Example	<pre>OS10(config)# iscsi aging time 30</pre>
Supported Releases	10.3.0E or later

iscsi enable

Enables iSCSI auto-detection of attached storage arrays and switch auto-configuration.

Syntax	<code>iscsi enable</code>
Parameter	None
Default	Enabled on S4048T-ON/S4048-ON; disabled on others
Command Mode	CONFIGURATION
Usage Information	iSCSI optimization automatically detects storage arrays and auto-configures switch ports with the iSCSI parameters received from a connected device. The <code>no</code> version of this command disables iSCSI auto-detection.
Example	<pre>OS10(config)# iscsi enable</pre>
Supported Releases	10.3.0E or later

iscsi priority-bits

Resets the priority bitmap advertised in iSCSI application TLVs.

Syntax	<code>iscsi priority-bits {priority-bitmap}</code>
---------------	--

Parameter	<i>priority-bitmap</i> — Enter a bitmap value for the dot1p priority advertised for iSCSI traffic in iSCSI application TLVs (0x1 to 0xff).
Default	0x10 (dot1p 4)
Command Mode	CONFIGURATION
Usage Information	iSCSI traffic uses dot1p priority 4 in frame headers by default. Use this command to reconfigure the dot1p-priority bits advertised in iSCSI application TLVs. Enter only one dot1p-bitmap value — setting more than one bitmap value with this command is not supported. The default dot1p 4 value is advertised only if you enabled PFC pause frames for dot1p 4 traffic (<i>pfc-cos dot1p-priority</i> command). The <i>no</i> version of this command resets to the default value.
Example	<pre>OS10(config)# iscsi priority-bits 0x20</pre>
Supported Releases	10.3.0E or later


iscsi profile-storage

Configures a port for direct connection to a storage device that is not automatically detected by iSCSI.

Syntax	<i>iscsi profile-storage storage-device-name</i>
Parameter	<i>storage-device-name</i> — Enter a user-defined name of a storage array that iSCSI does not automatically detect.
Default	Not configured
Command Mode	INTERFACE
Usage Information	Configure directly attached storage arrays to be supported by iSCSI if they are not automatically detected. This command is required for storage devices that do not support LLDP. The <i>no</i> version of this command disables the connection.
Example	<pre>OS10(conf-if-eth1/1/2)# iscsi profile-storage compellant</pre>
Supported Releases	10.3.0E or later

iscsi session-monitoring enable

Enables iSCSI session monitoring.

Syntax	<i>iscsi session-monitoring enable</i>
Parameter	None
Default	Disabled
Command Mode	CONFIGURATION
Usage Information	Use the <i>iscsi aging time</i> command to configure the aging timeout in iSCSI monitoring sessions, and use the <i>iscsi target port</i> command to configure the TCP ports that listen for connected storage devices in iSCSI monitoring sessions. The <i>no</i> version of this command disables iSCSI session monitoring.
	 NOTE: When iSCSI session monitoring is enabled, you can monitor a maximum of 100 connections.
Example	<pre>OS10(config)# iscsi session-monitoring enable</pre>
Supported Releases	10.3.0E or later

iscsi target port

Configures the TCP ports used to monitor iSCSI sessions with target storage devices.

Syntax	<code>iscsi target port tcp-port1 [tcp-port2, ..., tcp-port16] [ip-address ip-address]</code>
Parameters	<ul style="list-style-type: none">• <code>tcp-port</code> — Enter one or more TCP port numbers (0 to 65535). Separate TCP port numbers with a comma.• <code>ip-address ip-address</code> — (Optional) Enter the IP address in A.B.C.D format of a storage array whose iSCSI traffic is monitored on the TCP port.
Default	3260,860
Command Mode	CONFIGURATION
Usage Information	You can configure up to 16 TCP ports to monitor iSCSI traffic from target storage devices. The no version of this command including the IP address removes a TCP port from iSCSI monitoring.
Example	<pre>OS10(config)# iscsi target port 26,40</pre>
Supported Releases	10.3.0E or later

lldp tlv-select dcbxp-appln iscsi

Enables a port to advertise iSCSI application TLVs to DCBX peers.

Syntax	<code>lldp tlv-select dcbxp-appln iscsi</code>
Parameter	None
Default	iSCSI application TLVs are advertised to DCBX peers.
Command Mode	INTERFACE
Usage Information	DCB devices use DCBX to exchange iSCSI configuration information with peers and self-configure. iSCSI parameters are exchanged in time, length, and value (TLV) messages. DCBX requires LLDP enabled to advertise iSCSI application TLVs. iSCSI application TLVs advertise the PFC dot1p priority-bitmap configured with the <code>iscsi priority-bits</code> command to DCBX peers. If you do not configure an iSCSI dot1p-bitmap value, iSCSI application TLVs advertise dot1p 4 by default only if you configure dot1p 4 as a PFC priority with the <code>pfc-cos</code> command. The <code>no</code> version of this command disables iSCSI TLV transmission.
Example	<pre>OS10(conf-if-eth1/1/1)# lldp tlv-select dcbxp-appln iscsi</pre>
Supported Releases	10.3.0E or later

show iscsi

Displays currently configured iSCSI settings.

Syntax	<code>show iscsi</code>
Parameters	None
Command Mode	EXEC
Usage Information	This command output displays global iSCSI configuration settings. Use the <code>show iscsi session</code> command to view target and initiator information.
Example	<pre>OS10# show iscsi iSCSI Auto configuration is Enabled</pre>

```
iSCSI session monitoring is Enabled
iSCSI COS                qos-group 4 remark dot1p 4
Session aging time       15
Maximum number of connections is 100
Port      IP Address
-----
3260
860
3261      10.1.1.1
```

Supported Releases 10.3.0E or later

show iscsi session

Displays information about active iSCSI sessions.

Syntax `show iscsi session [detailed]`

Parameter `detailed` — Displays a detailed version of the active iSCSI sessions.

Command Mode EXEC

Usage Information In an iSCSI session, `Target` is the storage device, and `Initiator` is the server connected to the storage device.

Example

```
OS10# show iscsi session
```

Example (detailed)

```
OS10# show iscsi session detailed
Session 1
-----
Target:iqn.2001-05.com.equallogic:0-8a0906-00851a00c-98326939fba510a1-517
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:18:12 (DD:HH:MM:SS)
Time for aging out:29:23:59:35 (DD:HH:MM:SS)
ISID:400001370000
Initiator      Initiator      Target          Target          Connection
IP Address     TCP Port       IP Address      TCP Port        ID
-----
10.10.10.210  54748         10.10.10.40    3260            1

Session 2
-----
Target:iqn.2001-05.com.equallogic:0-8a0906-01251a00c-8ab26939fbd510a1-518
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:16:02 (DD:HH:MM:SS)
Time for aging out:29:23:59:35 (DD:HH:MM:SS)
ISID:400001370000
Initiator      Initiator      Target          Target          Connection
IP Address     TCP Port       IP Address      TCP Port        ID
-----
10.10.10.210  54835         10.10.10.40    3260            1
```

Supported Releases 10.3.0E or later

show iscsi storage-devices

Displays information about the storage arrays directly attached to OS10 ports.

Syntax `show iscsi storage-devices`

Parameters None

Command Mode EXEC

Usage Information

The command output displays the storage device connected to each switch port and whether iSCSI automatically detects it.

Example

```
OS10# show iscsi storage-devices
Interface Name      Storage Device Name  Auto Detected Status
-----
ethernet1/1/23     EQL-MEM              true
```

Supported Releases

10.3.0E or later

Converged network DCB example

A converged data center network carries multiple traffic types (SAN, server, and LAN) that are sensitive to different aspects of data transmission. For example, storage traffic is sensitive to packet loss, while server traffic is latency-sensitive. In a single converged link, all traffic types coexist without imposing serious restrictions on others' performance. DCB allows iSCSI and FCoE SAN traffic to co-exist with server and LAN traffic on the same network. DCB features reduce or avoid dropped frames, retransmission, and network congestion.

DCB provides lossless transmission of FCoE and iSCSI storage traffic using:

- Separate traffic classes for the different service needs of network applications.
- PFC flow control to pause data transmission and avoid dropping packets during congestion.
- ETS bandwidth allocation to guarantee a percentage of shared bandwidth to bursty traffic, while allowing each traffic class to exceed its allocated bandwidth if another traffic class is not using its share.
- DCBX discovery of peers, including parameter exchange (PFC, ETS, and other DCB settings), mismatch detection, and remote configuration of DCB parameters.
- iSCSI application protocol TLV information in DCBX advertisements to communicate iSCSI support to peer ports

This example shows how to configure a sample DCB converged network in which:

- DCBX is enabled globally to ensure the exchange of DCBX, PFC, ETS, and iSCSI configurations between DCBX-enabled devices.
- PFC is configured to ensure lossless traffic for dot1p priority 4, 5, 6, and 7 traffic.
- ETS allocates 30% bandwidth for dot1p priority 0, 1, 2, and 3 traffic and 70% bandwidth for priority 4, 5, 6, and 7 traffic.
- iSCSI is configured to use dot1p priority 6 for iSCSI traffic, and advertise priority 6 in iSCSI application TLVs.
- The default `class-trust` class map honors dot1p priorities in ingress flows and applies a 1-to-1 dot1p-to-qos-group and a 1-to-1 qos-group-to-queue mapping. In OS10, `qos-group` represents a traffic class used only for internal processing.

1. DCBX configuration (global)

Configure DCBX globally on a switch to enable the exchange of DCBX TLV messages with PFC, ETS, and iSCSI configurations.

```
OS10# configure terminal
OS10(config)# dcbx enable
```

2. PFC configuration (global)

PFC is enabled on traffic classes with dot1p 4, 5, 6, and 7 traffic. The traffic classes all use the default PFC pause settings for shared buffer size and pause frames in ingress queue processing in the network-qos policy map. The pclass policy map honors (trusts) all dot1p ingress traffic. The reserved class-trust class map is configured by default. Trust does not modify ingress values in output flows.

```
OS10(config)# class-map type network-qos test4
OS10(config-cmap-nqos)# match qos-group 4
OS10(config-cmap-nqos)# exit
OS10(config)# class-map type network-qos test5
OS10(config-cmap-nqos)# match qos-group 5
OS10(config-cmap-nqos)# exit
OS10(config)# class-map type network-qos test6
OS10(config-cmap-nqos)# match qos-group 6
OS10(config-cmap-nqos)# exit
OS10(config)# class-map type network-qos test7
OS10(config-cmap-nqos)# match qos-group 7
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos test
```

```

OS10(config-pmap-network-qos)# class test4
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 4
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# class test5
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 5
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# class test6
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 6
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# class test7
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 7
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# exit

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dscp default

```

3. PFC configuration (interface)

Apply the service policies with dot1p trust and PFC configurations to an interface.

```

OS10(config)# interface ethernet 1/1/53
OS10(conf-if-eth1/1/53)# no shutdown
OS10(conf-if-eth1/1/53)# service-policy input type network-qos test
OS10(conf-if-eth1/1/53)# service-policy input type qos pclass
OS10(conf-if-eth1/1/53)# priority-flow-control mode on
OS10(conf-if-eth1/1/53)# end

```

4. ETS configuration (global)

A trust dot1p-map assigns dot1p 0, 1, 2, and 3 traffic to qos-group 0, and dot1p 4, 5, 6, and 7 traffic to qos-group 1. A qos-map traffic-class map assigns the traffic class in qos-group 0 to queue 0, and qos-group 1 traffic to queue 1. A queuing policy map assigns 30% of interface bandwidth to queue 0, and 70% of bandwidth to queue 1.

The pclass policy map applies trust to all dot1p ingress traffic. Trust does not modify ingress dot1p values in output flows. The reserved class-trust class map is configured by default.

```

OS10(config)# trust dot1p-map tmap1
OS10(config-tmap-dot1p-map)# qos-group 0 dot1p 0-3
OS10(config-tmap-dot1p-map)# qos-group 1 dot1p 4-7
OS10(config-tmap-dot1p-map)# exit

OS10(config)# qos-map traffic-class tmap2
OS10(config-qos-map)# queue 0 qos-group 0
OS10(config-qos-map)# queue 1 qos-group 1
OS10(config-qos-map)# exit

OS10(config)# class-map type queuing cmap1
OS10(config-cmap-queuing)# match queue 0
OS10(config-cmap-queuing)# exit
OS10(config)# class-map type queuing cmap2
OS10(config-cmap-queuing)# match queue 1
OS10(config-cmap-queuing)# exit

OS10(config)# policy-map type queuing pmap1
OS10(config-pmap-queuing)# class cmap1
OS10(config-pmap-c-que)# bandwidth percent 30
OS10(config-pmap-c-que)# exit
OS10(config-pmap-queuing)# class cmap2
OS10(config-pmap-c-que)# bandwidth percent 70
OS10(config-pmap-c-que)# end

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p default

```

5. ETS configuration (interface and global)

Apply the service policies with dot1p trust and ETS configurations to an interface or on all switch interfaces. Only one qos-map traffic-class map is supported on a switch.

```
OS10(config)# interface ethernet 1/1/53
OS10(config-if-eth1/1/53)# trust-map dot1p tmap1
OS10(config-if-eth1/1/53)# qos-map traffic-class tmap2
OS10(config-if-eth1/1/53)# service-policy input type qos pclass
OS10(config-if-eth1/1/53)# service-policy output type queuing pmap1
OS10(config-if-eth1/1/53)# ets mode on
OS10(config-if-eth1/1/53)# end
```

```
OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p tmap1
OS10(config-sys-qos)# qos-map traffic-class tmap2
OS10(config-sys-qos)# service-policy input type qos pclass
OS10(config-sys-qos)# service-policy output type queuing pmap1
OS10(config-sys-qos)# ets mode on
```

6. Verify DCB configuration

```
OS10(config-if-eth1/1/53)# show configuration
!
interface ethernet1/1/53
  switchport access vlan 1
  no shutdown
  service-policy input type network-qos test
  service-policy input type qos pclass
  service-policy output type queuing pmap1
  ets mode on
  qos-map traffic-class tmap2
  trust-map dot1p tmap1
  priority-flow-control mode on
```

7. Verify DCBX operational status

```
OS10(config-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53
E-ETS Configuration TLV enabled          e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled         r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled         p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled i-Application Priority for iSCSI disabled
-----

Interface ethernet1/1/53
  Port Role is Manual
  DCBX Operational Status is Enabled
  Is Configuration Source? FALSE
  Local DCBX Compatibility mode is IEEEv2.5
  Local DCBX Configured mode is AUTO
  Peer Operating version is IEEEv2.5
  Local DCBX TLVs Transmitted: ERPfI
  4 Input PFC TLV pkts, 3 Output PFC TLV pkts, 0 Error PFC pkts
  2 Input ETS Conf TLV Pkts, 27 Output ETS Conf TLV Pkts, 0 Error ETS Conf TLV Pkts
  2 Input ETS Reco TLV pkts, 27 Output ETS Reco TLV pkts, 0 Error ETS Reco TLV Pkts

Total DCBX Frames transmitted 0
Total DCBX Frames received 0
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0
```

8. Verify PFC configuration and operation

```
OS10(config-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53 pfc detail

Interface ethernet1/1/53
  Admin mode is on
  Admin is enabled, Priority list is 4,5,6,7
  Remote is enabled, Priority list is 4,5,6,7
  Remote Willing Status is disabled
  Local is enabled, Priority list is 4,5,6,7
```

```

Oper status is init
PFC DCBX Oper status is Up
State Machine Type is Symmetric
PFC TLV Tx Status is enabled
Application Priority TLV Parameters :
-----
ISCSI TLV Tx Status is enabled
Local ISCSI PriorityMap is 0x10
Remote ISCSI PriorityMap is 0x10

4 Input TLV pkts, 3 Output TLV pkts, 0 Error pkts
4 Input Appln Priority TLV pkts, 3 Output Appln Priority TLV pkts,
0 Error Appln Priority TLV Pkts

```

9. Verify ETS configuration and operation

```
OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53 ets detail
```

```

Interface ethernet1/1/53
Max Supported PG is 8
Number of Traffic Classes is 8
Admin mode is on

```

```
Admin Parameters :
```

```
-----
Admin is enabled
```

PG-grp	Priority#	Bandwidth	TSA
0	0,1,2,3,	30%	ETS
1	4,5,6,7	70%	ETS
2		0%	ETS
3		0%	ETS
4		0%	ETS
5		0%	ETS
6		0%	ETS
7		0%	ETS

```
Remote Parameters :
```

```
-----
Remote is enabled
```

PG-grp	Priority#	Bandwidth	TSA
0	0,1,2,3,	30%	ETS
1	4,5,6,7	70%	ETS
2		0%	SP
3		0%	SP
4		0%	SP
5		0%	SP
6		0%	SP
7		0%	SP

```
Remote Willing Status is disabled
```

```
Local Parameters :
```

```
-----
Local is enabled
```

PG-grp	Priority#	Bandwidth	TSA
0	0,1,2,3,	30%	ETS
1	4,5,6,7	70%	ETS
2		0%	ETS
3		0%	ETS
4		0%	ETS
5		0%	ETS
6		0%	ETS
7		0%	ETS

```

Oper status is init
ETS DCBX Oper status is Up
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled

```

```
2 Input Conf TLV Pkts, 27 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
2 Input Reco TLV Pkts, 27 Output Reco TLV Pkts, 0 Error Reco TLV Pkts
```

10. iSCSI optimization configuration (global)

This example accepts the default settings for aging time and TCP ports used in monitored iSCSI sessions. A Compellent storage array is connected to the port. The policy-iscsi policy map sets the CoS dot1p priority used for iSCSI traffic to 6 globally on the switch. By default, iSCSI traffic uses priority 4. The `iscsi priority-bits 0x40` command sets the advertised dot1p priority used by iSCSI traffic in application TLVs to 6. Hexadecimal 0x40 is binary 0 1 0 0 0 0 0 0.

```
OS10(conf-if-eth1/1/53)# iscsi profile-storage compellent
OS10(conf-if-eth1/1/53)# lldp tlv-select dcbxp-appln iscsi
OS10(conf-if-eth1/1/53)# exit

OS10(config)# iscsi target port 3261 ip-address 10.1.1.1
OS10(config)# policy-map type application policy-iscsi
OS10(config-pmap-application)# class class-iscsi
OS10(config-pmap-c-app)# set qos-group 6
OS10(config-pmap-c-app)# set cos 6
OS10(config-pmap-c-app)# exit
OS10(config-pmap-application)# exit

OS10(config)# system qos
OS10(config-sys-qos)# service-policy type application policy-iscsi
OS10(config-sys-qos)# exit

OS10(config)# iscsi session-monitoring enable
OS10(config)# iscsi priority-bits 0x40
OS10(config)# iscsi enable
```

11. Verify iSCSI optimization (global)

After you enable iSCSI optimization, the iSCSI application priority TLV parameters are added in the `show` command output to verify a PFC configuration.

```
OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53 pfc detail

Interface ethernet1/1/53
  Admin mode is on
  Admin is enabled, Priority list is 4,5,6,7
  Remote is enabled, Priority list is 4,5,6,7
  Remote Willing Status is disabled
  Local is enabled, Priority list is 4,5,6,7
  Oper status is init
  PFC DCBX Oper status is Up
  State Machine Type is Symmetric
  PFC TLV Tx Status is enabled
  Application Priority TLV Parameters :
  -----
  ISCSI TLV Tx Status is enabled
  Local ISCSI PriorityMap is 0x40
  Remote ISCSI PriorityMap is 0x10

  4 Input TLV pkts, 3 Output TLV pkts, 0 Error pkts
  4 Input Appln Priority TLV pkts, 3 Output Appln Priority TLV pkts, 0 Error Appln
  Priority TLV Pkts
```

12. DCBX configuration (interface)

This example shows how to configure and verify different DCBX versions.

```
OS10(conf-if-eth1/1/53)# dcbx version cee
OS10(conf-if-eth1/1/53)# show configuration
!
interface ethernet1/1/53
  switchport access vlan 1
  no shutdown
  dcbx version cee
  service-policy input type network-qos test
  service-policy input type qos pclass
  service-policy output type queuing pmap1
```



```
ets mode on
qos-map traffic-class tmap2
trust-map dot1p tmap1
priority-flow-control mode on
```

```
OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53
E-ETS Configuration TLV enabled          e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled         r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled         p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled  i-Application Priority for iSCSI disabled
-----
```

```
Interface ethernet1/1/53
Port Role is Manual
DCBX Operational Status is Enabled
Is Configuration Source? FALSE
Local DCBX Compatibility mode is CEE
Local DCBX Configured mode is CEE
Peer Operating version is CEE
Local DCBX TLVs Transmitted: ErPfi
```

```
Local DCBX Status
```

```
-----
DCBX Operational Version is 0
DCBX Max Version Supported is 0
Sequence Number: 2
Acknowledgment Number: 1
Protocol State: In-Sync
```

```
Peer DCBX Status
```

```
-----
DCBX Operational Version is 0
DCBX Max Version Supported is 0
Sequence Number: 1
Acknowledgment Number: 2
 3 Input PFC TLV pkts, 3 Output PFC TLV pkts, 0 Error PFC pkts
 3 Input PG TLV Pkts, 3 Output PG TLV Pkts, 0 Error PG TLV Pkts
 3 Input Appln Priority TLV pkts, 3 Output Appln Priority TLV pkts,
 0 Error Appln Priority TLV Pkts
```

```
Total DCBX Frames transmitted 3
Total DCBX Frames received 3
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0
```

```
OS10(conf-if-eth1/1/53)# dcbx version cee
OS10(conf-if-eth1/1/53)# show configuration
```

```
!
interface ethernet1/1/53
 switchport access vlan 1
 no shutdown
 dcbx version ieee
 service-policy input type network-qos test
 service-policy input type qos pclass
 service-policy output type queuing pmap1
 ets mode on
 qos-map traffic-class tmap2
 trust-map dot1p tmap1
 priority-flow-control mode on
```

```
OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53
E-ETS Configuration TLV enabled          e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled         r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled         p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled  i-Application Priority for iSCSI disabled
-----
```

```
Interface ethernet1/1/53
Port Role is Manual
```

```
DCBX Operational Status is Enabled
Is Configuration Source? FALSE
Local DCBX Compatibility mode is IEEEv2.5
Local DCBX Configured mode is IEEEv2.5
Peer Operating version is IEEEv2.5
Local DCBX TLVs Transmitted: ERPfI
13 Input PFC TLV pkts, 4 Output PFC TLV pkts, 0 Error PFC pkts
3 Input ETS Conf TLV Pkts, 26 Output ETS Conf TLV Pkts, 0 Error ETS Conf TLV Pkts
3 Input ETS Reco TLV pkts, 26 Output ETS Reco TLV pkts, 0 Error ETS Reco TLV Pkts

Total DCBX Frames transmitted 0
Total DCBX Frames received 0
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0
```

sFlow is a standard-based sampling technology embedded within switches and routers that monitors network traffic. It provides traffic monitoring for high-speed networks with many switches and routers.

- OS10 supports sFlow version 5
- sFlow collector is supported only on data ports
- A maximum of two sFlow collectors
- OS10 does not support sFlow on SNMP, VLAN, VRF, tunnel interfaces, extended sFlow, backoff mechanism, and egress sampling

sFlow uses two types of sampling:

- Statistical packet-based sampling of switched or routed packet flows
- Time-based sampling of interface counters

The sFlow monitoring system consists of an sFlow agent (embedded in the device) and an sFlow collector:

- The sFlow agent resides anywhere within the path of the packet and combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow collector at regular intervals. The datagrams consist of information on, but not limited to, the packet header, ingress and egress interfaces, sampling parameters, and interface counters. Application-specific integrated circuits (ASICs) handle the packet sampling.
- The sFlow collector analyses the datagrams received from different devices and produces a network-wide view of traffic flows.

Enable sFlow

You can enable sFlow either on all interfaces globally or on a specific set of interfaces. The system displays an error message if you try to enable sFlow on both modes at a time.

If you configure sFlow only on a set of interfaces, any further change to the sFlow-enabled ports triggers the sFlow agent to restart. This results in a gap in the polling counter statistics of 30 seconds and the sFlow counters are reset on all sFlow-enabled ports.

When you enable sFlow on a port-channel:

- When you enable sFlow in Per-Interface mode, the counter statistics of sFlow-enabled ports reset to zero when you add a new member port or remove an existing member port from any sflow enabled port-channel group.
- sFlow counter statistics that are individually reported for the port members of a port-channel data source are accurate. Counter statistics reported for the port-channel may not be accurate. To calculate the correct counters for a port-channel data source, add together the counter statistics of the individual port members.

Enable or disable sFlow globally

sFlow is disabled globally by default.

- Enable sFlow globally on all interfaces in CONFIGURATION mode.

```
sflow enable all-interfaces
```

- Disable sFlow in CONFIGURATION mode.

```
no sflow
```

Enable or disable sFlow on a specific interface

- Enable sFlow in CONFIGURATION mode.

```
sflow enable
```

- Disable sFlow in CONFIGURATION mode.

```
no sflow enable
```

Enable sFlow on a specific interface

```
OS10(config)# sflow enable
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# sflow enable
```

Enable sFlow on a range of interfaces

```
OS10(config)# sflow enable
OS10(config)# interface range ethernet 1/1/1-1/1/10
OS10(conf-range-eth1/1/1-1/1/10)# sflow enable
```

Enable sFlow on a port-channel

```
OS10(config)# sflow enable
OS10(config)# interface range port-channel 1-10
OS10(conf-range-po-1-10)# sflow enable
```

Max-header size configuration

- Set the packet maximum size in CONFIGURATION mode, from 64 to 256. The default is 128 bytes.

```
max-header-size header-size
```

- Disable the header size in CONFIGURATION mode.

```
no sflow max-header-size
```

- View the maximum packet header size in EXEC mode.

```
show sflow
```

Configure sFlow maximum header size

```
OS10(config)# sflow max-header-size 80
```

View sFlow information

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 20
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

View sFlow running configuration

```
OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 30
sflow sample-rate 4096
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767 max-datagram-size 800
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
```

```
sflow enable
!
```

Collector configuration

Configure the IPv4 or IPv6 address for the sFlow collector. You can configure a maximum of two sFlow collectors. If you specify two collectors, the samples are sent to both. The agent IP address must be the same for both the collectors.

- Enter an IPv4 or IPv6 address for the sFlow collector, IPv4 or IPv6 address for the agent, UDP collector port number (default 6343), maximum datagram size (up to 1400), and the VRF instance number in CONFIGURATION mode.

```
sflow collector {ip-address | ipv6-address} agent-addr {ip-address | ipv6-address}
[collector-port-number] [vrf default]
```

The `no` form of the command disables sFlow collectors in CONFIGURATION mode.

sFlow collector

```
OS10(config)# sflow collector 10.1.1.1 agent-addr 2.2.2.2 6443 vrf default
```

Polling-interval configuration

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. Unless there is a specific deployment need to configure a lower polling interval value, configure the polling interval to the maximum value.

- Change the default counter polling interval in CONFIGURATION mode, from 10 to 300. The default is 20.

```
sflow polling-interval interval-size
```

- Disable the polling interval in CONFIGURATION mode.

```
no sflow polling-interval
```

- View the polling interval in EXEC mode.

```
show sflow
```

Configure sFlow polling interval

```
OS10(config)# sflow polling-interval 200
```

View sFlow information

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 200
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

View sFlow running configuration

```
OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 200
sflow sample-rate 4096
```

```
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767 max-datagram-size 800
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
sflow enable
!
```

Sample-rate configuration

Sampling rate is the number of packets skipped before the sample is taken. If the sampling rate is 4096, one sample generates for every 4096 packets observed.

- Set the sampling rate in CONFIGURATION mode, from 4096 to 65535. The default is 32768.

```
sflow sample-rate sampling-size
```

- Disable packet sampling in CONFIGURATION mode.

```
no sflow sample-rate
```

- View the sampling rate in EXEC mode.

```
show sflow
```

Configure sFlow sampling rate

```
OS10(config)# sflow sample-rate 4096
```

View sFlow packet header size

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 4096
Global default counter polling interval: 20
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

View sFlow running configuration

```
OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 20
sflow sample-rate 4096
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767 max-datagram-size 800
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
sflow enable
!
```

Source interface configuration

You can configure an interface as a source for sFlow. The sFlow agent uses IP address of the configured source interface as agent IP address.

- Configure the source interface in CONFIGURATION mode.

```
sflow source-interface {ethernet node/slot/port[:subport] | loopback loopback-ID|
port-channel port-channel-ID| vlan vlan-ID}
```

- View the interface details.

```
show running-configuration sflow
```

```
show sflow
```

Configure sFlow source interface

```
OS10(config)# sflow source-interface ethernet 1/1/1
OS10(config)# sflow source-interface port-channel 1
OS10(config)# sflow source-interface loopback 1
OS10(config)# sflow source-interface vlan 10
```

View sFlow running configuration

```
OS10# show running-configuration sflow
sflow enable all-interfaces
sflow source-interface vlan10
sflow collector 5.1.1.1 agent-addr 4.1.1.1 6343
sflow collector 6.1.1.1 agent-addr 4.1.1.1 6343

OS10(config)#show running-configuration interface vlan
!
interface vlan1
no shutdown
!
interface vlan10
no shutdown
ip address 10.1.1.1/24
```

View sFlow details

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 30
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
2 collector(s) configured
Collector IP addr:5.1.1.1 Agent IP addr:10.1.1.1 UDP port:6343 VRF:Default → It shows
active agent-ip
Collector IP addr:6.1.1.1 Agent IP addr:10.1.1.1 UDP port:6343 VRF:Default → It shows
active agent-ip
2 UDP packets exported
0 UDP packets dropped
2 sFlow samples collected
```

View sFlow information

The current release does not support the statistics for UDP packets dropped.

- View sFlow configuration details and statistics in EXEC mode.

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
```

```

Global default sampling rate: 32768
Global default counter polling interval: 30
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected

```

- View sFlow configuration details on a specific interface in EXEC mode.

```

OS10# show sflow interface port-channel 1
port-channell
sFlow is enabled on port-channell
Samples rcvd from h/w: 0

```

- View the sFlow running configuration in EXEC mode.

```

OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 30
sflow sample-rate 4096
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
sflow enable
!

```

sFlow commands

sflow collector

Configures an sFlow collector IP address to which sFlow datagrams are forwarded to. You can configure a maximum of two collectors.

Syntax	<code>sflow collector {ipv4-address ipv6-address} agent-addr {ipv4-address ipv6-address} [collector-port-number] [vrf default]</code>
Parameters	<ul style="list-style-type: none"> • <code>ipv4-address ipv6-address</code> — Enter an IPv4 or IPv6 address in A.B.C.D/A::B format. • <code>agent-addr ipv4-address ipv6-address</code> — Enter the sFlow agent IP address. If you are configuring two collectors, the agent IP address must be the same for both the collectors. • <code>collector-port-number</code> — (Optional) Enter the UDP port number, from 1 to 65535. The default is 6343. • <code>vrf</code> — (Optional) Enter <code>default</code> to configure the sFlow collector corresponding to the front panel ports.
Defaults	Not configured
Command Modes	CONFIGURATION
Usage Information	You must enter a valid and reachable IPv4 or IPv6 address. If you configure two collectors, traffic samples are sent to both. The sFlow agent address is the IPv4 or IPv6 address used to identify the agent to the collector. The <code>no</code> version of this command removes the configured sFlow collector.
Example	<pre>OS10(conf)# sflow collector 10.1.1.1 agent-addr 2.2.2.2 6343vrf default</pre>
Supported Releases	10.3.0E or later

sflow enable

Enables sFlow on a specific interface or globally on all interfaces.

Syntax	<code>sflow enable [all-interfaces]</code>
Parameters	<code>all-interfaces</code> — (Optional) Enter to enable sFlow globally.
Default	Disabled
Command Mode	CONFIGURATION

Usage Information The `no` version of this command to disables sFlow.

Example (interface)

```
OS10(config)# sflow enable
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# sflow enable
```

Example (interface range)

```
OS10(config)# sflow enable
OS10(config)# interface range ethernet 1/1/1-1/1/10
OS10(conf-range-eth1/1/1-1/1/10)# sflow enable
```

Example (port-channel)

```
OS10(config)# sflow enable
OS10(config)# interface range port-channel 1-10
OS10(conf-range-po-1-10)# sflow enable
```

Supported Releases 10.3.0E or later

sflow max-header-size

Sets the maximum header size of a packet.

Syntax	<code>sflow max-header-size <i>header-size</i></code>
Parameter	<code>header-size</code> — Enter the header size in bytes, from 64 to 256. The default is 128.
Default	128 bytes
Command Mode	CONFIGURATION

Usage Information Use the `no` version of the command to reset the header size to the default value.

Example

```
OS10(conf)# sflow max-header-size 256
```

Supported Releases 10.3.0E or later

sflow polling-interval

Sets the sFlow polling interval.

Syntax	<code>sflow polling-interval <i>interval-value</i></code>
Parameter	<code>interval-value</code> — Enter the interval value in sections, from 10 to 300. The default is 30.
Defaults	30
Command Mode	CONFIGURATION

Usage Information 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. The `no` version of the command resets the interval time to the default value.

Example

```
OS10(config)# sflow polling-interval 200
```

Supported Releases 10.3.0E or later

sflow sample-rate

Configures the sampling rate.

Syntax `sflow sample-rate value`

Parameter `value` — Enter the packet sample rate, from 4096 to 65535. The default is 32768.

Default 32768

Command Mode CONFIGURATION

Usage Information Sampling rate is the number of packets skipped before the sample is taken. For example, if the sampling rate is 4096, one sample generates for every 4096 packets observed. The `no` version of the command resets the sampling rate to the default value.

Example

```
OS10(config)# sflow sample-rate 4096
```

Supported Releases 10.3.0E or later

sflow source-interface

Configures an interface as source for sFlow. The sFlow agent uses IP address of the configured source interface as agent IP address.

Syntax `sflow source-interface {ethernet node/slot/port[:subport] | loopback loopback-ID | port-channel port-channel-ID | vlan vlan-ID}`

Parameters

- `ethernet node/slot/port[:subport]`—Enter the physical interface type details.
- `loopback loopback-ID`—Enter the loopback interface details. The loopback ID ranges from 0 to 16383.
- `port-channel port-channel-ID`—Enter the port channel details. The port channel ID ranges from 1 to 128.
- `vlan vlan-ID`—Enter the VLAN details. The VLAN ID ranges from 1 to 4093.

Default Disabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command removes the configuration from the interface.

Example (Ethernet)

```
OS10(config)# sflow source-interface ethernet 1/1/1
```

Example (Loopback)

```
OS10(config)# sflow source-interface loopback 1
```

Example (port-channel)

```
OS10(config)# sflow source-interface port-channel 1
```

Example (VLAN)

```
OS10(config)# sflow source-interface vlan 10
```

Supported Releases

10.4.1.0 or later

show sflow

Displays the current sFlow configuration for all interfaces or by a specific interface type.

Syntax `show sflow [interface type]`

Parameter `interface type` — (Optional) Enter either `ethernet` or `port-channel` for the interface type.

Command Mode EXEC

Usage Information OS10 does not support statistics for UDP packets dropped and samples received from the hardware.

Example

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 30
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP
port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

Example (port-channel)

```
OS10# show sflow interface port-channel 1
port-channell
sFlow is enabled on port-channell
Samples rcvd from h/w: 0
```

Supported Releases

10.3.0E or later

RESTCONF API

RESTCONF is a REST-like protocol that uses HTTPS connections. Use the OS10 RESTCONF API to set up the configuration parameters on OS10 switches using JavaScript Object Notation (JSON)-structured messages. Use any programming language to create and send JSON messages. The examples in this chapter use curl.

The OS10 RESTCONF implementation complies with RFC 8040. You can use the RESTCONF API to configure and monitor an OS10 switch.

The OS10 RESTCONF API uses HTTP with the Transport Layer Security (TLS) protocol over port 443. OS10 supports HTTP/1.1 transport as defined in RFC 7230. The RESTCONF API uses pluggable authentication modules (PAM)-based authentication.

On supported platforms, the OS10 RESTCONF API is disabled by default. To configure and enable the RESTCONF API, see the *Configure the RESTCONF API* section.

To configure and monitor an OS10 switch, use REST API client tools, such as Postman or Swagger, to execute web requests. REST API requests, such as GET, PUT, POST, DELETE, and PATCH, operate on OS10 RESTCONF resources.

Table 42. OS10 RESTCONF resources

Resource	Description	URL
Data	Configuration and operational data accessed by a RESTCONF API client	/restconf/data
Operations	Container for the protocol-specific data model operations advertised by OS10	/restconf/operations

To browse OS10 RESTCONF API end-points and operations, see the OpenAPI JavaScript Object Notation (JSON) files available on the OS10 Enterprise Edition Software page at the [Dell EMC Support](#) site. Download the JSON files and import them to REST API client tools — for example, Swagger or Postman — to generate code, documentation, and test cases. For information about the OpenAPI specification, go to <https://swagger.io/docs/specification/about/>.

Configure RESTCONF API

To use the RESTCONF API on an OS10 interface, you must enable the RESTCONF API service using the `rest api restconf` command. You can also configure HTTPS access, including:

- Hostname required in an SSL self-signed server certificate
- Timeout for an HTTPS connection
- Cipher suites for encrypting data in an HTTPS connection

After you enable the RESTCONF API, you can send HTTPS requests from a remote device.

1. (Optional) Configure the hostname required in the SSL self-signed server certificate in a RESTCONF HTTPS connection in CONFIGURATION mode, using a maximum of 30 alphanumeric characters. Enter the IP address or domain name of the OS10 switch. By default, the domain name of the OS10 switch is used as the hostname.

```
rest https server-certificate name hostname
```

2. (Optional) Configure the timeout that a RESTCONF HTTPS session uses in CONFIGURATION mode, from 30 to 65535 seconds; default 30.

```
rest https session timeout seconds
```

3. (Optional) Limit the ciphers that the switch uses in a RESTCONF HTTPS session to encrypt and decrypt data in CONFIGURATION mode. By default, all cipher suites installed on OS10 are supported. Separate multiple entries with a blank space. Valid cipher-suite values are:
 - `dhe-rsa-with-aes-128-gcm-SHA256`
 - `dhe-rsa-with-aes-256-gcm-SHA384`
 - `ecdhe-rsa-with-aes-128-gcm-SHA256`

- ecdhe-rsa-with-aes-256-gcm-SHA384

```
rest https cipher-suite
```

4. Enable the RESTCONF API in CONFIGURATION mode.

```
rest api restconf
```

RESTCONF API configuration

```
OS10(config)# rest https server-certificate name OS10.dell.com
OS10(config)# rest https session timeout 60
OS10(config)# rest https cipher-suite dhe-rsa-with-aes-128-gcm-SHA256
dhe-rsa-with-aes-256-gcm-SHA384 ecdhe-rsa-with-aes-256-gcm-SHA384
OS10(config)# rest api restconf
```

CLI commands for RESTCONF API

rest api restconf

Enables the RESTCONF API service on the switch.

Syntax	<code>rest api restconf</code>
Parameters	None
Default	RESTCONF API is disabled.
Command Mode	CONFIGURATION
Usage Information	<ul style="list-style-type: none"> • After you enable the RESTCONF API, you can send curl commands in HTTPS requests from a remote device. • The <code>no</code> version of the command disables the RESTCONF API.
Example	<pre>OS10(config)# rest api restconf</pre>
Supported Releases	10.4.1.0 or later

rest https cipher-suite

Limits the ciphers used to encrypt and decrypt REST HTTPS data.

Syntax	<code>rest https cipher-suite cipher-list</code>
Parameters	<p><code>cipher-list</code> — Enter the ciphers supported in a REST API HTTPS session. Separate multiple entries with a blank space. Valid cipher suites are:</p> <ul style="list-style-type: none"> • dhe-rsa-with-aes-128-gcm-SHA256 • dhe-rsa-with-aes-256-gcm-SHA384 • ecdhe-rsa-with-aes-128-gcm-SHA256 • ecdhe-rsa-with-aes-256-gcm-SHA384
Default	All cipher suites installed in OS10 are supported.
Command Mode	CONFIGURATION
Usage Information	<ul style="list-style-type: none"> • Use the <code>rest https cipher-suite</code> command to restrict the ciphers that a RESTCONF HTTPS session uses. • The <code>no</code> version of the command removes the configured cipher list and restores the default value.

Example

```
OS10(config)# rest https cipher-suite dhe-rsa-with-aes-128-gcm-SHA256
dhe-rsa-with-aes-256-gcm-SHA384 ecdhe-rsa-with-aes-256-gcm-SHA384
```

Supported Releases 10.4.1.0 or later

rest https server-certificate

Creates the SSL self-signed server certificate used in a RESTCONF HTTPS connection.

Syntax `rest https server-certificate name hostname`

Parameters `name hostname` — Enter the IP address or domain name of the OS10 switch.

Default `hostname` is the domain name of the OS10 switch.

Command Mode CONFIGURATION

Usage Information The `no` version of the command removes the host name from the SSL server certificate.

Example

```
OS10(config)# rest https server-certificate name 10.10.10.10
```

Supported Releases 10.4.1.0 or later

rest https session timeout

Configures the timeout used in a RESTCONF HTTPS connection.

Syntax `rest https session timeout seconds`

Parameters `seconds` — Enter the timeout used to wait for an HTTPS request from a RESTCONF client (30 to 65535 seconds).

Default 30 seconds

Command Mode CONFIGURATION

Usage Information

- If no HTTPS request is received within the configured time, the switch closes the RESTCONF HTTPS session.
- The `no` version of the command removes the configured RESTCONF HTTPS session timeout.

Example

```
OS10# rest https session timeout 60
```

Supported Releases 10.4.1.0 or later

RESTCONF API tasks

Using the RESTCONF API, you can provision OS10 switches using HTTPS requests. The examples in this section show how to access the OS10 RESTCONF API using `curl` commands. `curl` is a Linux shell command that generates HTTPS requests and is executed on an external server.

curl Commands

`curl` command options include:

- `-X` specifies the HTTPS request type; for example, `POST`, `PATCH`, or `GET`.
- `-u` specifies the user name and password to use for server authentication.

- `-k` specifies a text file to read curl arguments from. The command line arguments found in the text file will be used as if they were provided on the command line. Use the IP address or URL of the OS10 switch when you access the OS10 RESTCONF API from a remote orchestration system.
- `-H` specifies an extra header to include in the request when sending HTTPS to a server. You can enter multiple extra headers.
- `-d` sends the specified data in an HTTPS request.

In curl commands, use `%2F` to represent a backslash (`/`); for example, enter `ethernet1/2/3` as `ethernet1%2F1%2F3`.

View XML structure of CLI commands

To use the RESTCONF API to configure and monitor an OS10 switch, create an HTTPS request with data parameters in JSON format. The JSON data parameters correspond to the same parameters in the XML structure of an OS10 command.

To display the parameter values in the XML code of an OS10 command as reference, enter the `debug cli netconf` command in EXEC mode. In CONFIGURATION mode, enter the `do debug cli netconf` command.

This command enables a CLI-to-XML display. At the prompt, enter the OS10 command for which you want to display the XML request and reply. To exit the CLI-to-XML display, enter the `no debug cli netconf` command.

Locate the XML parameters values for the same JSON data arguments. For example, to configure VLAN 20 on an OS10 switch, you would enter the RESTCONF endpoint and JSON contents in the curl command. Note how the JSON `type` and `name` parameters are displayed in the XML structure of the `interface vlan` command.

- RESTCONF endpoint: `/restconf/data/interfaces`
- JSON data content:

```
{
  "interface": [{
    "type": "iana-if-type:l2vlan",
    "enabled": true,
    "description": "vlan20",
    "name": "vlan20"
  }]
}
```

- curl command:

```
curl -X POST -u admin:admin -k "https://10.11.86.113/restconf/data/interfaces"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{"interface": [{ "type": "iana-if-type:l2vlan", "enabled": true,
"description":"vlan20", "name":"vlan20"}]}'
```

To display the values for the `type` and `name` parameters in the curl command, display the XML structure of the `interface vlan 20` configuration command:

```
OS10(config)# do debug cli netconf
OS10(config)# interface vlan 10

Request:
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <candidate/>
    </target>
    <default-operation>merge</default-operation>
    <error-option>stop-on-error</error-option>
    <test-option>set</test-option>
    <config>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-
interfaces" xmlns:ianaift="urn:ietf:params:xml:ns:yang:iana-if-type" xmlns:dell-
if="http://www.dellemc.com/networking/os10/dell-interface" xmlns:dell-eth="http://
www.dellemc.com/networking/os10/dell-ethernet" xmlns:dell-lag="http://www.dellemc.com/
networking/os10/dell-lag">
        <interface>
          <type>ianaift:l2vlan</type>
          <name>vlan10</name>
        </interface>
```

```
    </interfaces>
  </config>
</edit-config>
</rpc>
```

```
Reply:
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="10">
  <ok/>
</rpc-reply>
OS10(config)# do no debug cli netconf
```

RESTCONF API layer 2 configuration

Some common RESTCONF API L2 operations include provisioning and displaying VLAN, port channel, VLT, LLDP, and LACP configuration. The examples in this section use curl commands to send the HTTPS request.

LACP

Configure system priority

RESTCONF endpoint /restconf/data/sys-config/system-priority

JSON content

```
{
  "system-priority": 65535
}
```

Parameters

- `system-priority int` — Enter the LACP system priority used during negotiation with other devices, from 1 to 65535; the higher the number, the lower the priority. The default is 32768.

Example

```
curl -X PATCH -k -u admin:admin -H "accept:application/json"
-H "Content-Type:application/json"
"https://10.11.86.113/restconf/data/sys-config/system-priority"
-d '{"system-priority":65535}'
```

Configure port priority

RESTCONF endpoint /restconf/data/interfaces/interface/ethernet1/1/1

JSON content

```
{
  "interface": [{
    "name": "ethernet1/1/1",
    "lACP-config": {
      "actor-port-priority": 4096
    }
  }]
}
```

Parameters

- `ethernet-interface` — Enter the physical Ethernet interface in the format `ethernetnode/slot/port`.
- `name string` — Enter `ethernetnode/slot/port` to configure the port interface for LACP. Specify the same `node/slot/port` value in the `name string` and `ethernet-interface` parameters.
- `actor-port-priority int` — Enter the priority for the port interface, from 0 to 65535; the higher the number, the lower the priority. The default is 32768.

Example

```
curl -X PATCH -k -u admin:admin -H "accept:application/json"
-H "Content-Type:application/json"
```



```
"https://10.11.86.113/restconf/data/interfaces/interface/
ethernet1%2F1%2F1"
-d '{"interface":[{"name":"ethernet1/1/1", "lACP-config":{"actor-
port-priority":4096}}]}'
```

Configure LACP rate priority

RESTCONF endpoint /restconf/data/interfaces/interface/ethernet1/1/1

JSON content

```
{
  "interface": [{
    "name": "ethernet1/1/1",
    "lACP-config": {
      "rate": "fast"
    }
  }]
}
```

Parameters

- *ethernet-interface* — Enter the physical Ethernet interface in the format *ethernetnode/slot/port*.
- *name string* — Enter *ethernetnode/slot/port* to configure the LACP rate for sending control packets on the port interface.
- *rate string* — Enter *fast* to send LACP packets at one-second intervals; enter *normal* to send LACP packets at thirty-second intervals. The default is *normal*.

Example

```
curl -X PATCH -k -u admin:admin -H "accept:application/json"
-H "Content-Type:application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/
ethernet1%2F1%2F1"
-d '{"interface":[{"name":"ethernet1/1/1", "lACP-config":
{"rate":"fast"}}]}'
```

Display LACP configuration

RESTCONF endpoint /restconf/data/sys-config

JSON content None

Example

```
curl -X GET -k -u admin:admin -H "accept:application/json"
"https://10.11.86.113/restconf/data/sys-config"
```

LLDP

Create LLDP-MED network policy for voice applications

RESTCONF endpoint /restconf/data/dell-llDP-med:sys-config

JSON content

```
{
  "media-policy": [{
    "policy-id": 10,
    "app-type": "voice",
    "vlan-id": 10,
    "tagged": "true",
    "priority": 2,
    "dscp": 1
  }]
}
```

Parameters

- *policy-id int* — Enter the LLDP-MED network policy number, from 1 to 32.

- `app-type string` — Enter the application type defined by the policy: `voice` for a voice application or `guest-voice` for a guest-voice application.
- `vlan-id int` — Enter the VLAN ID number, from 1 to 4093.
- `tagged bool` — Enter `true` for a tagged VLAN; enter `false` for an untagged VLAN.
- `priority int` — Enter the Layer 2 class-of-service (CoS) priority value for the configured VLAN, from 0 to 7; default 0.
- `dscp int` — Enter the DSCP value for the configured VLAN (0 to 63; default 0).

Example

```
curl -X POST -k -u admin:admin -H "accept:application/json"
-H "Content-Type:application/json"
"https://10.11.86.113/restconf/data/dell-lldp-med:sys-config"
-d '{"media-policy":[{"policy-id": 10, "app-type":"voice",
"vlan-id":10, "tagged":"true", "priority":2, "dscp":1}]}'
```

Configure LLDP packet timer

RESTCONF endpoint /restconf/data/global-params

JSON content

```
{
  "tx-interval": 60
}
```

Parameters

- `tx-interval int` — Enter the rate at which LLDPDU packets are sent to peers, from 5 to 254 seconds; default 30.

Example

```
curl -X POST -k -u admin:admin -H "accept:application/json"
-H "Content-Type:application/json"
"https://10.11.86.113/restconf/data/global-params" -d '{"tx-
interval":60}'
```

Configure LLDPDU hold time

RESTCONF endpoint /restconf/data/global-params

JSON content

```
{
  "txhold-multiplier": 2
}
```

Parameters

- `txhold-multiplier int` — Enter the time that an LLDP peer device holds LLDP packets before discarding them, from 2 to 10 seconds; default 4.

Example

```
curl -X POST -k -u admin:admin -H "accept: application/json" -H
"Content-Type: application/json"
"https://10.11.86.113/restconf/data/global-params"
-d '{"txhold-multiplier":2}'
```

Configure basic TLV advertisement

RESTCONF endpoint /restconf/data/interfaces/interface/ethernet1/1/1

JSON content

```
{
  "interface": [{
    "name": "ethernet1/1/1",
    "lldp": [{
      "basic-tlvs": [{
        "sys-name-enable": "true"
      }]
    }]
  }]
}
```

```
    }]  
}
```

Parameters

- *ethernet-interface* — Enter the physical Ethernet interface in the format *ethernetnode/slot/port*.
- *name string* — Enter *ethernetnode/slot/port* to configure the interface that sends LLDPDUs with the specified TLVs.
- *sys-name-enable bool* — Enter *true* to enable system TLV advertisement on the interface; enter *false* to disable system TLV advertisement.

Example

```
curl -X PATCH -u admin:admin  
-k "https://10.11.86.113/restconf/data/interfaces/interface/  
ethernet1%2F1%2F1"  
-H "accept:application/json" -H "Content-Type:application/json"  
-d '{"interface":[{"name":"ethernet1/1/1", "lldp":[{"basic-tlvs":  
[{"sys-name-enable":"true"}]}]}'
```

Configure dot3 TLV advertisement

RESTCONF endpoint

/restconf/data/interfaces/interface/ethernet1/1/1

JSON content

```
{  
  "interface": [{  
    "name": "ethernet1/1/1",  
    "lldp": [{  
      "dot3-tlvs": [{  
        "mac-phy-config-enable": "true",  
        "max-frame-size-enable": "true"  
      }]  
    }]  
  }]  
}
```

Parameters

- *ethernet-interface* — Enter the physical Ethernet interface in the format *ethernetnode/slot/port*.
- *name string* — Enter *ethernetnode/slot/port* to identify the interface that sends LLDPDUs with the specified TLVs.
- *mac-phy-config-enable bool* — Enter *true* to enable MAC/PHY configuration/status TLV advertisement on the interface; enter *false* to disable VLAN ID TLV advertisement.
- *max-frame-size-enable bool* — Enter *true* to enable maximum-frame-size TLV advertisement on the interface; enter *false* to disable maximum-frame-size TLV advertisement.
- *linkagg-enable bool* — Enter *true* to enable link-aggregation TLV advertisement on the interface; enter *false* to disable link-aggregation TLV advertisement.

Example

```
curl -X PATCH -u admin:admin  
-k "https://10.11.86.113/restconf/data/interfaces/interface/  
ethernet1%2F1%2F1"  
-H "accept: application/json"  
-H "Content-Type: application/json"  
-d '{"interface": [{"name":"ethernet1/1/1", "lldp":[{"dot3-tlvs":  
[{"mac-phy-config-enable":"true", "max-frame-size-enable":"true"}]}]}'
```

```
curl -X PATCH -u admin:admin  
-k "https://10.11.86.113/restconf/data/interfaces/interface/  
ethernet1%2F1%2F1"  
-H "accept: application/json"  
-H "Content-Type: application/json"  
-d '{"interface":[{"name":"ethernet1/1/1", "lldp":[{"dot3-tlvs":  
[{"linkagg-enable":"true"}]}]}'
```

Enable LLDP-MED network policy advertisement

**RESTCONF
endpoint**

/restconf/data/interfaces/interface/ethernet1/1/1

JSON content

```
{
  "interface": [{
    "name": "ethernet1/1/1",
    "lldp-med-cfg": [{
      "policy-id": 1
    }]
  }]
}
```

Parameters

- *ethernet-interface* — Enter the physical Ethernet interface in the format *ethernetnode/slot/port*.
- *name string* — Enter *ethernetnode/slot/port* to configure the interface that sends LLDP-MED policy TLVs.
- *policy-id int* — Enter the LLDP-MED network policy number, from 1 to 32.

Example

```
curl -X PATCH -u admin:admin
-k "https://10.11.86.113/restconf/data/interfaces/interface/
ethernet1%2F1%2F1"
-H "accept:application/json" -H "Content-Type:application/json"
-d '{"interface":[{"name":"ethernet1/1/1", "lldp-med-cfg":
[{"policy-id":1}]}]}'
```

Disable TLV advertisement

**RESTCONF
endpoint**

/restconf/data/interfaces/interface/ethernet1/1/1

JSON content

```
{
  "interface": [{
    "name": "ethernet1/1/1",
    "lldp": [{
      "basic-tlvs": [{
        "sys-name-enable": "false"
      }],
      "dot3-tlvs": [{
        "mac-phy-config-enable": "false",
        "max-frame-size-enable": "false",
        "linkagg-enable": "false"
      }]
    }]
  }]
}
```

Parameters

- *ethernet-interface* — Enter the physical Ethernet interface in the format *ethernetnode/slot/port*.
- *name string* — Enter *ethernetnode/slot/port* to identify the interface that sends LLDPDUs with the specified TLVs.
- *sys-name-enable bool* — Enter *false* to disable system TLV advertisement on the interface; enter *true* to re-enable system TLV advertisement.
- *mac-phy-config-enable bool* — Enter *false* to disable MAC/PHY configuration/status TLV advertisement on the interface; enter *true* to re-enable VLAN ID TLV advertisement.
- *max-frame-size-enable bool* — Enter *false* to disable maximum-frame-size TLV advertisement on the interface; enter *true* to re-enable maximum-frame-size TLV advertisement.
- *linkagg-enable bool* — Enter *false* to disable link-aggregation TLV advertisement on the interface; enter *true* to re-enable link-aggregation TLV advertisement.

Example

```
curl -X PATCH -u admin:admin
-k "https://10.11.86.113/restconf/data/interfaces/interface/
ethernet1%2F1%2F1"
-H "accept: application/json" -H "Content-Type: application/json"
```

```
-d '{"interface":[{"name":"ethernet1/1/1", "lldp":[{"basic-tlvs": [{"sys-name-enable":"false"}], "dot3-tlvs":[{"mac-phy-config-enable":"false","max-frame-size-enable":"false", "linkagg-enable":"false"}]}]}'
```

Disable LLDP-MED network policy advertisement

RESTCONF endpoint /restconf/data/dell-lldp-med:sys-config/media-policy/10

JSON content None

- Parameters**
- *ethernet-interface* — Enter the physical Ethernet interface in the format *ethernetnode/slot/port*.
 - *name string* — Enter *ethernetnode/slot/port* to configure the interface that sends LLDP-MED policy TLVs.
 - *policy-id int* — Enter the LLDP-MED network policy number, from 1 to 32.

Example

```
curl -X DELETE -k -u admin:admin -H "accept: application/json" -H "Content-Type: application/json" https://10.11.86.113/restconf/data/dell-lldp-med:sys-config/media-policy/10
```

Remove configured LLDP packet timer — Reset to default

RESTCONF endpoint /restconf/data/global-params/tx-interval

JSON content None

Example

```
curl -X DELETE -k -u admin:admin -H "accept:application/json" -H "Content-Type:application/json" "https://10.11.86.113/restconf/data/global-params/tx-interval"
```

Remove configured LLDPDU hold time — Reset to default

RESTCONF endpoint /restconf/data/global-params/txhold-multiplier

JSON content None

Example

```
curl -X DELETE -k -u admin:admin -H "accept:application/json" -H "Content-Type:application/json" "https://10.11.86.113/restconf/data/global-params/txhold-multiplier"
```

Port-channel

Create port channel

RESTCONF endpoint /restconf/data/interfaces

JSON content

```
{
  "interface": [{
    "type": "iana-if-type:ieee8023adLag",
    "name": "port-channel10"
  }]
}
```

- Parameters**
- *type string* — Enter *iana-if-type:ieee8023adLag* for a port-channel interface.
 - *name string* — Enter *port-channelid-number*, where *id-number* is from 1 to 128.

Example

```
curl -X POST -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces"
-d '{"interface": [{"type": "iana-if-type:ieee8023adLag", "name": "port-
channel10"}]}'
```

Enable port channel

RESTCONF endpoint /restconf/data/interfaces/interface/port-channel10

JSON content

```
{
  "interface": [{
    "type": "iana-if-type:ieee8023adLag",
    "name": "port-channel10",
    "enabled": "true"
  }]
}
```

Parameters

- `port-channelid-number` — Enter `port-channelid-number`, where `port-channel id-number` is from 1 to 128.
- `type string` — Enter `iana-if-type:ieee8023adLag` for a port-channel interface.
- `name string` — Enter `port-channelid-number`.
- `enabled bool` — Enter `true` (no shutdown) to enable the port channel; enter `false` (shutdown) to disable the port channel.

Example

```
curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10"
-d '{"interface": [{"type": "iana-if-type:ieee8023adLag", "name": "port-
channel10", "enabled": "true"}]}'
```

Add member interface to static port channel

RESTCONF endpoint /restconf/data/interfaces/interface/port-channel10

JSON content

```
{
  "interface": [{
    "name": "port-channel10",
    "lag-mode": "STATIC",
    "member-ports": [{
      "name": "ethernet1/1/2"
    }]
  }]
}
```

Parameters

- `port-channelid-number` — Enter `port-channelid-number`, where `port-channel id-number` is from 1 to 128.
- `name string` — Enter `port-channelid-number`.
- `lag-mode bool` — Enter `STATIC` for a statically configured port channel; enter `DYNAMIC` for a dynamically configured port channel.
- `ethernet-interface` — Enter the physical Ethernet interface in the format `ethernetnode/slot/port`.

Example

```
curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10"
-d '{"interface": [{"name": "port-channel10", "lag-mode": "STATIC",
"member-ports": [{"name": "ethernet1/1/2"}]}]}'
```

Add member interface to dynamic port channel

RESTCONF endpoint /restconf/data/interfaces/interface/port-channel20

JSON content

```
{
  "interface": [{
    "name": "port-channel20",
    "lag-mode": "DYNAMIC",
    "member-ports": [{
      "name": "ethernet1/1/5",
      "lACP-mode": "ACTIVE"
    }]
  }]
}
```

Parameters

- `port-channelid-number` — Enter `port-channelid-number`, where `id-number` is from 1 to 128.
- `name string` — Enter `port-channelid-number`.
- `lag-mode bool` — Enter `DYNAMIC` for a dynamically configured port channel; enter `STATIC` for a statically configured port channel.
- `ethernet-interface` — Enter the physical Ethernet interface in the format `ethernetnode/slot/port`.
- `lACP-mode mode` — Enter the LACP actor mode. Valid values are `active`, `on`, and `passive`.

Example

```
curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel20"
-d '{"interface": [{"name": "port-channel20", "lag-mode": "DYNAMIC",
"member-ports": [{"name": "ethernet1/1/5", "lACP-mode": "ACTIVE"}]}]}'
```

Configure minimum links in port channel

RESTCONF endpoint /restconf/data/interfaces/interface/port-channel10

JSON content

```
{
  "interface": [{
    "name": "port-channel10",
    "min-links": 5
  }]
}
```

Parameters

- `port-channelid-number` — Enter `port-channelid-number`, where `port-channel id-number` is from 1 to 128.
- `name string` — Enter `port-channelid-number`.
- `min-links number` — Enter the minimum number of port-channel links that must be in an operational up status for the port channel to be operationally up.

Example

```
curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10"
-d '{"interface": [{"name": "port-channel10", "min-links": 5}]}'
```

Assign IP address to port channel

RESTCONF endpoint /restconf/data/interfaces/interface/port-channel10

JSON content

```
{
  "interface": [{
    "name": "port-channel10",
    "dell-ip:ipv4": {
      "address": {
        "primary-addr": "1.1.1.1/24"
      }
    }
  }]
}
```

```

    }
  }
}

```

Parameters

- `port-channelid-number` — Enter `port-channelid-number`, where `id-number` is from 1 to 128.
- `name string` — Enter `port-channelid-number`.
- `primary-addr A.B.C.D/prefix-length` — Enter the port-channel IP address and mask.

Example

```

curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10"
-d '{"interface": [{"name": "port-channel10", "dell-ip:ipv4":
{"address": {"primary-addr": "1.1.1.1/24"}}}]}'

```

Configure load balancing

RESTCONF endpoint

`/restconf/data/load-balancing/ip-selection`

JSON content

```

{
  "ip-selection": [{
    "destination-ip": "true",
    "source-ip": "true"
  }]
}

```

Parameters

- `destination-ip bool` — Enter `true` to use the destination IP address or the source IP address in the hash calculation; enter `false` to not use the destination IP address or the source IP address.

Example

```

curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/load-balancing/ip-selection"
-d '{"ip-selection": [{"destination-ip": "true", "source-ip": "true"}]}'

```

Change the hash algorithm

RESTCONF endpoint

`/restconf/data/hash-algorithm/lag-algorithms`

JSON content

```

{
  "lag-algorithms": "xor"
}

```

Parameters

- `lag-algorithms mode` — Enter the LAG algorithm. Valid values are `crc`, `xor`, and `seed`.

Example

```

curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/hash-algorithm/lag-algorithms"
-d '{"lag-algorithms": "xor"}'

```

Display port-channel configuration

RESTCONF endpoint

`/restconf/data/interfaces/interface/port-channel10`

JSON content

None

Parameters

- `port-channelid-number` — Enter `port-channelid-number`, where `id-number` is from 1 to 128.

Example

```
curl -X GET -k -u admin:admin -H "accept:application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10"
```

Delete a port-channel configuration

RESTCONF endpoint /restconf/data/interfaces/interface/port-channel10

JSON content None

Parameters

- `port-channel id-number` — Enter `port-channelid-number`, where `id-number` is from 1 to 128.

Example

```
curl -X DELETE -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10"
```

Remove port-channel minimum link configuration

RESTCONF endpoint /restconf/data/interfaces/interface/port-channel10/min-links

JSON content None

Parameters

- `port-channel id-number` — Enter `port-channelid-number`, where `id-number` is from 1 to 128.

Example

```
curl -X DELETE -k -u admin:admin -H "accept:application/json"
-H "Content-Type:application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10/
min-links"
```

VLAN

Create VLAN interface

RESTCONF endpoint /restconf/data/interfaces

JSON content

```
{
  "interface": [{
    "type": "iana-if-type:l2vlan",
    "enabled": true,
    "description": "vlan20",
    "name": "vlan20"
  }]
}
```

Parameters

- `type string` — Enter `iana-if-type:l2vlan` for a VLAN interface.
- `enabled bool` — Enter `true` to enable the VLAN; enter `false` to disable the VLAN.
- `description string` — Enter a text string to describe the VLAN, using a maximum of 80 alphanumeric characters.
- `name string` — Enter `vlan vlan-id`, where `vlan-id` is from 1 to 4093.

Example

```
curl -X POST -u admin:admin -k "https://10.11.86.113/restconf/data/
interfaces"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{ "interface": [{ "type": "iana-if-type:l2vlan", "enabled": true,
"description": "vlan20", "name": "vlan20" } ]}'
```

Configure VLAN IP address

RESTCONF endpoint /restconf/data/interfaces/interface/vlan20

JSON content

```
{
  "interface": [{
    "type": "iana-if-type:l2vlan",
    "enabled": true,
    "description": "vlan20",
    "name": "vlan20",
    "dell-ip:ipv4": {
      "address": {
        "primary-addr": "192.42.10.254/24"
      }
    }
  }]
}
```

Parameters

- `interface` *vlan-id* — Enter the VLAN ID, from 1 to 4093.
- `type` *string* — Enter `iana-if-type:l2vlan` for a VLAN interface.
- `enabled` *bool* — Enter `true` to enable the interface; enter `false` to disable the interface.
- `description` *string* — Enter a text string to describe the VLAN, using a maximum of 80 alphanumeric characters.
- `name` *string* — Enter `vlan vlan-id`, where `vlan-id` is from 1 to 4093.
- `primary-addr` *A.B.C.D/prefix-length* — Enter the VLAN IP address and mask.

Example

```
curl -X PATCH -u admin:admin
-k "https://10.11.86.113/restconf/data/interfaces/interface/vlan20"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{"interface":[{"type":"iana-if-type:l2vlan","enabled":true,
"description":"vlan20","name":"vlan20","dell-ip:ipv4":{"address":
{"primary-addr":"192.42.10.254/24"}}}]}'
```

Change Ethernet port from Access to Trunk mode and enable port

RESTCONF endpoint /restconf/data/interfaces/interface/ethernet1/1/3

JSON content

```
{
  "interface": [{
    "name": "ethernet1/1/3",
    "enabled": "true",
    "dell-interface:mode": "MODE_L2HYBRID"
  }]
}
```

Parameters

- `ethernet-interface` — Enter the physical Ethernet interface in the format `ethernetnode/slot/port`.
- `name` *string* — Enter `vlan vlan-id`, where `vlan-id` is from 1 to 4093.
- `enabled` *bool* — Enter `true` to enable the VLAN; enter `false` to disable the VLAN.
- `mode` *string* — Enter a text value for the port mode. For Access mode, enter `MODE_L2`; for Trunk mode, enter `MODE_L2HYBRID`; for L3 mode, enter `MODE_L2DISABLED`.

Example

```
curl -X PATCH -u admin:admin
-k "https://10.11.86.113/restconf/data/interfaces/interface/
ethernet1%2F1%2F3"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{"interface":[{"name":"ethernet1/1/3", "enabled": "true","dell-
interface:mode":"MODE_L2HYBRID"}]}'
```

Add untagged port to VLAN

RESTCONF endpoint /restconf/data/interfaces/interface/vlan20

JSON content

```
{
  "interface": [{
    "name": "vlan20",
    "type": "iana-if-type:l2vlan",
    "enabled": true,
    "description": "vlan20",
    "dell-interface:untagged-ports": ["ethernet1/1/3"],
    "dell-ip:ipv4": {
      "address": {
        "primary-addr": "192.42.10.254/24"
      }
    }
  }]
}
```

Parameters

- `type` *string* — Enter `iana-if-type:l2vlan` for a VLAN interface.
- `enabled` *bool* — Enter `true` to enable the VLAN; enter `false` to disable the VLAN.
- `description` *string* — Enter a text string to describe the VLAN, using a maximum of (80 alphanumeric characters).
- `name` *string* — Enter `vlan` *vlan-id*, where *vlan-id* is from 1 to 4093.
- `untagged-ports` *string* — Enter the untagged port interface in the format `ethernetnode/slot/port`.
- `primary-addr` *A.B.C.D/prefix-length* — Enter the VLAN IP address and mask.

Example

```
curl -X PATCH -u admin:admin
-k "https://10.11.86.113/restconf/data/interfaces/interface/vlan20"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{"interface":[{"name":"vlan20","type":"iana-if-type:l2vlan",
"enabled":true,"description":"vlan20","dell-interface:untagged-ports":
["ethernet1/1/3"],"dell-ip:ipv4":
{"address":{"primary-addr":"192.42.10.254/24"}}}]}'
```

Display VLAN configuration

RESTCONF endpoint /restconf/data/interfaces/interface/vlan20

JSON content None

Parameters • `interface` *vlan-id* — Enter the VLAN ID, from 1 to 4093.

Example

```
curl -X GET -u admin:admin
-k "https://10.11.86.113/restconf/data/interfaces/interface/vlan20"
-H "accept: application/json"
```

Delete a VLAN configuration

RESTCONF endpoint /restconf/data/interfaces/interface/vlan10

JSON content None

Parameters • `interface` *vlan-id* — Enter the VLAN ID, from 1 to 4093.

Example

```
curl -X DELETE -u admin:admin
-k "https://10.11.86.113/restconf/data/interfaces/interface/vlan10"
-H "accept: application/json"
```

VLT

Create VLT domain on each peer

RESTCONF endpoint /restconf/data

JSON content

```
{
  "node-topology": [{
    "topology-id": 1,
    "topology-type": "VLT",
    "dell-vlt:vlt-domain": {}
  }]
}
```

- Parameters**
- `topology-id int` — Configure the same VLT domain ID on each peer, from 1 to 255.
 - `topology-type value` — Enter VLT for a VLT domain.

Example

```
curl -X POST -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json" "https://10.11.86.113/restconf/data"
-d '{"node-topology": [{"topology-id":1, "topology-type":"VLT", "dell-
vlt:vlt-domain":{}}]}'
```

Configure and enable VLTi ports in L2 Access mode

RESTCONF endpoint /restconf/data/interfaces/interface=ethernet1/1/1

JSON content

```
{
  "interface": [{
    "name": "ethernet1/1/1",
    "enabled": "true",
    "dell-interface:mode": "MODE_L2DISABLED"
  }]
}
```

- Parameters**
- `ethernet-interface` — Enter the physical Ethernet interface in the format `ethernetnode/slot/port`.
 - `name string` — Enter `ethernetnode/slot/port` to identify the VLTi port on each peer.
 - `enabled bool` — Enter `true` (no shutdown) to enable the VLTi port; enter `false` (shutdown) to disable the VLTi port.
 - `dell-interface:mode string` — Enter `MODE_L2DISABLED` to disable L2 switching (switchport mode) on the VLTi port.

Example

```
curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/
interface=ethernet1%2F1%2F1"
-d '{"interface": [{"name":"ethernet1/1/1",
"enabled": "true", "dell-interface:mode":"MODE_L2DISABLED"}]}'
```

Configure VLTi interfaces on each peer

RESTCONF endpoint /restconf/data/node-topology/1

JSON content

```
{
  "node-topology": [{
    "topology-id": 1,
    "discovery-interface": ["ethernet1/1/1"],
    "topology-type": "VLT",
    "dell-vlt:vlt-domain": {}
  }]
}
```

- Parameters**
- `topology-id int` — Enter the same VLT domain ID on each peer, from 1 to 255.

- `discovery-interface string` — Enter `ethernetnode/slot/port` for the VLTi discovery interface on each peer.
- `topology-type value` — Enter VLT for a VLT domain.

Example

```
curl -X PATCH -k -u admin:admin "https://10.11.86.113/restconf/data/node-topology/1"
-H "accept: application/json"
-H "Content-Type: application/json"
-d '{"node-topology":[{"topology-id":1, "discovery-interface":
["ethernet1/1/1"], "topology-type":"VLT", "dell-vlt:vlt-domain":{}}]}
```

Configure VLT port channel between peers

RESTCONF endpoint `/restconf/data/interfaces`

JSON content

```
{
  "interface": [{
    "type": "iana-if-type:ieee8023adLag",
    "name": "port-channel10"
  }]
}
```

Parameters

- `type string` — Enter `iana-if-type:ieee8023adLag` for a port-channel interface.
- `name string` — Enter `port-channel id-number`, where `id-number` is from 1 to 128.

Example

```
curl -X POST -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json" "https://10.11.86.113/restconf/data/interfaces"
-d '{"interface": [{"type":"iana-if-type:ieee8023adLag", "name":"port-channel10"}]}
```

Assign VLT port-channel ID to VLT port channel

RESTCONF endpoint `/restconf/data/interfaces/interface/port-channel10`

JSON content

```
{
  "interface": [{
    "type": "iana-if-type:ieee8023adLag",
    "name": "port-channel10",
    "enabled": "true",
    "dell-vlt:vlt": {
      "vlt-id": "1"
    }
  }]
}
```

Parameters

- `port-channelid-number` — Enter `port-channelid-number`, where `id-number` is 1 to 128.
- `type string` — Enter `iana-if-type:ieee8023adLag` for a port-channel interface.
- `name string` — Enter `port-channelid-number`.
- `enabled bool` — Enter `true` (no shutdown) to enable the port channel; enter `false` (shutdown) to disable the port channel.
- `vlt-id int` — Enter the VLT port-channel ID, from 1 to 1024.

Example

```
curl -X PATCH -k -u admin:admin -H "accept: application/json"
-H "Content-Type: application/json"
"https://10.11.86.113/restconf/data/interfaces/interface/port-channel10"
-d '{"interface":[{"type":"iana-if-type:ieee8023adLag", "name":"port-channel10",
"enabled":"true", "dell-vlt:vlt":{"vlt-id":"1"}}]}
```

Delete VLT domain

RESTCONF endpoint	/restconf/data/node-topology/1
JSON content	None
Parameters	<ul style="list-style-type: none">• <code>topology-id int</code> — Specify the same VLT domain ID on each peer, from 1 to 255.
Example	<pre>curl -X DELETE -k -u admin:admin -H "accept: application/json" -H "Content-Type: application/json" "https://10.11.86.113/restconf/data/node-topology/1"</pre>

Troubleshoot OS10

Critical workloads and applications require constant availability. Dell EMC Networking offers tools to help you monitor and troubleshoot problems before they happen.

Packet and flow capture	Packet and traffic management
Metrics measurement	Ping, round-trip time, jitter, response time, and so on
Analysis and reporting	Metrics and packet capturing
Alerting	Triggers problem reporting
Logging	Captures system history
Performance monitoring	Establishes baselines and defines triggers for detecting performance problems
Mapping and representation	Defines device locations and status

Dell EMC recommends the following best practices:

- View traffic end-to-end from the application's view point.
- Deploy “just-in-time” network management infrastructure rapidly, where needed, when needed, and on-demand.
- Extend analysis beyond the network and watch traffic to and from your host.
- Focus on real-time assessment and use trend analysis to backup your conclusions.
- Emphasize *effective* over *absolute* — leverage management solutions that resolve your most common, most expensive problem quickly.
- Address networking performance issues before you focus on the application performance.
- Use methodologies and technologies that fit your network and needs.
- Continuously monitor performance and availability as a baseline for system performance and system up time to quickly separate network issues from application issues.

Diagnostic tools

This section contains information on advanced software and hardware commands to debug, monitor, and troubleshoot network devices. Output examples are for reference purposes only and may not apply to your specific system.

View inventory

Use the `show inventory` command to view the module IDs of the device..

```
OS10# show inventory
Product       : S4048T-ON
Description   : S4048T-ON 48x10GbE copper, 6x40GbE QSFP+ Interface Module
Software version : 10.4.1

Unit Type          Part Number  Rev  Piece Part ID          Svc Tag  Exprs Svc
Code
-----
--
* 1 S4048T-ON          0YVCK0   X01  TW-0YVCK0-28298-615-0023
  1 S4048T-ON-PWR-1-UNKNOW          ----
  1 S4048T-ON-FANTRAY-1          061DJT   X01  TW-061DJT-28298-615-0089
  1 S4048T-ON-FANTRAY-2          061DJT   X01  TW-061DJT-28298-615-0090
  1 S4048T-ON-FANTRAY-3          061DJT   X01  TW-061DJT-28298-615-0091
```

Boot partition and image

Display system boot partition-related and image-related information.

- View all boot information in EXEC mode.

```
show boot
```

- View boot details in EXEC mode.

```
show boot detail
```

View boot information

```
OS10# show boot
Current system image information:
=====
Type          Boot Type  Active          Standby          Next-Boot
-----
Node-id 1 Flash Boot [A] 10.1.9999P.2182 [B] 10.1.9999P.2182 [A] active
```

View boot detail

```
OS10# show boot detail
Current system image information detail:
=====
Type:                Node-id 1
Boot Type:           Flash Boot
Active Partition:    A
Active SW Version:   10.1.9999P.2182
Active Kernel Version: Linux 3.16.7-ckt20
Active Build Date/Time: 2016-07-12T20:47:17Z
Standby Partition:   B
Standby SW Version:  10.1.9999P.2182
Standby Build Date/Time: 2016-07-12T20:47:17Z
Next-Boot:           active[A]
```

Monitor processes

Display CPU process information.

- View process CPU utilization information in EXEC mode.

- `show processes node-id node-id-number [pid process-id]`

View CPU utilization

```
OS10# show processes node-id 1
top - 09:19:32 up 5 days, 6 min, 2 users, load average: 0.45, 0.39, 0.34
Tasks: 208 total, 2 running, 204 sleeping, 0 stopped, 2 zombie
%Cpu(s): 9.7 us, 3.9 sy, 0.3 ni, 85.8 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st
KiB Mem: 3998588 total, 2089416 used, 1909172 free, 143772 buffers
KiB Swap: 399856 total, 0 used, 399856 free. 483276 cached Mem
  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+  COMMAND
    9 root        20   0     0     0     0   S   6.1   0.0    5:22.41 rcuos/1
   819 snmp       20   0   52736   6696  4132  S   6.1   0.2    2:44.18 snmpd
 30452 admin      20   0   22076   2524  2100  R   6.1   0.1    0:00.02 top
    1 root        20   0  112100   5840  3032  S   0.0   0.1    0:12.32 systemd
    2 root        20   0     0     0     0   S   0.0   0.0    0:00.00 kthreadd
    3 root        20   0     0     0     0   S   0.0   0.0    0:25.37 ksoftirqd/0
    5 root        0 -20     0     0     0   S   0.0   0.0    0:00.00 kworker/0:+
    7 root        20   0     0     0     0   R   0.0   0.0    5:15.27 rcu_sched
    8 root        20   0     0     0     0   S   0.0   0.0    2:43.64 rcuos/0
   10 root        20   0     0     0     0   S   0.0   0.0    0:00.00 rcu_bh
```



```

11 root      20    0    0    0    0 S    0.0  0.0   0:00.00 rcuob/0
12 root      20    0    0    0    0 S    0.0  0.0   0:00.00 rcuob/1
13 root      rt     0    0    0    0 S    0.0  0.0   0:07.30 migration/0
14 root      rt     0    0    0    0 S    0.0  0.0   0:02.18 watchdog/0
15 root      rt     0    0    0    0 S    0.0  0.0   0:02.12 watchdog/1
16 root      rt     0    0    0    0 S    0.0  0.0   0:04.98 migration/1
17 root      20    0    0    0    0 S    0.0  0.0   0:03.92 ksoftirqd/1
19 root      0 -20    0    0    0 S    0.0  0.0   0:00.00 kworker/1:+
20 root      0 -20    0    0    0 S    0.0  0.0   0:00.00 khelper
21 root      20    0    0    0    0 S    0.0  0.0   0:00.00 kdevtmpfs
22 root      0 -20    0    0    0 S    0.0  0.0   0:00.00 netns
23 root      20    0    0    0    0 S    0.0  0.0   0:00.41 khungtaskd
24 root      0 -20    0    0    0 S    0.0  0.0   0:00.00 writeback
25 root      25    5    0    0    0 S    0.0  0.0   0:00.00 ksm
--more--

```

```

OS10# show processes node-id 1 pid 1019
top - 09:21:58 up 5 days, 8 min, 2 users,  load average: 0.18, 0.30, 0.31
Tasks:  1 total,  0 running,  1 sleeping,  0 stopped,  0 zombie
%Cpu(s):  9.7 us,  3.9 sy,  0.3 ni, 85.8 id,  0.0 wa,  0.0 hi,  0.3 si,  0.0 st
KiB Mem:  3998588 total, 2089040 used, 1909548 free, 143772 buffers
KiB Swap:  399856 total,  0 used,  399856 free. 483276 cached Mem
  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+  COMMAND
  1019 root      20   0 1829416 256080 73508  S   6.6   6.4   1212:36 base_nas
OS10#

```

LED settings

Beacon LEDs enable to identify the location of ports and system with blinking or glowing LEDs.

Change current state of the location LED of the system or interface using the following commands:

```
location-led system {node-id | node-id/unit-id} {on | off}
```

```
location-led interface ethernet {chassis/slot/port[:subport]} {on | off}
```

Change the state of system location LED

```
OS10# location-led system 1 on
OS10# location-led system 1 off
```

Change the state of interface location LED

```
OS10# location-led interface ethernet 1/1/1 on
OS10# location-led interface ethernet 1/1/1 off
```

Packet analysis

Use the Linux `tcpdump` command to analyze network packets. Use filters to limit packet collection and output. You must be logged into the Linux shell to use this command (see [Log into OS10 Device](#)).

Use the `tcpdump` command without parameters to view packets that flow through all interfaces. To write captured packets to a file, use the `-w` parameter. To read the captured file output offline, you can use open source software packages such as **wireshark**.

Capture packets from Ethernet interface

```

$ tcpdump -i e101-003-0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on e101-003-0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:39:22.457185 IP 3.3.3.1 > 3.3.3.4: ICMP echo request, id 5320, seq 26, length 64
01:39:22.457281 IP 3.3.3.1 > 3.3.3.4: ICMP echo reply, id 5320, seq 26, length 64

```

Capture two packets from interface

```
$ tcpdump -c 2 -i e101-003-0
listening on e101-003-0, link-type EN10MB (Ethernet), capture size 96 bytes
01:39:22.457185 IP 3.3.3.1 > 3.3.3.4: ICMP echo request, id 5320, seq 26, length 64
01:39:22.457281 IP 3.3.3.1 > 3.3.3.4: ICMP echo reply, id 5320, seq 26, length 64
2 packets captured
13 packets received by filter
0 packets dropped by kernel
```

Capture packets and write to file

```
$ tcpdump -w 06102016.pcap -i e101-003-0
listening on e101-003-0, link-type EN10MB (Ethernet), capture size 96 bytes
32 packets captured
32 packets received by filter
0 packets dropped by kernel
```

Port adapters and modules

Use the `show diag` command to view diagnostics information for OS10 port adapters and hardware modules.

View diagnostic hardware information

```
OS10# show diag
00:00.0 Host bridge: Intel Corporation Atom Processor S1200 Internal (rev 02)
00:01.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 1 (rev 02)
00:02.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 2 (rev 02)
00:03.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 3 (rev 02)
00:04.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 4 (rev 02)
00:0e.0 IOMMU: Intel Corporation Atom Processor S1200 Internal (rev 02)
00:13.0 System peripheral: Intel Corporation Atom Processor S1200 SMBus 2.0 Controller 0 (rev 02)
00:13.1 System peripheral: Intel Corporation Atom Processor S1200 SMBus 2.0 Controller 1 (rev 02)
00:14.0 Serial controller: Intel Corporation Atom Processor S1200 UART (rev 02)
00:1f.0 ISA bridge: Intel Corporation Atom Processor S1200 Integrated Legacy Bus (rev 02)
01:00.0 Ethernet controller: Broadcom Corporation Device b850 (rev 03)
02:00.0 SATA controller: Marvell Technology Group Ltd. Device 9170 (rev 12)
03:00.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
04:01.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
04:02.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
04:03.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
07:00.0 USB controller: Pericom Semiconductor PI7C9X442SL USB OHCI Controller (rev 01)
07:00.1 USB controller: Pericom Semiconductor PI7C9X442SL USB OHCI Controller (rev 01)
07:00.2 USB controller: Pericom Semiconductor PI7C9X442SL USB EHCI Controller (rev 01)
08:00.0 Ethernet controller: Intel Corporation 82574L Gigabit Network Connection
```

Test network connectivity

Use the `ping` and `traceroute` commands to test network connectivity. When you *ping* an IP address, you send packets to a destination and wait for a response. If there is no response, the destination is not active. The `ping` command is useful during configuration if you have problems connecting to a hostname or IP address.

When you execute `traceroute`, the output shows the path a packet takes from your device to the destination IP address. It also lists all intermediate hops (routers) that the packet traverses to reach its destination, including the total number of hops traversed.

Check IPv4 connectivity

```
OS10# ping 172.31.1.255

Type Ctrl-C to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2 seconds:
Reply to request 1 from 172.31.1.208 0 ms
Reply to request 1 from 172.31.1.216 0 ms
Reply to request 1 from 172.31.1.205 16 ms
::
Reply to request 5 from 172.31.1.209 0 ms
Reply to request 5 from 172.31.1.66 0 ms
Reply to request 5 from 172.31.1.87 0 ms
```

Check IPv6 connectivity

```
OS10# ping 100::1

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max = 0/0/0 (ms)
```

Trace IPv4 network route

```
OS10# traceroute www.Dell Networking.com

Translating "www.Dell Networking.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.

-----
Tracing the route to www.Dell Networking.com (10.11.84.18),
30 hops max, 40 byte packets
-----
TTL  Hostname          Probel      Probe2      Probe3
 1  10.11.199.190 001.000 ms 001.000 ms 002.000 ms
 2  gwegress-sjc-02.Dell Networking.com (10.11.30.126) 005.000 ms 001.000 ms 001.000 ms
 3  fw-sjc-01.Dell Networking.com (10.11.127.254) 000.000 ms 000.000 ms 000.000 ms
 4  www.Dell Networking.com (10.11.84.18) 000.000 ms 000.000 ms 000.000 ms
```

Trace IPv6 network route

```
OS10# traceroute 100::1

Type Ctrl-C to abort.

-----
Tracing the route to 100::1, 64 hops max, 60 byte packets
-----
Hops  Hostname          Probel      Probe2      Probe3
 1    100::1 000.000 ms 000.000 ms 000.000 ms

OS10# traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b

Type Ctrl-C to abort.

-----
Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b,
64 hops max, 60 byte packets
-----
Hops  Hostname          Probel      Probe2      Probe3
 1    3ffe:501:ffff:100:201:e8ff:fe00:4c8b
      000.000 ms 000.000 ms 000.000 ms
```

View diagnostics

View system diagnostic information using show commands. The show hash-algorithm command is used to view the current hash algorithms configured for LAG and ECMP.

View environment

```
OS10# show environment
```

Unit	State	Temperature
1	up	43

Thermal sensors			
Unit	Sensor-Id	Sensor-name	Temperature
1	1	CPU On-Board temp sensor	32
1	2	Switch board temp sensor	28
1	3	System Inlet Ambient-1 temp sensor	27
1	4	System Inlet Ambient-2 temp sensor	25
1	5	System Inlet Ambient-3 temp sensor	26
1	6	Switch board 2 temp sensor	31
1	7	Switch board 3 temp sensor	41
1	8	NPU temp sensor	43

View hash algorithm

```
OS10# show hash-algorithm
LagAlgo - CRC EcmpAlgo - CRC
```

View inventory

```
OS10# show inventory
Product       : S4048ON
Description   : S4048-ON 48x10GbE, 6x40GbE QSFP+ Interface Module
Software version : 10.4.1
```

Unit Code	Type	Part Number	Rev	Piece Part ID	Svc Tag	Exprs	Svc
* 1	S4048ON			----			
1	S4048ON-PWR-2-AC-R	0T9FNW	X01	TW-0T9FNW-28298-49Q-0034	AEIOU##	226 457	410
55							
1	S4048ON-FANTRAY-1-R	0MGDH8	X01	TW-0MGDH8-28298-49Q-0451	AEIOU##	226 457	410
55							
1	S4048ON-FANTRAY-2-R	0MGDH8	X01	TW-0MGDH8-28298-49Q-0450	AEIOU##	226 457	410
55							
1	S4048ON-FANTRAY-3	P1FAN1	A01	CN-123456-FAN10-058-901			

View system information

```
OS10#show system
```

```
Node Id       : 1
MAC           : 34:17:18:19:20:21
Number of MACs : 0
Up Time       : 1 week 4 days 08:08:17
```

```
-- Unit 1 --
```

```
Status       : up
System Identifier : 1
Down Reason   :
System Location LED : off
Required Type  : S4048
Current Type   : S4048
Hardware Revision :
Software Version : 10.3.9999E(X)
Physical Ports : 48x10GbE, 6x40GbE
BIOS          : 3.21.0.4
System CPLD    : 15
Master CPLD    : 12
Slave CPLD     : 5
```

```
-- Power Supplies --
```

PSU-ID	Status	Type	AirFlow	Fan	Speed(rpm)	Status
--------	--------	------	---------	-----	------------	--------

```

-----
1      fail
2      up          AC          REVERSE    1      14720          up

-- Fan Status --
FanTray  Status      AirFlow   Fan   Speed (rpm)   Status
-----
1      up          REVERSE   1     13063         up
                REVERSE   2     13063         up
2      up          REVERSE   1     13020         up
                REVERSE   2     12977         up
3      up          NORMAL    1     13085         up
                NORMAL    2     13063         up

```

Diagnostic commands

location-led interface

Changes the location LED of the interface.

- Syntax** `location-led interface ethernet {chassis/slot/port[:subport]} {on | off}`
- Parameters**
 - `chassis/slot/port[:subport]` — Enter the ethernet interface number.
 - `on | off` — Set the interface LED to be on or off.
- Default** Not configured
- Command Mode** EXEC
- Usage Information** Use the `location-led interface` command to change the location LED for the specified interface.
- Example**

```
OS10# location-led interface ethernet 1/1/1 on
OS10# location-led interface ethernet 1/1/1 off
```
- Supported Releases** 10.3.0E or later

location-led system

Changes the location LED of the system.

- Syntax** `location-led system {node-id | node-id/unit-id} {on | off}`
- Parameters**
 - `node-id | node-id/unit-id` — Enter the system ID.
 - `on | off` — Set the system LED to be on or off.
- Default** Not configured
- Command Mode** EXEC
- Usage Information** Use the `location-led system` command to change the location LED for the specified system ID.
- Example**

```
OS10# location-led system 1 on
OS10# location-led system 1 off
```
- Supported Releases** 10.3.0E or later

ping

Tests network connectivity to an IPv4 device.

Syntax ping [vrf {management | vrf-name}] [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface] [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline] [-W timeout] [hop1 ...] destination

- Parameters**
- vrf management — (Optional) Pings an IP address in the management VRF instance.
 - vrf vrf-name — (Optional) Ping an IP address in the specified VRF instance.
 - -a — (Optional) Audible ping.
 - -A — (Optional) Adaptive ping. An inter-packet interval adapts to the round-trip time so that not more than one (or more, if preload option is set) unanswered probe is present in the network. The minimum interval is 200 msec 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 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.
 - -h — (Optional) View help for this command.
 - -i interval — (Optional) Enter the interval in seconds to wait between sending each packet (default 1 second).
 - -i interval — (Optional) Enter the number of seconds to wait before sending the next packet (0 to 60, default 1).
 - -I interface-address — (Optional) Enter the source interface address (with no spaces):
 - For a physical Ethernet interface, enter ethernetnode/slot/port; for example, ethernet1/1/1.
 - For a VLAN interface, enter vlanvlan-id; for example, vlan10.
 - For a loopback interface, enter loopbackid; for example, loopback1.
 - For a port-channel interface, enter port-channelchannel-id; for example, port-channel1.
 - -l preload — (Optional) Enter the number of packets that ping sends before waiting for a reply. Only a super-user may preload more than 3.
 - -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 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 up to 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 the number of datagrams (up to 1500 bytes in decimal or hex) to set quality of service (QoS)-related bits.
 - -s packetsize — (Optional) Enter the number of data bytes to send (1 to 65468, default 56).
 - -S sndbuf — (Optional) Set the sndbuf socket. By default, the sndbuf socket buffers one packet maximum.
 - -t ttl — (Optional) Enter the IP time-to-live (TTL) value in seconds.
 - -T timestamp_option — (Optional) Set special IP timestamp options. Valid values for timestamp_option — tsonly (only timestamps), tsandaddr (timestamps and addresses) or tsprespec host1 [host2 [host3 [host4]]] (timestamp pre-specified hops).
 - -v — (Optional) Verbose output.
 - -V — (Optional) Display version and exit.

- `-w deadline` — (Optional) Enter the time-out value, in seconds, before the ping exits regardless of how many packets are sent or received.
- `-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).
- `hop1 ...` (Optional) Enter the IP addresses of the pre-specified hops for the ping packet to take.
- `target` — Enter the IP address where you are testing connectivity.

Default Not configured

Command Mode EXEC

Usage Information This command uses an ICMP ECHO_REQUEST datagram to receive an ICMP ECHO_RESPONSE from a network host or gateway. Each ping packet has an IP and ICMP header, followed by 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 then measures the time 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 IP address, number of bytes sent, lapse time (in milliseconds), and time to live (TTL) which is the number of hops back from the source to the destination.

Example

```
OS10# ping 20.1.1.1
PING 20.1.1.1 (20.1.1.1) 56(84) bytes of data.
64 bytes from 20.1.1.1: icmp_seq=1 ttl=64 time=0.079 ms
64 bytes from 20.1.1.1: icmp_seq=2 ttl=64 time=0.081 ms
64 bytes from 20.1.1.1: icmp_seq=3 ttl=64 time=0.133 ms
64 bytes from 20.1.1.1: icmp_seq=4 ttl=64 time=0.124 ms
^C
--- 20.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.079/0.104/0.133/0.025 ms
```

Supported Releases 10.2.0E or later

ping6

Tests network connectivity to an IPv6 device.

Syntax `ping6 [vrf {management | vrf-name}] [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface] [-l preload] [-m mark] [-M pmtudisc_option] [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline] [-W timeout] destination`

- Parameters**
- `vrf management` — (Optional) Pings an IPv6 address in the management VRF instance.
 - `vrf vrf-name` — (Optional) Pings an IPv6 address in the specified VRF instance.
 - `-a` — (Optional) Audible ping.
 - `-A` — (Optional) Adaptive ping. An inter-packet interval adapts to the round-trip time so that not more than one (or more, if preload option is set) unanswered probe is present in the network. The minimum interval is 200 msec 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 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 flowlabel` — (Optional) Sets a 20-bit flow label on echo request packets. If value is zero, the kernel allocates a random flow label.
 - `-h` — (Optional) View help for this command.
 - `-i interval` — (Optional) Enter the number of seconds to wait before sending the next packet (0 to 60, default 1).

- `-i interval` — (Optional) Enter the interval, in seconds, to wait between sending each packet (default 1 second).
- `-I interface-address` — (Optional) Enter the source interface address (with no spaces):
 - For a physical Ethernet interface, enter `ethernetnode/slot/port`; for example, `ethernet1/1/1`.
 - For a VLAN interface, enter `vlanvlan-id`; for example, `vlan10`.
 - For a loopback interface, enter `loopbackid`; for example, `loopback1`.
 - For a port-channel interface, enter `port-channelchannel-id`; for example, `port-channel1`.
- `-l preload` — (Optional) Enter the number of packets that ping sends before waiting for a reply. Only a super-user may preload more than 3.
- `-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 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 up to 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 the number of datagrams (up to 1500 bytes in decimal or hex) to set quality of service (QoS)-related bits.
- `-s packetsize` — (Optional) Enter the number of data bytes to send (1 to 65468, default 56).
- `-S sndbuf` — (Optional) Set the sndbuf socket. By default, the sndbuf socket buffers one packet maximum.
- `-t ttl` — (Optional) Enter the IP time-to-live (TTL) value in seconds.
- `-T timestamp_option` — (Optional) Set special IP timestamp options. Valid values for `timestamp_option` — `tsonly` (only timestamps), `tsandaddr` (timestamps and addresses) or `tsprespec host1 [host2 [host3 [host4]]]` (timestamp pre-specified hops).
- `-v` — (Optional) Verbose output.
- `-V` — (Optional) Display version and exit.
- `-w deadline` — (Optional) Enter the time-out value, in seconds, before the ping exits regardless of how many packets are sent or received.
- `-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).
- `hop1 ...` (Optional) Enter the IPv6 addresses of the pre-specified hops for the ping packet to take.
- `target` — Enter the IPv6 destination address in A:B::C:D format, where you are testing connectivity.

Default Not configured

Command Mode EXEC

Usage Information This command uses an ICMP ECHO_REQUEST datagram to receive an ICMP ECHO_RESPONSE from a network host or gateway. Each ping packet has an IPv6 and ICMP header, followed by a time value and a number of "pad" bytes used to fill out the packet. A pingv6 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

```
OS10# 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
```

Supported Releases 10.2.0E or later

show boot

Displays boot partition-related information.

- Syntax** show boot [detail]
- Parameters** detail — (Optional) Enter to display detailed information.
- Default** Not configured
- Command Mode** EXEC
- Usage Information** Use the `boot system` command to set the boot partition for the next reboot.

Example

```
OS10# show boot
Current system image information:
=====
Type          Boot Type   Active      Standby      Next-Boot
-----
Node-id 1    Flash Boot [B] 10.2.0E    [A] 10.2.0E  [B] active
```

Example (Detail)

```
OS10# show boot detail
Current system image information detail:
=====
Type:                Node-id 1
Boot Type:           Flash Boot
Active Partition:    B
Active SW Version:   10.2.0E
Active Kernel Version: Linux 3.16.7-ckt25
Active Build Date/Time: 2016-10-03T23:11:14Z
Standby Partition:   A
Standby SW Version:  10.2.0E
Standby Build Date/Time: 2016-10-03T23:11:14Z
Next-Boot:           active[B]
```

- Supported Releases** 10.2.0E or later

show diag

Displays diagnostic information for port adapters and modules.

- Syntax** show diag
- Parameters** None
- Default** Not configured
- Command Mode** EXEC
- Usage Information** None

Example

```
OS10# show diag
00:00.0 Host bridge: Intel Corporation Atom processor C2000 SoC
Transaction Router (rev 02)
00:01.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 1 (rev 02)
00:02.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 2 (rev 02)
00:03.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 3 (rev 02)
00:04.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 4 (rev 02)
00:0e.0 Host bridge: Intel Corporation Atom processor C2000 RAS (rev 02)
00:0f.0 IOMMU: Intel Corporation Atom processor C2000 RCEC (rev 02)
```

```

00:13.0 System peripheral: Intel Corporation Atom processor C2000 SMBus
2.0 (rev 02)
00:14.0 Ethernet controller: Intel Corporation Ethernet Connection I354
(rev 03)
00:14.1 Ethernet controller: Intel Corporation Ethernet Connection I354
(rev 03)
00:16.0 USB controller: Intel Corporation Atom processor C2000 USB
Enhanced Host Controller (rev 02)
00:17.0 SATA controller: Intel Corporation Atom processor C2000 AHCI
SATA2 Controller (rev 02)
00:18.0 SATA controller: Intel Corporation Atom processor C2000 AHCI
SATA3 Controller (rev 02)
00:1f.0 ISA bridge: Intel Corporation Atom processor C2000 PCU (rev 02)
00:1f.3 SMBus: Intel Corporation Atom processor C2000 PCU SMBus (rev 02)
01:00.0 Ethernet controller: Broadcom Corporation Device b340 (rev 01)
01:00.1 Ethernet controller: Broadcom Corporation Device b340 (rev 01)

```

Supported Releases 10.2.0E or later

show environment

Displays information about environmental system components, such as temperature, fan, and voltage.

Syntax show environment

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```

OS10# show environment

Unit      State      Temperature
-----
1         up         43

Thermal sensors
Unit      Sensor-Id  Sensor-name                                     Temperature
-----
1         1          CPU On-Board temp sensor                       32
1         2          Switch board temp sensor                       28
1         3          System Inlet Ambient-1 temp sensor             27
1         4          System Inlet Ambient-2 temp sensor             25
1         5          System Inlet Ambient-3 temp sensor             26
1         6          Switch board 2 temp sensor                     31
1         7          Switch board 3 temp sensor                     41
1         8          NPU temp sensor                               43

```

Supported Releases 10.2.0E or later

show hash-algorithm

Displays hash algorithm information.

Syntax show hash-algorithm

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show hash-algorithm
LagAlgo - CRC EcmpAlgo - CRC
```

Supported Releases 10.2.0E or later

show inventory

Displays system inventory information.

Syntax show inventory

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show inventory
Product       : S4048ON
Description   : S4048-ON 48x10GbE, 6x40GbE QSFP+ Interface Module
Software version : 10.4.1.0.X.9
```

Unit	Type	Part Number	Rev	Piece	Part ID	Svc Tag	Exprs
*	1	S4048ON		----			
	1	S4048ON-PWR-2-AC-R	0T9FNW	X01	TW-0T9FNW-28298-49Q-0034	AEIOU##	226 4
	1	S4048ON-FANTRAY-1-R	OMGDH8	X01	TW-OMGDH8-28298-49Q-0451	AEIOU##	226 4
	1	S4048ON-FANTRAY-2-R	OMGDH8	X01	TW-OMGDH8-28298-49Q-0450	AEIOU##	226 4
	1	S4048ON-FANTRAY-3	P1FAN1	A01	CN-123456-FAN10-058-901		

Supported Releases 10.2.0E or later

show processes

View process CPU utilization information.

Syntax show processes node-id node-id-number [pid process-id]

Parameters

- *node-id-number* — Enter the Node ID number <1-1>.
- *process-id* — (Optional) Enter the process ID number <1-2147483647>.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show processes node-id 1
top - 09:19:32 up 5 days, 6 min,  2 users,  load average: 0.45, 0.39,
0.34
Tasks: 208 total,  2 running, 204 sleeping,  0 stopped,  2 zombie
%Cpu(s):  9.7 us,  3.9 sy,  0.3 ni, 85.8 id,  0.0 wa,  0.0 hi,  0.3 si,
0.0 st
KiB Mem:  3998588 total, 2089416 used, 1909172 free, 143772 buffers
KiB Swap:  399856 total,    0 used, 399856 free. 483276 cached
Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+
COMMAND										
9	root	20	0	0	0	0	S	6.1	0.0	5:22.41
rcuos/1										
819	snmp	20	0	52736	6696	4132	S	6.1	0.2	2:44.18
30452	admin	20	0	22076	2524	2100	R	6.1	0.1	0:00.02
snmpd top										
1	root	20	0	112100	5840	3032	S	0.0	0.1	0:12.32
systemd										
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00
kthreadd										
3	root	20	0	0	0	0	S	0.0	0.0	0:25.37
ksoftirqd/0										
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00
kworker/0:+										
7	root	20	0	0	0	0	R	0.0	0.0	5:15.27
rcu_sched										
8	root	20	0	0	0	0	S	0.0	0.0	2:43.64
rcuos/0										
10	root	20	0	0	0	0	S	0.0	0.0	0:00.00
rcu_bh										
11	root	20	0	0	0	0	S	0.0	0.0	0:00.00
rcuob/0										
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00
rcuob/1										
13	root	rt	0	0	0	0	S	0.0	0.0	0:07.30
migration/0										
14	root	rt	0	0	0	0	S	0.0	0.0	0:02.18
watchdog/0										
15	root	rt	0	0	0	0	S	0.0	0.0	0:02.12
watchdog/1										
16	root	rt	0	0	0	0	S	0.0	0.0	0:04.98
migration/1										
17	root	20	0	0	0	0	S	0.0	0.0	0:03.92
ksoftirqd/1										
19	root	0	-20	0	0	0	S	0.0	0.0	0:00.00
kworker/1:+										
20	root	0	-20	0	0	0	S	0.0	0.0	0:00.00
khelper										
21	root	20	0	0	0	0	S	0.0	0.0	0:00.00
kdevtmpfs										
22	root	0	-20	0	0	0	S	0.0	0.0	0:00.00
netns										
23	root	20	0	0	0	0	S	0.0	0.0	0:00.41
khungtaskd										
24	root	0	-20	0	0	0	S	0.0	0.0	0:00.00
writeback										
25	root	25	5	0	0	0	S	0.0	0.0	0:00.00
ksmd										
--more--										

```

OS10# show processes node-id 1 pid 1019
top - 09:21:58 up 5 days, 8 min, 2 users, load average: 0.18, 0.30, 0.31
Tasks: 1 total, 0 running, 1 sleeping, 0 stopped, 0 zombie
%Cpu(s): 9.7 us, 3.9 sy, 0.3 ni, 85.8 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st
KiB Mem: 3998588 total, 2089040 used, 1909548 free, 143772 buffers
KiB Swap: 399856 total, 0 used, 399856 free. 483276 cached Mem
  PID USER      PR  NI  VIRT  RES  SHR S  %CPU  %MEM    TIME+
  COMMAND
  1019 root      20   0 1829416 256080 73508 S   6.6   6.4  1212:36
base_nas
OS10#

```

Supported Releases

10.3.0E or later

show system

Displays system information.

- Syntax** show system [brief | node-id]
- Parameters**
- **brief** — View abbreviated list of system information.
 - **node-id** — Node ID number.
- Default** Not configured
- Command Mode** EXEC
- Usage Information** None
- Example**

```
OS10# show system

Node Id           : 1
MAC               : 00:0c:29:00:a5:d2
Number of MACs    : 256
Up Time           : 07:44:26

-- Unit 1 --
Status            : up
Down Reason       : unknown
System Location LED : off
Required Type     : S4048-ON
Current Type      : S4048-ON
Hardware Revision :
Software Version  : 10.4.9999EX
Physical Ports    : 32x40GbE

-- Power Supplies --
PSU-ID  Status   Type   AirFlow  Fan  Speed(rpm)  Status
-----
1       up       DC     REVERSE  1    7200        up
2       up       DC     REVERSE  1    7200        up

-- Fan Status --
FanTray  Status   AirFlow  Fan  Speed(rpm)  Status
-----
1       up       REVERSE  1    7000        up
                2    7000        up
2       up       REVERSE  1    7000        up
                2    7000        up
3       up       REVERSE  1    7000        up
                2    7000        up
```

Example (node-id)

```
OS10# show system node-id 1 fanout-configured

Interface          Breakout capable  Breakout state
-----
Eth 1/1/1          Yes               BREAKOUT_1x1
Eth 1/1/2          Yes               BREAKOUT_1x1
Eth 1/1/3          Yes               BREAKOUT_1x1
Eth 1/1/4          Yes               BREAKOUT_1x1
Eth 1/1/5          Yes               BREAKOUT_1x1
Eth 1/1/6          Yes               BREAKOUT_1x1
Eth 1/1/7          Yes               BREAKOUT_1x1
Eth 1/1/8          Yes               BREAKOUT_1x1
Eth 1/1/9          Yes               BREAKOUT_1x1
Eth 1/1/10         Yes               BREAKOUT_1x1
Eth 1/1/11         Yes               BREAKOUT_1x1
Eth 1/1/12         Yes               BREAKOUT_1x1
```

```

Eth 1/1/13      No      BREAKOUT_1x1
Eth 1/1/14      No      BREAKOUT_1x1
Eth 1/1/15      No      BREAKOUT_1x1
Eth 1/1/16      No      BREAKOUT_1x1
Eth 1/1/17      Yes     BREAKOUT_1x1
Eth 1/1/18      Yes     BREAKOUT_1x1
Eth 1/1/19      Yes     BREAKOUT_1x1
Eth 1/1/20      Yes     BREAKOUT_1x1
Eth 1/1/21      Yes     BREAKOUT_1x1
Eth 1/1/22      Yes     BREAKOUT_1x1
Eth 1/1/23      Yes     BREAKOUT_1x1
Eth 1/1/24      Yes     BREAKOUT_1x1
Eth 1/1/25      Yes     BREAKOUT_1x1
Eth 1/1/26      Yes     BREAKOUT_1x1
Eth 1/1/27      Yes     BREAKOUT_1x1
Eth 1/1/28      Yes     BREAKOUT_1x1
Eth 1/1/29      No      BREAKOUT_1x1
Eth 1/1/30      No      BREAKOUT_1x1
Eth 1/1/31      No      BREAKOUT_1x1
Eth 1/1/32      No      BREAKOUT_1x1

```

Example (brief)

```

OS10# show system brief

Node Id       : 1
MAC           : 34:17:18:19:20:21

-- Unit --
Unit  Status      ReqType    CurType    Version
-----
1     up           S4048     S4048     10.4.9999E(X)

-- Power Supplies --
PSU-ID  Status      Type      AirFlow    Fan  Speed(rpm)  Status
-----
1       fail
2       up        AC        REVERSE    1    14688       up

-- Fan Status --
FanTray  Status      AirFlow    Fan  Speed(rpm)  Status
-----
1        up        REVERSE    1    13063       up
                2    13020       up
2        up        REVERSE    1    12956       up
                2    12977       up
3        up        NORMAL     1    12956       up
                2    13063       up

```

Supported Releases 10.2.0E or later

traceroute

Displays the routes that packets take to travel to an IP address.

Syntax `traceroute [vrf {management | vrf-name}] host [-46dFITnreAUDV] [-f first_ttl] [-g gate,...] [-i device] [-m max_ttl] [-N squeries] [-p port] [-t tos] [-l flow_label] [-w waittime] [-q nqueries] [-s src_addr] [-z sendwait] [--fwmark=num] host [packetlen]`

Parameters

- `vrf management`— (Optional) Traces the route to an IP address in the management VRF instance.
- `vrf vrf-name`— (Optional) Traces the route to an IP address in the specified VRF instance.
- `host`— Enter the host to trace packets from.

- `-i interface` — (Optional) Enter the IP address of the interface through which traceroute sends packets. By default, the interface is selected according to the routing table.
- `-m max_ttl` — (Optional) Enter the maximum number of hops (maximum time-to-live value) that traceroute probes (default 30).
- `-p port` — (Optional) Enter a destination port:
 - For UDP tracing, enter the destination port base that traceroute uses (the destination port number is incremented by each probe).
 - For ICMP tracing, enter the initial ICMP sequence value (incremented by each probe).
 - For TCP tracing, enter the (constant) destination port to connect.
 - `-P protocol` — (Optional) Use a raw packet of the specified protocol for traceroute. Default protocol is 253 (RFC 3692).
 - `-s source_address` — (Optional) Enter an alternative source address of one of the interfaces. By default, the address of the outgoing interface is used.
 - `-q nqueries` — (Optional) Enter the number of probe packets per hop (default 3).
 - `-N squeries` — (Optional) Enter the number of probe packets that are sent out simultaneously to accelerate traceroute (default 16).
 - `-t tos` — (Optional) For IPv4, enter the Type of Service (TOS) and Precedence values to use. 16 sets a low delay; 8 sets a high throughput.
 - `-UL` — (Optional) Use UDPLITE for tracerouting (default port is 53).
 - `-w waittime` — (Optional) Enter the time (in seconds) to wait for a response to a probe (default 5 seconds).
 - `-z sendwait` — (Optional) Enter the minimal time interval to wait between probes (default 0). A value greater than 10 specifies a number in milliseconds, otherwise it specifies a number of seconds. This option is useful when routers rate-limit ICMP messages.
 - `--mtu` — (Optional) Discovers the MTU from the path being traced.
 - `--back` — (Optional) Prints the number of backward hops when it seems different with the forward direction.
 - `host` — (Required) Enter the name or IP address of the destination device.
 - `packet_len` — (Optional) Enter the total size of the probing packet (default 60 bytes for IPv4 and 80 for IPv6).

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# traceroute www.dell.com
traceroute to www.dell.com (23.73.112.54), 30 hops max, 60 byte packets
 1 10.11.97.254 (10.11.97.254) 4.298 ms 4.417 ms 4.398 ms
 2 10.11.3.254 (10.11.3.254) 2.121 ms 2.326 ms 2.550 ms
 3 10.11.27.254 (10.11.27.254) 2.233 ms 2.207 ms 2.391 ms
 4 Host65.hbms.com (63.80.56.65) 3.583 ms 3.776 ms 3.757 ms
 5 host33.30.198.65 (65.198.30.33) 3.758 ms 4.286 ms 4.221 ms
 6 3.GigabitEthernet3-3.GW3.SCL2.ALTER.NET (152.179.99.173) 4.428 ms
 2.593 ms 3.243 ms
 7 0.xe-7-0-1.XL3.SJC7.ALTER.NET (152.63.48.254) 3.915 ms 3.603 ms
 3.790 ms
 8 TenGigE0-4-0-5.GW6.SJC7.ALTER.NET (152.63.49.254) 11.781 ms 10.600
 ms 9.402 ms
 9 23.73.112.54 (23.73.112.54) 3.606 ms 3.542 ms 3.773 ms
```

Example (IPv6)

```
OS10# traceroute 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
```

Supported Releases 10.2.0E or later

Password recovery

You may need to recover a lost password.

1. Connect to the serial console port. The serial settings are 115200 baud, 8 data bits, and no parity.
2. Reboot or power up the system.
3. Press **ESC** at the Grub prompt to view the boot menu. The OS10-A partition is selected by default.

```
+-----+
|*OS10-A      |
| OS10-B      |
| ONIE        |
+-----+
```

4. Press **e** to open the OS10 GRUB editor.
5. Use the arrow keys to highlight the line that starts with `linux`. Add `init=/bin/bash` at the end of the line.

```
+-----+
|setparams 'OS10-
A'
|
|
| set
root='(hd0,gpt7)'
|
| echo 'Loading
OS10 ...'
| linux (hd0,gpt7)/boot/os10.linux console=ttyS0,115200 root=/dev/sda7 \rw
init=/bin/bash |
| initrd (hd0,gpt7)/boot/
os10.initrd
+-----+
```

6. Press **Ctrl + x** to reboot your system. If **Ctrl + x** does not cause the system to reboot, press **Alt + 0**. The system boots up to a root shell without a password.
7. Enter `linuxadmin` for the username at the system prompt.

```
root@OS10: /# linuxadmin
```

8. Enter your password at the system prompt, then enter the new password twice.

```
root@OS10: /# passwd linuxadmin
Enter new UNIX password: xxxxxxxxxxxx
Retype new UNIX password: xxxxxxxxxxxx
passwd: password updated successfully
```

9. Enter the `sync` command to save the new password.

```
root@OS10: /# sync
```

10. Reboot the system, then enter your new password.

```
root@OS10:~# reboot -f
Rebooting.
[ 3466.946967] reboot: Restarting system
```

```
BIOS Boot Selector for S5148F
Primary BIOS Version 3.36.0.1-2
```



```
SMF Version: MSS 1.2.2, FPGA 0.1
Last POR=0x11, Reset Cause=0x55
```

Restore factory defaults

Reboots the system to ONIE Rescue mode to restore the ONIE-enabled device to factory defaults.

 **CAUTION: Restoring factory defaults erases any installed operating system and requires a long time to erase storage.**

ONIE Rescue bypasses the installed operating system and boots the system into ONIE until you reboot the system. After ONIE Rescue completes, the system resets and boots to the ONIE console.

1. Use the up and down arrows to select the ONIE: Rescue, then press Enter. The highlight entry (*) runs automatically in the operating system.

```
+-----+
| *ONIE: Install OS |
| ONIE: Rescue     |
| ONIE: Uninstall OS |
| ONIE: Update ONIE |
| ONIE: Embed ONIE  |
| ONIE: Diag ONIE   |
+-----+
```

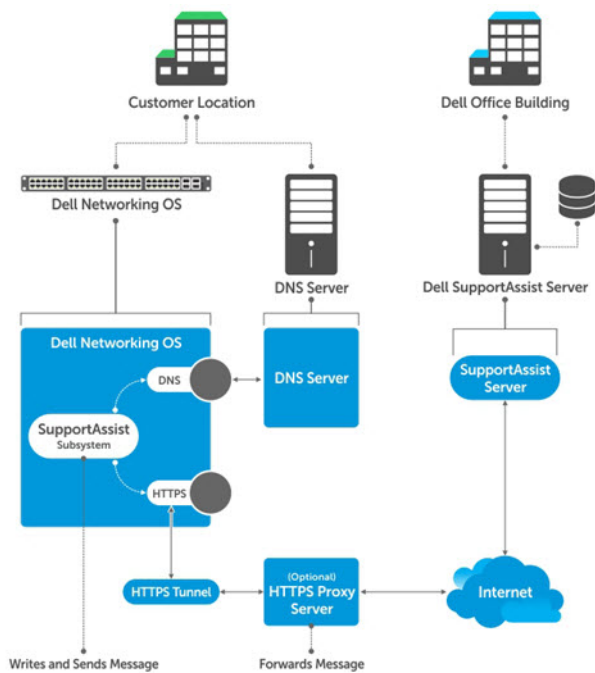
2. Press Enter again to enable the console.
3. Use the `onie-uninstall` command to return to the default ONIE settings.

```
ONIE:/ # onie-uninstall
Erasing unused NOR flash region Erasing 128 Kibyte @ 20000 - 100% complete. Erasing
internal mass storage device: /dev/mmcblk0 (7832MB) Percent complete: 100%
```

SupportAssist

By default, SupportAssist is enabled. SupportAssist sends troubleshooting data securely to Dell Technical Support. SupportAssist does not support automated email notification at the time of hardware fault alert, automatic case creation, automatic part dispatch, or reports.

To disable SupportAssist, use the `eula-consent support-assist reject` command.



Configure SupportAssist

SupportAssist is started by default. If you do not accept end user license agreement (EULA), SupportAssist is disabled.

1. Enter SupportAssist mode from CONFIGURATION mode.

```
support-assist
```

2. (Optional) Configure the SupportAssist server URL or IP address in SUPPORT-ASSIST mode.

```
server url server-url
```

3. (Optional) Configure the interface used to connect to the SupportAssist server in SUPPORT-ASSIST mode.

```
source-interface interface
```

4. (Optional) Configure the contact information for your company in SUPPORT-ASSIST mode.

```
contact-company name {company-name}
```

5. (Optional) Configure a proxy to reach the SupportAssist server in SUPPORT-ASSIST mode.

```
proxy-server ip {ipv4-address | ipv6-address} port port-number [username user-name  
password password]
```

6. Trigger an activity immediately or at a scheduled time in SUPPORT-ASSIST mode.

```
do support-assist activity full-transfer {start-now | schedule [hourly | daily |  
weekly | monthly | yearly]}
```

Configure SupportAssist

```
OS10(config)# support-assist
OS10(conf-support-assist)# contact-company name Eureka
OS10(conf-support-assist-Eureka)# exit
OS10(conf-support-assist)# server url http://eureka.com:701
OS10(conf-support-assist)# do support-assist-activity full-transfer start-now
```

Remove SupportAssist schedule

```
OS10# no support-assist activity full-transfer schedule
```

Show EULA license

```
OS10# show support-assist eula
I accept the terms of the license agreement. You can reject the license agreement by
configuring this command 'eula-consent support-assist reject.'
By installing SupportAssist, you allow Dell to save your contact information (e.g. name,
phone number and/or email address) which would be used to provide technical support
for your Dell products and services. Dell may use the information for providing
recommendations to improve your IT infrastructure.
Dell SupportAssist also collects and stores machine diagnostic information, which
may include but is not limited to configuration information, user supplied contact
information, names of data volumes, IP addresses, access control lists, diagnostics &
performance information, network configuration information, host/server configuration
& performance information and related data ("Collected Data") and transmits this
information to Dell. By downloading SupportAssist and agreeing to be bound by these
terms and the Dell end user license agreement, available at: www.dell.com/aeula, you
agree to allow Dell to provide remote monitoring services of your IT environment and
you give Dell the right to collect the Collected Data in accordance with Dell's Privacy
Policy, available at: www.dell.com/privacypolicycountryspecific, in order to enable the
performance of all of the various functions of SupportAssist during your entitlement to
receive related repair services from Dell. You further agree to allow Dell to transmit
and store the Collected Data from SupportAssist in accordance with these terms. You
agree that the provision of SupportAssist may involve international transfers of data
from you to Dell and/or to Dell's affiliates, subcontractors or business partners. When
making such transfers, Dell shall ensure appropriate protection is in plac/opt/dell/ose
to safeguard the Collected Data being transferred in connection with SupportAssist. If
you are downloading SupportAssist on behalf of a company or other legal entity, you are
further certifying to Dell that you have appropriate authority to provide this consent
on behalf of that entity. If you do not consent to the collection, transmission and/or
use of the Collected Data, you may not download, install or otherwise use SupportAssist.

(END)
```

Set company name

You can optionally configure name, address and territory information. Although this information is optional, it is used by Dell Technical Support to identify which company owns the device.

1. (Optional) Configure contact information in SUPPORT-ASSIST mode.

```
contact-company name name
```

2. (Optional) Configure address information in SUPPORT-ASSIST mode. Use the `no address` command to remove the configuration.

```
address city name state name country name zipcode number
```

3. (Optional) Configure street address information in SUPPORT-ASSIST mode. Use double quotes to add spaces within an address. Use the `no street-address` command to remove the configuration.

```
street-address {address-line-1} [{address-line-2} {address-line-3}]
```

4. (Optional) Configure the territory and set the coverage in SUPPORT-ASSIST mode. Use the `no territory` command to remove the configuration.

```
territory company-territory
```

Configure SupportAssist company

```
OS10(conf-support-assist)# contact-company name Eureka
OS10(conf-support-assist-Eureka)# address city San Jose state California Country America
zipcode 95123
OS10(conf-support-assist-Eureka)# street-address "123 Main Street" "Bldg 999"
OS10(conf-support-assist-Eureka)# territory sales
```

Set contact information

Configure contact details in SupportAssist Company mode. You can set the name, email addresses, phone, method, and time zone. SupportAssist `contact-person` configurations are optional for the SupportAssist service.

1. (Optional) Enter the contact name in SUPPORT-ASSIST mode.

```
contact-person first firstname last lastname
```

2. Enter the email addresses in SUPPORT-ASSIST mode.

```
email-address email-address
```

3. Enter the preferred contact method in SUPPORT-ASSIST mode.

```
preferred-method {email | phone | no-contact}
```

4. Enter a contact phone number in SUPPORT-ASSIST mode.

```
phone primary number [alternate number]
```

Configure contact details

```
OS10(config)# support-assist
OS10(conf-support-assist)# contact-company name Eureka
OS10(conf-support-assist-Eureka)# contact-person first John last Smith
OS10(conf-support-assist-Eureka)# email-address abc@dell.com
OS10(conf-support-assist-Eureka-JohnJamesSmith)# preferred-method email
OS10(conf-support-assist-Eureka)# phone primary 408-123-4567
```

Schedule activity

Configure the schedule for a full transfer of data. The default schedule is a full data transfer weekly — every Sunday at midnight (hour 0 minute 0).

- Configure full-transfer or log-transfer activities in EXEC mode.

```
support-assist-activity {full-transfer} schedule {hourly | daily | weekly | monthly |
yearly}
```

- `hourly min number` — Enter the time to schedule an hourly task (0 to 59).
- `daily hour number min number` — Enter the time to schedule a daily task (0 to 23 and 0 to 59).
- `weekly day-of-week number hour number min number` — Enter the time to schedule a weekly task (0 to 6, 0 to 23, and 0 to 59).
- `monthly day number hour number min number` — Enter the time to schedule a monthly task (1 to 31, 0 to 23, and 0 to 59).
- `yearly month number day number hour number min number` — Enter the time to schedule a yearly task (1 to 12, 1 to 31, 0 to 23, and 0 to 59).

Configure activity schedule for full transfer

```
OS10# support-assist-activity full-transfer schedule daily hour 22 min 50
OS10# support-assist-activity full-transfer schedule weekly day-of-week 6 hour 22 min 30
OS10# support-assist-activity full-transfer schedule monthly day 15 hour 12 min 30
OS10# support-assist-activity full-transfer schedule yearly month 6 day 12 hour 6 min 30
```

Set default activity schedule

```
OS10(conf-support-assist)# no support-assist-activity full-transfer schedule
```

View status

Display the SupportAssist configuration status, details, and EULA information using the `show` commands.

1. Display the SupportAssist activity in EXEC mode.

```
show support-assist status
```

2. Display the EULA license agreement in EXEC mode.

```
show support-assist eula
```

View SupportAssist status

```
OS10# show support-assist status
EULA          : Accepted
Service       : Enabled
Contact-Company : DellCMLCAEOS10
Street Address : 7625 Smetana Lane Dr
               Bldg 7615
               Cube F577
City          : Minneapolis
State         : Minnesota
Country       : USA
Zipcode       : 55418
Territory     : USA
Contact-person : Michael Dale
Email         : abc@dell.com
Primary phone  : 555-123-4567
Alternate phone :
Contact method : email
Server(configured) : https://web.dell.com
Proxy IP      :
Proxy Port    :
Proxy username :
Activity Enable State :
  Activity      State
-----
  coredump-transfer  enabled
  event-notification  enabled
  full-transfer       enabled

Scheduled Activity List :
Activity      Schedule                               Schedule created on
-----
full-transfer weekly: on sun at 00:00  Sep 12,2016 18:57:40

Activity Status :
Activity      Status      last start      last success
-----
coredump-transfer  success  Sep 12,2016 20:48:41  Sep 12,2016 20:48:42
event-notification  success  Sep 12,2016 20:51:51  Sep 12,2016 20:51:51
full-transfer       success  Sep 12,2016 20:30:28  Sep 12,2016 20:30:52
```

View EULA license

```
OS10# show support-assist eula
I accept the terms of the license agreement. You can reject the license agreement by
configuring this command 'eula-consent support-assist reject.'
By installing SupportAssist, you allow Dell to save your contact information (e.g. name,
phone number and/or email address) which would be used to provide technical support
for your Dell products and services. Dell may use the information for providing
recommendations to improve your IT infrastructure.
Dell SupportAssist also collects and stores machine diagnostic information, which
may include but is not limited to configuration information, user supplied contact
information, names of data volumes, IP addresses, access control lists, diagnostics &
performance information, network configuration information, host/server configuration
& performance information and related data ("Collected Data") and transmits this
information to Dell. By downloading SupportAssist and agreeing to be bound by these
terms and the Dell end user license agreement, available at: www.dell.com/aeula, you
agree to allow Dell to provide remote monitoring services of your IT environment and
you give Dell the right to collect the Collected Data in accordance with Dell's Privacy
Policy, available at: www.dell.com/privacypolicycountryspecific, in order to enable the
performance of all of the various functions of SupportAssist during your entitlement
to receive related repair services from Dell,. You further agree to allow Dell to
transmit and store the Collected Data from SupportAssist in accordance with these terms.
```

You agree that the provision of SupportAssist may involve international transfers of data from you to Dell and/or to Dell's affiliates, subcontractors or business partners. When making such transfers, Dell shall ensure appropriate protection is in place to safeguard the Collected Data being transferred in connection with SupportAssist. If you are downloading SupportAssist on behalf of a company or other legal entity, you are further certifying to Dell that you have appropriate authority to provide this consent on behalf of that entity. If you do not consent to the collection, transmission and/or use of the Collected Data, you may not download, install or otherwise use SupportAssist.

(END)

SupportAssist commands

activity

Enables SupportAssist activities to run on an associated trigger or schedule time.

Syntax `activity [coredump-transfer | event-notification | full-transfer} enable`

- Parameters**
- `coredump-transfer` — Enables transfer of core dump files.
 - `event-notification` — Enables transfer of event notification files.
 - `full-transfer` — Enables transfer of logs and technical support information.

Default Enabled

Command Mode SUPPORT-ASSIST

Usage Information Use the `no` version of this command to remove the configuration.

Example (Event)

```
OS10(conf-support-assist)# activity event-notification enable
```

Example (Full)

```
OS10(conf-support-assist)# activity full-transfer enable
```

Example (Turn Off)

```
OS10(conf-support-assist)# no activity coredump-transfer enable
```

Supported Releases 10.2.0E or later

contact-company

Configures the company contact information.

Syntax `contact-company name`

Parameters `name` — Enter the contact company name (up to 140 characters).

Default Not configured

Command Mode SUPPORT-ASSIST

Usage Information You can enter only one contact-company, and use double quotes to enclose additional contact information. The `no` version of this command removes the configuration.

Example

```
OS10(conf-support-assist)# contact-company name Eureka
OS10(conf-support-assist-Eureka)#
```

Supported Releases 10.2.0E or later

contact-person

Configures the contact name for an individual.

Syntax	<code>contact-person [first <i>firstname</i> last <i>lastname</i>]</code>
Parameters	<ul style="list-style-type: none">• <code>first <i>firstname</i></code> — Enter the keyword and the first name for the contact person. Use double quotes for more than one first name.• <code>last <i>lastname</i></code> — Enter the keyword and the last name for the contact person.
Default	Not configured
Command Mode	SUPPORT-ASSIST
Usage Information	The <code>no</code> version of this command removes the configuration.
Example	<pre>OS10(conf-support-assist-Eureka)# contact-person first "John James" last Smith</pre>
Supported Releases	10.2.0E or later

email-address

Configures the email address for the contact name.

Syntax	<code>email-address <i>address</i></code>
Parameters	<code><i>address</i></code> — Enter the email address for the contact name.
Default	Not configured
Command Mode	SUPPORT-ASSIST
Usage Information	The <code>no</code> version of this command removes the configuration.
Example	<pre>OS10(conf-support-assist-Eureka-JohnJamesSmith)# email-address jjsmith@eureka.com</pre>
Supported Releases	10.2.0E or later

eula-consent

Accepts or rejects the SupportAssist end-user license agreement (EULA).

Syntax	<code>eula-consent {support-assist} {accept reject}</code>
Parameters	<ul style="list-style-type: none">• <code>support-assist</code> — Enter to accept or reject the EULA for the service.• <code>accept</code> — Enter to accept the EULA-consent.• <code>reject</code> — Enter to reject EULA-consent.
Default	Not configured
Command Mode	CONFIGURATION
Usage Information	If you reject the end-user license agreement, you cannot access Configuration mode. If there is an existing SupportAssist configuration, the configuration is not removed and the feature is disabled.
Example (Accept)	<pre>OS10(config)# eula-consent support-assist accept</pre>

Example (Reject)

```
OS10(config)# eula-consent support-assist reject

This action will disable Support Assist and erase all configured data.Do
you want to proceed ? [Y/N]:Y
```

Supported Releases 10.2.0E or later

preferred-method

Configures a preferred method to contact an individual.

Syntax `preferred-method {email | phone | no-contact}`

Parameters

- `email` — Enter to select email as the preferred contact method.
- `phone` — Enter to select phone as the preferred contact method.
- `no-contact` — Enter to select no-contact as the preferred contact method.

Default No-contact

Command Mode SUPPORT-ASSIST

Usage Information The no version of this command removes the configuration.

Example

```
OS10(conf-support-assist-Eureka-JohnJamesSmith)# preferred-method email
```

Supported Releases 10.2.0E or later

proxy-server

Configures a proxy IP address for reaching the SupportAssist server.

Syntax `proxy-server ip ipv4-address port number`

Parameters

- `ipv4-address` — Enter the IPv4 address of the proxy server in a dotted decimal format (A.B.C.D).
- `number` — Enter the port number (0 to 65535).

Default Not configured

Command Mode SUPPORT-ASSIST

Usage Information You cannot use an IPv6 address with this command.

Example

```
OS10(conf-support-assist)# proxy-server ip 10.1.1.5 port 701
```

Supported Releases 10.2.0E or later

server url

Configures the domain or IP address of the remote SupportAssist server.

Syntax `server url server-url-string`

Parameters `server-url-string` — Enter the domain or IP address of the remote SupportAssist server. To include a space, enter a space within double quotes.

Default `https://stor.g3.ph.dell.com`

Command Mode SUPPORT-ASSIST

Usage Information Only configure one SupportAssist server. If you do not configure the SupportAssist server, the system uses the non-configurable default server. Use the `show support-assist status` command to view the server configuration. The `no` version of this command removes the remote server.

Example

```
OS10(conf-support-assist)# server url https://eureka.com:444
```

Supported Releases 10.2.0E or later

show support-assist eula

Displays the EULA for SupportAssist.

Syntax `show support-assist eula`

Parameters None

Default None

Command Mode EXEC

Usage Information Use the `eula-consent support-assist accept` command to accept the license agreement.

Example

```
OS10# show support-assist eula
I accept the terms of the license agreement. You can reject the
license agreement by configuring this command 'eula-consent support-
assist reject.'
By installing SupportAssist, you allow Dell, Inc. to save your contact
information (e.g. name, phone number and/or email address) which would
be used to provide technical support for your Dell, Inc. products
and services. Dell, Inc. may use the information for providing
recommendations to improve your IT infrastructure.
SupportAssist also collects and stores machine diagnostic information,
which may include but is not limited to configuration information,
user supplied contact information, names of data volumes, IP addresses,
access control lists, diagnostics & performance information, network
configuration information, host/server configuration & performance
information and related data ("Collected Data") and transmits this
information to Dell, Inc. By downloading SupportAssist and agreeing
to be bound by these terms and the Dell, Inc. end user license
agreement, available at: www.dell.com/aeula, you agree to allow Dell,
Inc. to provide remote monitoring services of your IT environment
and you give Dell, Inc. the right to collect the Collected Data in
accordance with Dell, Inc.'s Privacy Policy, available at: www.dell.com/
privacypolicycountryspecific, in order to enable the performance of all
of the various functions of SupportAssist during your entitlement to
receive related repair services from Dell, Inc. You further agree
to allow Dell, Inc. to transmit and store the Collected Data from
SupportAssist in accordance with these terms. You agree that the
provision of SupportAssist may involve international transfers of data
from you to Dell, Inc. and/or to Dell, Inc.'s affiliates, subcontractors
or business partners. When making such transfers, Dell, Inc. shall
ensure appropriate protection is in place to safeguard the Collected
Data being transferred in connection with SupportAssist. If you are
downloading SupportAssist on behalf of a company or other legal entity,
you are further certifying to Dell, Inc. that you have appropriate
authority to provide this consent on behalf of that entity. If you do
not consent to the collection, transmission and/or use of the Collected
Data, you may not download, install or otherwise use SupportAssist.

(END)
```

Supported Releases 10.2.0E or later

show support-assist status

Displays SupportAssist status information including activities and events.

Syntax `show support-assist status`

Parameters None

Default Not configured

Command Mode EXEC

Example

```
OS10# show support-assist status
EULA           : Accepted
Service        : Enabled
Contact-Company : DellCMLCAEOS10
Street Address : 7625 Smetana Lane Dr
                Bldg 7615
                Cube F577
City           : Minneapolis
State          : Minnesota
Country        : USA
Zipcode        : 55418
Territory      : USA
Contact-person : Michael Dale
Email          : abc@dell.com
Primary phone  : 555-123-4567
Alternate phone :
Contact method : email
Server(configured) : https://web.dell.com
Proxy IP       :
Proxy Port     :
Proxy username :
Activity Enable State :
    Activity          State
-----
    coredump-transfer enabled
    event-notification enabled
    full-transfer      enabled

Scheduled Activity List :
    Activity          Schedule          Schedule created on
-----
    full-transfer    weekly: on sun at 00:00    Sep 12,2016 18:57:40

Activity Status :
    Activity          Status    last start          last success
-----
    coredump-transfer success    Sep 12,2016 20:48:41    Sep 12,2016
    20:48:42
    event-notification success    Sep 12,2016 20:51:51    Sep 12,2016
    20:51:51
    full-transfer      success    Sep 12,2016 20:30:28    Sep 12,2016
    20:30:52
```

Supported Releases 10.2.0E or later

source-interface

Configures the interface used to connect to the SupportAssist server.

Syntax `source-interface interface`

Parameters `interface:`

- `ethernet node/slot/port[:subport]` — Enter a physical Ethernet interface.
- `loopback number` — Enter a loopback interface (0 to 16383).

- `management 1/1/1` — Enter the management interface.
- `port-channel channel-id` — Enter a port-channel ID (1 to 28).
- `vlan vlan-id` — Enter a VLAN ID (1 to 4093).

Default A source interface is not configured.

Command Mode SUPPORT-ASSIST

Usage Information The `no` version of this command removes the configured source interface.

Example

```
OS10(conf-support-assist)# source-interface ethernet 1/1/4
```

Supported Releases 10.4.0E(R1) or later

street-address

Configures the street address information for the company.

Syntax `street-address {address}`

Parameters `address` — Enter one or more addresses in double quotes (up to 140 characters).

Default Not configured

Command Mode SUPPORT-ASSIST

Usage Information Add spaces to the company street address by enclosing the address in quotes. Separate each address with a space to place on a new line. The `no` version of this command removes the company address configuration.

Example

```
OS10(conf-support-assist-Eureka)# street-address "One Dell Way" "Suite 100"
```

Supported Releases 10.2.0E or later

support-assist-activity

Schedules a time to transfer the activity log.

Syntax `support-assist-activity full-transfer [start-now] [schedule {hourly minute | daily hour number min number | weekly day-of-week number hour number | monthly day number hour number min number | yearly month number day number}]`

- Parameters**
- `start-now` — Schedules the transfer to start immediately.
 - `hourly minute` — Schedule an hourly task (0 to 59).
 - `daily` — Schedule a daily task:
 - `hour number` — Enter the keyword and number of hours to schedule the daily task (0 to 23).
 - `min number` — Enter the keyword and number of minutes to schedule the daily task (0 to 59).
 - `weekly` — Schedule a weekly task:
 - `day-of-week number` — Enter the keyword and number for the day of the week to schedule the task (0 to 6).
 - `hour number` — Enter the keyword and number of the hour to schedule the weekly task (0 to 23).
 - `monthly` — Schedule a monthly task:
 - `day number` — Enter the number for the day of the month to schedule the task (1 to 31).
 - `hour number` — Enter the number for the hour of the day to schedule the task (0 to 23).
 - `min number` — Enter the number for the minute of the hour to schedule the task (0 to 59).

- `yearly` — Schedule the yearly task:
 - `month number` — Enter the keyword and number of the month to schedule the yearly task (1 to 12).
 - `day number` — Enter the keyword and the number of the day to schedule the monthly task (1 to 31).

Default Weekly on Sunday at midnight (hour 0 minute 0)

Command Mode EXEC

Usage Information The `no` version of this command removes the schedule activity.

Example

```
OS10# support-assist-activity full-transfer schedule daily hour 22 min 50
```

Supported Releases 10.2.0E or later

territory

Configures the territory for the company.

Syntax `territory territory`

Parameters `territory` — Enter the territory for the company.

Default Not configured

Command Mode CONFIG-SUPPORT-ASSIST

Usage Information The `no` version of this command removes the company territory configuration.

Example

```
OS10(conf-support-assist)# contact-company name Eureka
OS10(conf-support-assist-Eureka)# territory west
```

Supported Releases 10.2.0E or later

Support bundle

The Support Bundle is based on the `sosreport` tool. Use the Support Bundle to generate an `sosreport` tar file that collects Linux system configuration and diagnostics information, as well as `show` command output to send to Dell Technical Support.

To send Dell Technical Support troubleshooting details about the Linux system configuration and OS10 diagnostics, generate an `sosreport` tar file.

1. Generate the tar file in EXEC mode.

```
generate support-bundle
```

2. Verify the generated file in EXEC mode.

```
dir supportbundle
```

3. Send the support bundle using FTP/SFTP/SCP/TFTP in EXEC mode.

```
copy supportbundle://sosreport-filename.tar.gz tftp://server-address/path
```

Use the `delete supportbundle://sosreport-filename.tar.gz` command to delete a generated support bundle.

Event notifications

Event notifications for the `generate support-bundle` command are processed at the start and end of the bundle they support, and reports either success or failure.

Support bundle generation start event

```
Apr 19 16:57:55: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_STARTED: generate support-bundle execution has started successfully:All Plugin options disabled
Apr 19 16:57:55: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_STARTED: generate support-bundle execution has started successfully:All Plugin options enabled
```

sosreport generation start event

```
May 11 22:9:43: %Node.1-Unit.1:PRI:OS10 %log-notice:SOSREPORT_GEN_STARTED: CLI output collection task completed; sosreport execution task started:All Plugin options disabled
May 11 22:9:43: %Node.1-Unit.1:PRI:OS10 %log-notice:SOSREPORT_GEN_STARTED: CLI output collection task completed; sosreport execution task started:All Plugin options enabled
```

Support bundle generation successful event

```
Apr 19 17:0:9: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_COMPLETED: generate support-bundle execution has completed successfully:All Plugin options disabled
Apr 19 17:0:9: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_COMPLETED: generate support-bundle execution has completed successfully:All Plugin options enabled
```

Support bundle generation failure

```
Apr 19 17:0:14: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_FAILURE: Failure in generate support-bundle execution:All Plugin options disabled
Apr 19 17:0:14: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_FAILURE: Failure in generate support-bundle execution:All Plugin options enabled
```

generate support-bundle

Generates an `sosreport` tar file that collects configuration and diagnostic information on Linux systems.

Syntax	<code>generate support-bundle [enable-all-plugin-options]</code>
Parameters	<code>enable-all-plugin-options</code> — (Optional) Generate a full support bundle with all plugin options enabled.
Defaults	None
Command Mode	EXEC
Usage Information	To send the tar file to Dell Technical Support, use the <code>dir supportbundle</code> and <code>copy supportbundle://sosreport-OS10-file-number.tar.gz tftp://server-address/path</code> commands.
Example	<pre>OS10# generate support-bundle</pre>
Example (Enable Options)	<pre>OS10# generate support-bundle enable-all-plugin-options</pre>
Supported Releases	10.2.0E or later

System monitoring

Monitor OS10 using system alarm and log information.

System alarms

Alarms alert you to conditions that might prevent normal device operation:

- **Critical** — A critical condition exists and requires immediate action. A critical alarm may trigger if one or more hardware components have failed, or one or more hardware components exceeds temperature thresholds.
- **Major** — A major error occurred and requires escalation or notification. For example, a major alarm may trigger if an interface failure occurs, such as a port-channel being down.
- **Minor** — A minor error or non-critical condition occurred that, if left unchecked, might cause system service interruption or performance degradation. A minor alarm requires monitoring or maintenance.
- **Informational** — An informational error occurred but does not impact performance. Monitor an informational alarm until the condition changes.

Triggered alarms are in one of these states:

- **Active** — Alarms that are current and not cleared.
- **Cleared** — Alarms that are resolved and the device has returned to normal operation.

System logging

You can change system logging default settings using the severity level to control the type of system messages that are logged. Range of logging severities:

- `log-emerg` — System is unstable.
- `log-alert` — Immediate action needed.
- `log-crit` — Critical conditions.
- `log-err` — Error conditions.
- `log-warning` — Warning conditions.
- `log-notice` — Normal but significant conditions (default).
- `log-info` — Informational messages.
- `log-debug` — Debug messages.
- Enter the minimum severity level for logging to the console in CONFIGURATION mode.

```
logging console severity
```

- Enter the minimum severity level for logging to the system log file in CONFIGURATION mode.

```
logging log-file severity
```

- Enter the minimum severity level for logging to terminal lines in CONFIGURATION mode.

```
logging monitor severity
```

- Enter which server to use for syslog messages with the hostname or IP address in CONFIGURATION mode.

```
logging server {hostname/ip-address severity}
```

Disable system logging

You can use the `no` version of any logging command to disable system logging.

- Disable console logging and reset the minimum logging severity to the default in CONFIGURATION mode.

```
no logging console severity
```

- Disable log-file logging and reset the minimum logging severity to the default in CONFIGURATION mode.

```
no logging log-file severity
```

- Disable monitor logging and reset the minimum logging severity to the default in CONFIGURATION mode.

```
no logging monitor severity
```

- Disable server logging and reset the minimum logging severity to the default in CONFIGURATION mode.

```
no logging server severity
```

- Re-enable any logging command in CONFIGURATION mode.

```
no logging enable
```

Enable server logging for log notice

```
OS10(config)# logging server dell.com severity log-notice
```

View system logs

The system log-file contains system event and alarm logs.

Use the `show trace` command to view the current syslog file. All event and alarm information is sent to the syslog server, if one is configured.

The `show logging` command accepts the following parameters:

- `log-file` — Provides a detailed log including both software and hardware saved to a file.
- `process-names` — Provides a list of all processes currently running which can be filtered based on the process-name.

View logging log-file

```
OS10# show logging log-file
Jun  1 05:01:46 %Node.1-Unit.1:PRI:OS10 %log-notice:ETL_SERVICE_UP: ETL service
is up
Jun  1 05:02:06 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_UNIT_DETECTED: Unit pres
ent:Unit 1#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_PSU_DETECTED: Power Supp
ly Unit present:PSU 1#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_PSU_DETECTED: Power Supp
ly Unit present:PSU 2#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 1#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 2#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 3#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-crit:EQM_FAN_AIRFLOW_MISMATCH: MAJO
R ALARM: FAN AIRFLOW MISMATCH: SET: One or more fans have mismatching or unknown
airflow directions#003
Jun  1 05:02:10 %Node.1-Unit.1:PRI:OS10 %log-notice:NDM_SERVICE_UP: NDM Service
Ready!
Jun  1 05:02:10 %Node.1-Unit.1:PRI:OS10 %log-notice:SU_SERVICE_UP: Software upgr
ade service is up:software upgrade service up
--More--
```

View logging process names

```
OS10# show logging process-names
dn_alm
dn_app_vlt
dn_app_vrrp
dn_bgp
dn_dot1x
dn_eqa
dn_eqm
dn_eth_drv
dn_etl
dn_i3
dn_ifm
dn_infra_afs
dn_issu
dn_l2_services
dn_l2_services_
dn_l2_services_
```

```
dn_l2_services_
dn_l2_services_
dn_l3_core_serv
dn_l3_service
dn_lacp
dn_lldp
dn_mgmt_entity_
--More--
```

Environmental monitoring

Monitors the hardware environment to detect temperature, CPU, and memory utilization.

View environment

```
OS10# show environment

Unit      State          Temperature Voltage
-----
1         up             42
-----

Thermal sensors
Unit  Sensor-Id      Sensor-name          Temperature
-----
1     1              T2 temp sensor      28
1     2              system-NIC temp sensor 25
1     3              Ambient temp sensor  24
1     4              NPU temp sensor     40
-----
```

Link-bundle monitoring

Monitoring link aggregation group (LAG) bundles allows the traffic distribution amounts in a link to look for unfair distribution at any given time. A threshold of 60% is an acceptable amount of traffic on a member link.

Links are monitored in 15-second intervals for three consecutive instances. Any deviation within that time sends syslog and an alarm event generates. When the deviation clears, another syslog sends and a clear alarm event generates.

Link-bundle utilization is calculated as the total bandwidth of all links divided by the total bytes-per-second of all links. If you enable monitoring, the utilization calculation performs when the utilization of the link-bundle (not a link within a bundle) exceeds 60%.

Configure Threshold level for link-bundle monitoring

```
OS10(config)# link-bundle-trigger-threshold 10
```

View link-bundle monitoring threshold configuration

```
OS10(config)# do show running-configuration
link-bundle-trigger-threshold 10
!
...
```

Show link-bundle utilization

```
OS10(config)# do show link-bundle-utilization

Link-bundle trigger threshold - 10
```


Alarm commands

alarm clear

Clears the alarm based on the alarm index for a user-clearable alarm (a transient alarm).

- Syntax** `alarm clear alarm-index`
- Parameters** `clear alarm-index` — Enter the alarm ID to clear the alarm.
- Default** Not configured
- Command Mode** EXEC
- Usage Information** Use the `show alarm index` command to view a list of alarm IDs.

Example

```
OS10# alarm clear 200
```

- Supported Releases** 10.2.0E or later

show alarms

Displays all current active system alarms.

- Syntax** `show alarms`
- Parameters** None
- Default** Not configured
- Command Mode** EXEC
- Usage Information** None

Example

```
OS10# show alarms

Index  Severity  Name                                     Raise-time  Source
-----  -
0      major    EQM_MORE_PSU_FAULT                     Sep 7 18:36:11 Node.1-Unit.1
1      major    EQM_FAN_AIRFLOW_MISMATCH               Sep 7 18:36:11 Node.1-Unit.1
```

- Supported Releases** 10.2.0E or later

show alarms details

Displays details about active alarms.

- Syntax** `show alarms details`
- Parameters** None
- Default** Not configured
- Command Mode** EXEC
- Usage Information** None

Example

```
OS10# show alarms details
```

```

Active-alarm details - 0
-----
Index:          0
Sequence Number: 1
Severity:       critical
Type:          1081367
Source:        Node.1-Unit.1
Name:          EQM_THERMAL_CRIT_CROSSED
Description:
Raise-time:    Sep 20 0:1:5
Clear-time:
New:           true
State:         raised
-----
Active-alarm details - 1
-----
Index:          1
Sequence Number: 5
Severity:       warning
Type:          1081364
Source:        Node.1-Unit.1
Name:          EQM_THERMAL_WARN_CROSSED
Description:
Raise-time:    Sep 20 0:16:52
Clear-time:
New:           true
State:         raised

```

Supported Releases 10.2.0E or later

show alarms history

Displays the history of cleared alarms.

Syntax `show alarms history [summary]`

Parameters `summary` — Enter to view a summary of the alarm history.

Default Not configured

Command Mode EXEC

Usage Information None

Example

```

OS10# show alarms history

Index  Severity  Name                                     Raise-time  Source
-----  -
0      minor    EQM_THERMAL_MINOR_CROSSE              Sep 20 0:8:24  Node.1-Unit.1
1      major    EQM_THERMAL_MAJOR_CROSSE             Sep 20 0:16:28  Node.1-Unit.1
2      minor    EQM_THERMAL_MINOR_CROSSE              Sep 20 0:15:39  Node.1-Unit.1

```

Example (Summary)

```

OS10# show alarms history summary

Alarm History Summary
-----
Total-count:      0
Critical-count:   0
Major-count:      0
Minor-count:      0
Warning-count:    0
-----

```

Supported Releases 10.2.0E or later

show alarms index

Displays information about a specific alarm using the alarm ID.

Syntax	<code>show alarms index <i>alarm-id</i></code>
Parameters	<code>index <i>alarm-id</i></code> — Enter the keyword and the alarm ID to view specific information.
Default	Not configured
Command Mode	EXEC
Usage Information	Use the <code>alarm-id</code> to clear and view alarm details.

Example

```
OS10# show alarms index 1

Active-alarm details - 1
-----
Index:                1
Sequence Number:     5
Severity:             warning
Type:                 1081364
Source:               Node.1-Unit.1
Name:                 EQM_THERMAL_WARN_CROSSED
Description:
Raise-time:           Sep 20 0:16:52
Clear-time:
New:                  true
State:                raised
```

Supported Releases	10.2.0E or later
---------------------------	------------------

show alarms severity

Displays all active alarms using the severity level.

Syntax	<code>show alarms severity <i>severity</i></code>
Parameters	<code>severity</code> — Set the alarm severity: <ul style="list-style-type: none">• <code>critical</code> — Critical alarm severity.• <code>major</code> — Major alarm severity.• <code>minor</code> — Minor alarm severity.• <code>warning</code> — Warning alarm severity.
Default	Not configured
Command Mode	EXEC
Usage Information	None

Example (Warning)

```
OS10# show alarms severity warning

Active-alarm details - 1
-----
Index:                1
Sequence Number:     5
Severity:             warning
Type:                 1081364
Source:               Node.1-Unit.1
Name:                 EQM_THERMAL_WARN_CROSSED
Description:
Raise-time:           Sep 20 0:16:52
Clear-time:
```

```
New: true
State: raised
```

Example (Critical)

```
OS10# show alarms severity critical

Active-alarm details - 0
-----
Index: 0
Sequence Number: 1
Severity: critical
Type: 1081367
Source: Node.1-Unit.1
Name: EQM_THERMAL_CRIT_CROSSED
Description:
Raise-time: Sep 20 0:1:5
Clear-time:
New: true
State: raised
```

Supported Releases 10.2.0E or later

show alarms summary

Displays the summary of alarm information.

Syntax show alarms summary

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# show alarms summary

Active-alarm Summary
-----
Total-count: 6
Critical-count: 0
Major-count: 2
Minor-count: 2
Warning-count: 2
-----
```

Supported Releases 10.2.0E or later

Logging commands

clear logging

Clears messages in the logging buffer.

Syntax clear logging log-file

Parameters None

Default Not configured

Command Mode EXEC

Usage Information None

Example

```
OS10# clear logging log-file
Proceed to clear the log file [confirm yes/no(default)]:
```

Supported Releases 10.2.0E or later

logging console

Disables, enables, or configures the minimum severity level for logging to the console.

Syntax

```
logging console {disable | enable | severity}
```

To set the severity to the default level, use the `no logging console severity` command. The default severity level is `log-notice`.

Parameters

severity — Set the minimum logging severity level:

- `log-emerg` — Set to unusable.
- `log-alert` — Set to immediate action is needed.
- `log-crit` — Set to critical conditions.
- `log-err` — Set to error conditions.
- `log-warning` — Set to warning conditions.
- `log-notice` — Set to normal but significant conditions (default).
- `log-info` — Set to informational messages.
- `log-debug` — Set to debug messages.

Default Log-notice

Command Mode CONFIGURATION

Usage Information None

Example

```
OS10(config)# logging console disable
```

Example (Enable)

```
OS10(config)# logging console enable
```

Example (Severity)

```
OS10(config)# logging console severity log-warning
```

Supported Releases 10.2.0E or later

logging enable

Enables system logging.

Syntax

```
logging enable
```

To disable the logging capability, use the `no logging enable` command.

Parameters None

Default Enabled

Command Mode CONFIGURATION

Usage Information The `no` version of this command disables all logging.

Example

```
OS10(config)# logging enable
```

Supported Releases

10.2.0E or later

logging log-file

Disables, enables, or sets the minimum severity level for logging to the logfile.

Syntax

```
logging log-file {disable | enable | severity}
```

To reset the log-file severity to the default level, use the `no logging log-file severity` command. The default severity level is log-notice.

Parameters

severity — Set the minimum logging severity level:

- log-emerg — Set the system as unusable.
- log-alert — Set to immediate action is needed.
- log-crit — Set to critical conditions.
- log-err — Set to error conditions.
- log-warning — Set to warning conditions.
- log-notice — Set to normal but significant conditions (default).
- log-info — Set to informational messages.
- log-debug — Set to debug messages.

Default

Log-notice

Command Mode

CONFIGURATION

Usage

None

Information**Example**

```
OS10(config)# logging log-file disable
```

Example (Enable)

```
OS10(config)# logging log-file enable
```

Example (Severity)

```
OS10(config)# logging log-file severity log-notice
```

Supported Releases

10.2.0E or later

logging monitor

Set the minimum severity level for logging to the terminal lines.

Syntax

```
logging monitor severity severity-level
```

To reset the monitor severity to the default level, use the `no logging monitor severity` command. The default severity level is log-notice.

Parameters

severity-level — Set the minimum logging severity level:

- log-emerg — Set the system as unusable.
- log-alert — Set to immediate action is needed.
- log-crit — Set to critical conditions.
- log-err — Set to error conditions.
- log-warning — Set to warning conditions.
- log-notice — Set to normal but significant conditions (default).
- log-info — Set to informational messages.

- `log-debug` — Set to debug messages.

Default Log-notice

Command Mode CONFIGURATION

Usage Information None

Example

```
OS10(config)# logging monitor severity log-info
```

Supported Releases 10.2.0E or later

logging server

Configures the remote syslog server.

Syntax `logging server {hostname | ipv4-address | ipv6-address} [severity severity-level | vrf management [severity severity-level] [tcp port-number | udp port-number]`

- Parameters**
- `hostname | ipv4-address | ipv6-address` — (Optional) Enter either the hostname or IPv4/IPv6 address of the logging server.
 - `vrf management` — (Optional) Configure the logging server for the management VRF instance.
 - `severity-level` — (Optional) Set the logging threshold severity:
 - `log-emerg` — System as unusable.
 - `log-alert` — Immediate action is needed.
 - `log-crit` — Critical conditions.
 - `log-err` — Error conditions.
 - `log-warning` — Warning conditions.
 - `log-notice` — Normal but significant conditions (default).
 - `log-info` — Informational messages.
 - `log-debug` — Debug messages.
 - `tcp port-number` — (Optional) Send syslog messages over TCP to a specified port on a remote logging server (1-65535).
 - `udp port-number` — (Optional) Send syslog messages over UDP to a specified port on a remote logging server (1-65535; default 514).

Defaults System messages of the `log-notice` security level and lower are generated. Syslog messages are sent over UDP to port 514 on a remote logging server.

Command Mode CONFIGURATION

Usage Information Starting from 10.3.0E or later, this command supports IPv6 addresses. The previous versions support only IPv4 addresses. The `no` version of this command deletes the syslog server.

Example

```
OS10(config)# logging server dell.com severity log-info
```

```
OS10(config)# logging server fda8:6c3:ce53:a890::2 tcp 1468
```

```
OS10(config)# logging server dell.com vrf management severity log-debug
```

Supported Releases 10.2.0E or later

show logging

Displays system logging messages by log-file, process-names, or summary.

Syntax	<code>show logging {log-file [process-name line-numbers] process-names}</code>
Parameters	<ul style="list-style-type: none">• <i>process-name</i> — (Optional) Enter the process-name to use as a filter in syslog messages.• <i>line-numbers</i> — (Optional) Enter the number of lines to include in the logging messages (1 to 65535).
Default	None
Command Mode	EXEC
Usage Information	The output from this command is the <code>/var/log/eventlog</code> file.

Example (Log-File)

```
OS10# show logging log-file process-name dn_qos
```

Example (Process-Names)

```
OS10# show logging process-names
dn_pas_svc
dn_system_mgmt_
dn_env_tmptctl_
dn_pm
dn_eth_drv
dn_etl
dn_eqa
dn_alm
dn_eqm
dn_issu
dn_swupgrade
dn_ifm
dn_ppm
dn_l2_services
dn_dot1x
dn_l3_core_serv
dn_policy
dn_qos
dn_switch_res_m
dn_ospfv3
dn_lacp
dn_i3
dn_supportassis
--More--
```

Supported Releases 10.2.0E or later

show trace

Displays trace messages.

Syntax	<code>show trace [number-lines]</code>
Parameters	<i>number-lines</i> — (Optional) Enter the number of lines to include in log messages (1 to 65535).
Default	Enabled
Command Mode	EXEC
Usage Information	The output from this command is the <code>/var/log/syslog</code> file.

Example

```
OS10# show trace
May 23 17:10:03 OS10 base_nas: [NETLINK:NH-
EVENT]:ds api_linux_neigh.c:nl_to_nei
gh_info:109, Operation:Add-NH family:IPv4(2) flags:0x0 state:Failed(32)
```



```

if-idx:4
May 23 17:10:03 OS10 base_nas: [NETLINK:NH-
EVENT]:ds_api_linux_neigh.c:nl_to_nei
gh_info:120, NextHop IP:192.168.10.1
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359304)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Hash value - 20 can't be
converted
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359305)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359311)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Hash value - 20 can't be
converted
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359312)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59344)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59345)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59346)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59319)
May 23 17:10:08 OS10 base_nas: [NETLINK:NH-
EVENT]:ds_api_linux_neigh.c:nl_to_nei
--More--

```

Supported Releases 10.2.0E or later

Log into OS10 device

Linux shell access is available for troubleshooting and diagnostic purposes only. Use `linuxadmin` for both the default user name and password. For security reasons, you must change the default `linuxadmin` password during the first login from the Linux shell. The system saves the new password for future logins.

CAUTION: Changing the system state from the Linux shell can result in undesired and unpredictable system behavior. Only use Linux shell commands to display system state and variables, or as instructed by Dell Support.

```

OS10 login: linuxadmin
Password: linuxadmin >> only for first-time login
You are required to change your password immediately (root enforced)
Changing password for linuxadmin.
(current) UNIX password: linuxadmin
Enter new UNIX password: enter a new password
Retype new UNIX password: re-enter the new password
Linux OS10 3.16.7-ckt20 #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2017-05-01) x86_64

```

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in `/usr/share/doc/*/copyright`.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

```

-----*
-*          Dell EMC Network Operating System (OS10)          *-
-*                                                                 *-

```

```
-* Copyright (c) 1999-2017 by Dell Inc. All Rights Reserved. *-
-*
-*****-*****-*****-*****-*****-*****-*****-*****-*****-*****-
```

This product is protected by U.S. and international copyright and intellectual property laws. Dell EMC and the Dell EMC logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

linuxadmin@OS10:~\$

To log in to OS10 and access the command-line interface, enter `su - admin` at the Linux shell prompt, then `admin` as the password.

```
linuxadmin@OS10:~$ su - admin
Password: admin
OS10#
```

Frequently asked questions

This section contains answers to frequently asked questions for ONIE-enabled devices.

- [Installation](#) contains information about how to enter ONIE: Install mode after a reboot, find information about your specific switch, how to log into the OS10 shell, and so on.
- [Hardware](#) contains information about how to view default console settings, how to view hardware alarms and events, how to view LED status, and so on.
- [Configuration](#) contains information about how to enter CONFIGURATION mode, how to modify the candidate configuration, and so on.
- [Security](#) contains information about how to add users, troubleshoot RADIUS, how to view current DHCP information, and so on.
- [Layer 2](#) contains information about how to configure routing information including 802.1X, LACP, LLDP, MAC, and so on.
- [Layer 3](#) contains information about how to troubleshoot BCP, ECMP, OSPF, and so on.
- [System management](#) contains information about how to view current interface configuration information, how to view a list of all system devices, how to view the software version, and so on.
- [Quality of service](#) contains information about quality of service including classification and marking, congestion management, policing and shaping, and so on.
- [Monitoring](#) contains information about how to view alarms, events, logs, and so on.

Installation

How do I configure a default management route?

Although the default management route was configured during installation, you can use the `route add default gw` command from the Linux shell to configure the default management IP address for routing. SupportAssist requires the default management route is configured to work properly, as well as DNS configured and a route to a proxy server (see [Configure SupportAssist](#) and [proxy-server](#)).

How do I log into the OS10 shell as the system administration?

Use `linuxadmin` as the username and password to enter OS10 at root level.

Where can I find additional installation information for my specific device?

See the *Getting Started Guide* shipped with your device or the platform-specific *Installation Guide* on the Dell Support page (see dell.com/support).

Hardware

What are the default console settings for ON-Series devices?

- Set the data rate to 115200 baud
- Set the data format to 8 bits, stop bits to 1, and no parity

- Set flow control to none

How do I view the hardware inventory?

Use the `show inventory` command to view complete system inventory.

How do I view the process-related information?

Use the `show processes node-id node-id-number [pid process-id]` command to view the process CPU utilization information.

Configuration

How do I enter CONFIGURATION mode?

Use the `configure terminal` command to change from EXEC mode to CONFIGURATION mode.

I made changes to the running configuration file but the updates are not showing. How do I view my changes?

Use the `show running-configuration` command to view changes that you have made to the running-configuration file. Here are the differences between the available configuration files:

- startup-configuration contains the configuration applied at device startup
- running-configuration contains the current configuration of the device
- candidate-configuration is an intermediate temporary buffer that stores configuration changes prior to applying them to the running-configuration

Security

How do I add new users?

Use the `username` commands to add new users. Use the `show users` command to view a list of current users.

How do I view RADIUS transactions to troubleshoot problems?

Use the `debug radius` command.

How do I view the current DHCP binding information?

Use the `show ip dhcp binding` command.

Layer 2

How do I view the VLAN running configuration?

Use the `show vlan` command to view all configured VLANs.

Layer 3

How do I view IPv6 interface information?

Use the `show ipv6 route summary` command.

How do I view summary information for all IP routes?

Use the `show running-configuration` command.

How do I view summary information for the OSPF database?

Use the `show ip ospf database` command.

How do I view configuration of OSPF neighbors connected to the local router?

Use the `show ip ospf neighbor` command.

System management

How can I view the current interface configuration?

Use the `show running-configuration` command to view all currently configured interfaces.

How can I view a list of all system devices?

Use the `show inventory` command to view a complete list.

How can I view the software version?

Use the `show version` command to view the currently running software version.

Access control lists

How do I setup filters to deny or permit packets from on IPv4 or IPv6 address?

Use the `deny` or `permit` commands to create ACL filters.

How do I clear access-list counters?

Use the `clear ip access-list counters`, `clear ipv6 access-list counters`, or `clear mac access-list counters` commands.

How do I setup filters to automatically assign sequencer numbers for specific addresses?

Use the `seq deny` or `seq permit` commands for specific packet filtering.

How do I view access-list and access-group information?

Use the `show {ip | mac | ipv6} access-group` and `show {ip | mac | ipv6} access-list` commands.

Quality of service

What are the QoS error messages?

Flow control error messages:

- `Error: priority-flow-control mode is on, disable pfc mode to enable LLFC`
- `% Warning: Make sure all qos-groups are matched in a single class in attached policy-map`

Priority flow control mode error message:

`% Error: LLFC flowcontrol is on, disable LLFC to enable PFC`

PFC shared-buffer size error message:

`% Error: Hardware update failed.`

Pause error message:

`% Error: Buffer-size should be greater than Pause threshold and Pause threshold should be greater than equal to Resume threshold.`

PFC cost of service error messages:

- `% Error: Not enough buffers are available, to enable system-qos wide pause for all pfc-cos values in the policymap`
- `% Error: Not enough buffers are available, to enable system-qos wide pause for the pfc-cos values in the policymap`
- `% Error: Not enough buffers are available, to enable pause for all pfc-cos values in the policymap for this interface`
- `% Warning: Not enough buffers are available, for lossy traffic. Expect lossy traffic drops, else reconfigure the pause buffers`

Monitoring

How can I check if SupportAssist is enabled?

Use the `show support-assist status` command to view current configuration information.

How can I view a list of alarms?

Use the `show alarms details` to view a list of all system alarms.

How do I enable or disable system logging?

Use the `logging enable` command or the `logging disable` command.

How do I view system logging messages?

Use the `show logging` command to view messages by log-file or process name.

Support resources

The Dell EMC Support site provides a range of documents and tools to assist you with effectively using Dell EMC devices. Through the support site you can obtain technical information regarding Dell EMC products, access software upgrades and patches, download available management software, and manage your open cases. The Dell EMC support site provides integrated, secure access to these services.

To access the Dell EMC Support site, go to www.dell.com/support/. To display information in your language, scroll down to the bottom of the page and select your country from the drop-down menu.

- To obtain product-specific information, enter the 7-character service tag or 11-digit express service code of your switch and click **Submit**.

To view the service tag or express service code, pull out the luggage tag on the chassis or enter the `show chassis` command from the CLI.

- To receive additional kinds of technical support, click **Contact Us**, then click **Technical Support**.

To access system documentation, see www.dell.com/manuals/.

To search for drivers and downloads, see www.dell.com/drivers/.

To participate in Dell EMC community blogs and forums, see www.dell.com/community.