

Lenovo Flex System EN4093R 10Gb Ethernet Scalable Switch

# ISCLI—Industry Standard CLI Command Reference

For Lenovo Network Operating System 8.4

**Lenovo**<sup>TM</sup>

**Note:** Before using this information and the product it supports, read the general information in the *Safety information and Environmental Notices and User Guide* documents on the *Lenovo Documentation CD* and the *Warranty Information* document that comes with the product.

Second Edition (July 2017)

© Copyright Lenovo 2017

Portions © Copyright IBM Corporation 2014.

**LIMITED AND RESTRICTED RIGHTS NOTICE:** If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Lenovo and the Lenovo logo are trademarks of Lenovo in the United States, other countries, or both.

---

# Contents

<b>Contents</b>	<b>. 3</b>
<b>Preface</b>	<b>15</b>
Who Should Use This Book	.16
How This Book Is Organized	.17
Typographic Conventions	.18
<b>Chapter 1. ISCLI Basics</b>	<b>21</b>
ISCLI Command Modes	.22
Global Commands	.26
Command Line Interface Shortcuts	.28
CLI List and Range Inputs	.28
Command Abbreviation	.28
Tab Completion	.28
User Access Levels	.29
Idle Timeout	.30
<b>Chapter 2. Information Commands</b>	<b>31</b>
System Information	.33
CLI Display Information	.34
Error Disable and Recovery Information	.35
SNMPv3 System Information	.36
SNMPv3 USM User Table Information	.37
SNMPv3 View Table Information	.38
SNMPv3 Access Table Information	.39
SNMPv3 Group Table Information	.40
SNMPv3 Community Table Information	.40
SNMPv3 Target Address Table Information	.41
SNMPv3 Target Parameters Table Information	.42
SNMPv3 Notify Table Information	.43
SNMPv3 Dump Information	.44
General System Information	.45
Show Software Version Brief	.46
Show Recent Syslog Messages	.47
Show Security Audit Log Messages	.48
User Status	.49
LDAP Information	.50
Stacking Information	.51
Stacking Switch Information	.53
Attached Switches Information	.54
Stack Name Information	.54
Stack Backup Switch Information	.54
Stack Version Information	.55
Stack Packet Path Information	.55
Stack Push Status Information	.56
Layer 2 Information	.57

FDB Information . . . . .	60
Show All FDB Information . . . . .	61
Show FDB Multicast Address Information . . . . .	62
Clearing Entries from the Forwarding Database . . . . .	62
Link Aggregation Control Protocol Information. . . . .	63
Link Aggregation Control Protocol . . . . .	63
Layer 2 Failover Information Commands . . . . .	64
Layer 2 Failover Information . . . . .	64
Hot Links Information. . . . .	66
Edge Control Protocol Information . . . . .	67
LLDP Information . . . . .	68
LLDP Remote Device Information . . . . .	69
Unidirectional Link Detection Information . . . . .	70
UDLD Port Information . . . . .	70
OAM Discovery Information . . . . .	71
OAM Port Information. . . . .	71
vLAG Information . . . . .	72
vLAG Aggregation Information. . . . .	72
vLAG Peer Gateway Information . . . . .	73
vLAG VRRP Information. . . . .	74
802.1X Information . . . . .	75
Spanning Tree Information. . . . .	77
RSTP/PVRST Information . . . . .	82
Spanning Tree Bridge Information. . . . .	84
Spanning Tree Root Information . . . . .	85
Multiple Spanning Tree Information . . . . .	86
LAG Information . . . . .	88
VLAN Information . . . . .	89
Layer 3 Information. . . . .	91
IP Routing Information . . . . .	94
Show All IP Route Information . . . . .	95
ARP Information . . . . .	97
Show All ARP Entry Information . . . . .	98
ARP Address List Information . . . . .	98
Dynamic ARP Inspection Information . . . . .	99
BGP Information . . . . .	100
BGP Peer information . . . . .	100
BGP Summary Information. . . . .	101
BGP Aggregation Information . . . . .	101
Dump BGP Information . . . . .	101
OSPF Information. . . . .	102
OSPF General Information . . . . .	103
OSPF Interface Loopback Information . . . . .	104
OSPF Interface Information. . . . .	104
OSPF Information Route Codes . . . . .	104
OSPF Database Information . . . . .	105
OSPFv3 Information . . . . .	107
OSPFv3 Information Dump. . . . .	108
OSPFv3 Interface Information. . . . .	109
OSPFv3 Routes Information . . . . .	109
OSPFv3 Database Information . . . . .	110

Routing Information Protocol . . . . .	111
RIP Routes Information . . . . .	111
RIP Interface Information . . . . .	111
IPv6 Routing Information . . . . .	112
IPv6 Routing Table . . . . .	113
IPv6 Neighbor Discovery Cache Information . . . . .	114
IPv6 Neighbor Discovery Cache Information . . . . .	114
IPv6 Neighbor Discovery Prefix Information . . . . .	115
ECMP Static Route Information . . . . .	116
ECMP Hashing Result . . . . .	116
IGMP Information . . . . .	117
IGMP Querier Information . . . . .	119
IGMP Group Information . . . . .	120
IGMP Multicast Router Information . . . . .	121
IPMC Group Information . . . . .	121
MLD information . . . . .	122
MLD Mrouter Information . . . . .	123
VRRP Information . . . . .	124
Interface Information . . . . .	125
IPv6 Interface Information . . . . .	126
IPv6 Path MTU Information . . . . .	127
IP Information . . . . .	128
IKEv2 Information . . . . .	129
IKEv2 Information Dump . . . . .	130
IPsec Information . . . . .	131
IPsec Manual Policy Information . . . . .	132
DHCP Snooping Information . . . . .	133
PIM Information . . . . .	134
PIM Component Information . . . . .	135
PIM Interface Information . . . . .	135
PIM Neighbor Information . . . . .	136
PIM Multicast Route Information Commands . . . . .	137
PIM Multicast Route Information . . . . .	138
Quality of Service Information . . . . .	139
802.1p Information . . . . .	140
WRED and ECN Information . . . . .	141
Access Control List Information Commands . . . . .	142
Access Control List Information . . . . .	143
OpenFlow Information . . . . .	144
OpenFlow Global Configuration Information . . . . .	145
OpenFlow Flow Allocation Information . . . . .	147
OpenFlow Group Information . . . . .	149
OpenFlow Configuration Information . . . . .	150
OpenFlow Table Information . . . . .	152
RMON Information Commands . . . . .	154
RMON History Information . . . . .	155
RMON Alarm Information . . . . .	156
RMON Event Information . . . . .	157

Link Status Information . . . . .	158
Port Information . . . . .	159
Port Transceiver Status . . . . .	161
VM Ready Information . . . . .	163
VMReady Information. . . . .	165
VM OUI Information . . . . .	165
VM Port Information . . . . .	166
VM Portchannel Information . . . . .	166
VM Information . . . . .	167
VM Check Information . . . . .	167
VM Group Information . . . . .	168
VM Bandwidth Information . . . . .	168
VM Profile Information . . . . .	168
VMware Information . . . . .	169
VMware Hello Information. . . . .	170
VMware Host Information . . . . .	170
VMware VM Information . . . . .	172
ESX Server - Switchport Mapping . . . . .	172
EVB Information . . . . .	173
EVB VSIType Information . . . . .	174
EVB VMs Information . . . . .	175
vNIC Information . . . . .	176
Virtual NIC (vNIC) Information . . . . .	177
vNIC Group Information . . . . .	178
SLP Information . . . . .	179
UFP Information . . . . .	180
Port Information . . . . .	181
CDCP Information . . . . .	182
QoS Information . . . . .	182
TLV Status Information . . . . .	183
Virtual Port Information . . . . .	184
VLAN Information . . . . .	185
TLV Information . . . . .	186
DCBX Information Commands . . . . .	188
Converged Enhanced Ethernet Information . . . . .	189
DCBX Information . . . . .	190
DCBX Control Information. . . . .	191
DCBX Feature Information . . . . .	192
DCBX ETS Information . . . . .	193
DCBX PFC Information . . . . .	194
DCBX Application Protocol Information . . . . .	195
ETS Information . . . . .	197
PFC Information . . . . .	198
FCoE Information . . . . .	199
FIP Snooping Information . . . . .	199
Information Dump . . . . .	201
<b>Chapter 3. Statistics Commands . . . . .</b>	<b>203</b>
Forwarding Database Statistics . . . . .	204
Port Statistics . . . . .	205

802.1X Authenticator Statistics . . . . .	207
802.1X Authenticator Diagnostics . . . . .	208
Bridging Statistics . . . . .	211
Ethernet Statistics . . . . .	212
Interface Statistics . . . . .	215
Interface Protocol Statistics . . . . .	218
Link Statistics. . . . .	218
RMON Statistics . . . . .	219
QoS Queue Statistics. . . . .	222
Link Aggregation Group (LAG) Statistics . . . . .	226
Trunk Group Interface Statistics. . . . .	226
Layer 2 Statistics . . . . .	227
LACP Statistics . . . . .	229
Hotlinks Statistics . . . . .	230
LLDP Port Statistics . . . . .	231
Spanning Tree Statistics . . . . .	232
OAM Statistics . . . . .	233
vLAG Statistics . . . . .	234
vLAG ISL Statistics . . . . .	234
vLAG Statistics . . . . .	234
Layer 3 Statistics . . . . .	236
IPv4 Statistics. . . . .	240
IPv6 Statistics. . . . .	243
IPv4 Route Statistics. . . . .	248
IPv6 Route Statistics . . . . .	249
ARP statistics. . . . .	250
DHCP Statistics. . . . .	251
DHCP Snooping Statistics . . . . .	251
DNS Statistics . . . . .	252
ICMP Statistics . . . . .	253
TCP Statistics . . . . .	255
UDP Statistics . . . . .	257
IGMP Statistics . . . . .	258
MLD Statistics . . . . .	260
MLD Global Statistics . . . . .	261
OSPF Statistics . . . . .	263
OSPF Global Statistics . . . . .	264
OSPFv3 Statistics . . . . .	268
OSPFv3 Global Statistics . . . . .	269
VRRP Statistics . . . . .	272
PIM Statistics. . . . .	273
Routing Information Protocol Statistics. . . . .	274
OpenFlow Statistics . . . . .	275
Management Processor Statistics . . . . .	291
Packet Statistics . . . . .	292
MP Packet Statistics . . . . .	292
Packet Statistics Log . . . . .	297
Packet Log example . . . . .	297
Packet Statistics Last Packet . . . . .	298

Packet Statistics Dump . . . . .	298
Logged Packet Statistics . . . . .	299
TCP Statistics. . . . .	303
UDP Statistics . . . . .	304
CPU Statistics . . . . .	304
CPU Statistics History . . . . .	306
Access Control List Statistics . . . . .	307
ACL Statistics . . . . .	308
ACL Meter Statistics . . . . .	308
VMAP Statistics . . . . .	308
Fibre Channel over Ethernet Statistics . . . . .	309
SNMP Statistics . . . . .	310
NTP Statistics . . . . .	314
PTP Statistics . . . . .	316
SLP Statistics. . . . .	317
Statistics Dump . . . . .	318
<b>Chapter 4. Configuration Commands . . . . .</b>	<b>319</b>
Viewing and Saving Changes . . . . .	321
Saving the Configuration . . . . .	321
System Configuration . . . . .	322
System Error Disable and Recovery Configuration . . . . .	326
Link Flap Dampening Configuration. . . . .	327
System Host Log Configuration. . . . .	328
SSH Server Configuration . . . . .	331
RADIUS Server Configuration . . . . .	333
TACACS+ Server Configuration . . . . .	335
LDAP Server Configuration . . . . .	339
NTP Server Configuration . . . . .	341
NTP MD5 Key Commands . . . . .	343
System SNMP Configuration . . . . .	344
SNMPv3 Configuration . . . . .	346
User Security Model Configuration . . . . .	348
SNMPv3 View Configuration . . . . .	349
View-based Access Control Model Configuration . . . . .	350
SNMPv3 Group Configuration . . . . .	351
SNMPv3 Community Table Configuration . . . . .	352
SNMPv3 Target Address Table Configuration. . . . .	353
SNMPv3 Target Parameters Table Configuration . . . . .	354
SNMPv3 Notify Table Configuration . . . . .	355
System Access Configuration. . . . .	356
Management Network Configuration . . . . .	358
NETCONF Configuration . . . . .	359
User Access Control Configuration . . . . .	360
System User ID Configuration . . . . .	361
Strong Password Configuration . . . . .	362
HTTPS Access Configuration . . . . .	363
Custom Daylight Saving Time Configuration. . . . .	366
sFlow Configuration . . . . .	367



sFlow Port Configuration . . . . .	367
Port Configuration . . . . .	368
Port Error Disable and Recovery Configuration . . . . .	373
Port Link Configuration . . . . .	374
Temporarily Disabling a Port . . . . .	374
Unidirectional Link Detection Configuration . . . . .	375
Port OAM Configuration . . . . .	376
Port ACL Configuration . . . . .	377
Port WRED Configuration . . . . .	378
Port WRED Transmit Queue Configuration . . . . .	379
Management Port Configuration . . . . .	380
Stacking Configuration . . . . .	381
Stacking Switch Configuration . . . . .	382
Management Interface Configuration . . . . .	383
Quality of Service Configuration . . . . .	384
802.1p Configuration . . . . .	384
DSCP Configuration . . . . .	385
Control Plane Protection . . . . .	386
Weighted Random Early Detection Configuration . . . . .	388
WRED Transmit Queue Configuration . . . . .	388
Access Control Configuration . . . . .	390
Access Control List Configuration . . . . .	391
Ethernet Filtering Configuration . . . . .	392
IPv4 Filtering Configuration . . . . .	393
TCP/UDP Filtering Configuration . . . . .	394
Packet Format Filtering Configuration . . . . .	395
ACL IPv6 Configuration . . . . .	396
IPv6 Filtering Configuration . . . . .	397
IPv6 TCP/UDP Filtering Configuration . . . . .	398
IPv6 Metering Configuration . . . . .	399
Management ACL Filtering Configuration . . . . .	400
TCP/UDP Filtering Configuration . . . . .	401
VMAP Configuration . . . . .	402
ACL Group Configuration . . . . .	407
ACL Metering Configuration . . . . .	408
ACL Re-Mark Configuration . . . . .	409
Re-Marking In-Profile Configuration . . . . .	410
Re-Marking Out-Profile Configuration . . . . .	410
IPv6 Re-Marking Configuration . . . . .	411
IPv6 Re-Marking In-Profile Configuration . . . . .	412
IPv6 Re-Marking Out-Profile Configuration . . . . .	412
Port Mirroring . . . . .	413
Port Mirroring Configuration . . . . .	414
Layer 2 Configuration . . . . .	415
802.1X Configuration . . . . .	416
802.1X Global Configuration . . . . .	416
802.1X Guest VLAN Configuration . . . . .	418
802.1X Port Configuration . . . . .	419

Spanning Tree Configuration. . . . .	421
MSTP Configuration. . . . .	424
RSTP/PVRST Configuration . . . . .	427
Forwarding Database Configuration. . . . .	431
Static Multicast MAC Configuration . . . . .	433
Static FDB Configuration. . . . .	434
LLDP Configuration . . . . .	435
LLDP Port Configuration. . . . .	436
LLDP Optional TLV configuration. . . . .	437
Link Aggregation Group (LAG) Configuration . . . . .	439
Link Aggregation Group (LAG) Hash Configuration . . . . .	440
FCoE LAG Hash Configuration . . . . .	441
Layer 2 LAG Hash. . . . .	442
Layer 3 LAG Hash. . . . .	443
Virtual Link Aggregation Control Protocol Configuration . . . . .	444
vLAG Health Check Configuration . . . . .	446
vLAG ISL Configuration . . . . .	446
Link Aggregation Control Protocol Configuration. . . . .	447
LACP Port Configuration . . . . .	448
Layer 2 Failover Configuration . . . . .	450
Failover Trigger Configuration . . . . .	451
Auto Monitor Configuration . . . . .	451
Failover Manual Monitor Port Configuration . . . . .	452
Failover Manual Monitor Control Configuration . . . . .	453
Hot Links Configuration. . . . .	454
Hot Links Trigger Configuration . . . . .	455
Hot Links Master Configuration. . . . .	456
Hot Links Backup Configuration . . . . .	457
VLAN Configuration . . . . .	458
Protocol-Based VLAN Configuration . . . . .	460
Private VLAN Configuration . . . . .	462
Layer 3 Configuration. . . . .	463
IP Interface Configuration . . . . .	465
IPv6 Neighbor Discovery Configuration . . . . .	467
Default Gateway Configuration. . . . .	469
IPv4 Static Route Configuration. . . . .	471
IP Multicast Route Configuration . . . . .	472
ARP Configuration . . . . .	473
ARP Static Configuration. . . . .	474
Dynamic ARP Inspection Configuration . . . . .	475
IP Forwarding Configuration. . . . .	476
Network Filter Configuration. . . . .	477
Routing Map Configuration . . . . .	478
IP Access List Configuration . . . . .	480
Autonomous System Filter Path Configuration . . . . .	481
Routing Information Protocol Configuration . . . . .	482
RIP Interface Configuration. . . . .	482
RIP Route Redistribution Configuration . . . . .	484

Open Shortest Path First Configuration . . . . .	485
Area Index Configuration . . . . .	486
OSPF Summary Range Configuration . . . . .	488
OSPF Interface Configuration . . . . .	489
OSPF Virtual Link Configuration . . . . .	491
OSPF Host Entry Configuration . . . . .	492
OSPF Route Redistribution Configuration . . . . .	493
OSPF MD5 Key Configuration . . . . .	493
Open Shortest Path First Version 3 Configuration . . . . .	494
OSPFv3 Area Index Configuration . . . . .	496
OSPFv3 Summary Range Configuration . . . . .	498
OSPFv3 AS-External Range Configuration . . . . .	499
OSPFv3 Interface Configuration . . . . .	500
OSPFv3 over IPSec Configuration . . . . .	502
OSPFv3 Virtual Link Configuration . . . . .	504
OSPFv3 Host Entry Configuration . . . . .	506
OSPFv3 Redistribute Entry Configuration . . . . .	506
OSPFv3 Redistribute Configuration . . . . .	507
Border Gateway Protocol Configuration . . . . .	508
BGP Peer Configuration . . . . .	509
BGP Aggregation Configuration. . . . .	511
BGP Neighbor Redistribution Configuration . . . . .	513
Multicast Listener Discovery Protocol Configuration. . . . .	514
MLD Interface Configuration . . . . .	514
IGMP Configuration. . . . .	516
IGMP Snooping Configuration . . . . .	517
IGMPv3 Configuration . . . . .	518
IGMP Relay Configuration . . . . .	519
IGMP Filtering Configuration . . . . .	519
IGMP Relay Multicast Router Configuration . . . . .	521
IGMP Static Multicast Router Configuration . . . . .	522
IGMP Advanced Configuration . . . . .	523
IGMP Querier Configuration . . . . .	524
IKEv2 Configuration . . . . .	526
IKEv2 Proposal Configuration. . . . .	526
IKEv2 Preshare Key Configuration. . . . .	527
IKEv2 Identification Configuration . . . . .	527
IPsec Configuration . . . . .	528
IPsec Transform Set Configuration. . . . .	528
IPsec Traffic Selector Configuration . . . . .	529
IPsec Dynamic Policy Configuration . . . . .	529
IPsec Manual Policy Configuration . . . . .	530
Domain Name System Configuration . . . . .	533
Bootstrap Protocol Relay Configuration . . . . .	534
BOOTP Relay Broadcast Domain Configuration . . . . .	534
VRRP Configuration. . . . .	535
Virtual Router Configuration . . . . .	537
Virtual Router Priority Tracking Configuration . . . . .	539
Virtual Router Group Configuration . . . . .	540
Virtual Router Group Priority Tracking Configuration . . . . .	542
VRRP Interface Configuration. . . . .	543
VRRP Tracking Configuration. . . . .	544

Protocol Independent Multicast Configuration . . . . .	545
PIM Component Configuration . . . . .	546
RP Candidate Configuration . . . . .	546
RP Static Configuration . . . . .	546
PIM Interface Configuration . . . . .	547
IPv6 Default Gateway Configuration . . . . .	549
IPv6 Static Route Configuration. . . . .	550
IPv6 Neighbor Discovery Cache Configuration . . . . .	551
IPv6 Neighbor Discovery Prefix Configuration . . . . .	551
IPv6 Prefix Policy Table Configuration. . . . .	553
IPv6 Path MTU Configuration . . . . .	554
IP Loopback Interface Configuration . . . . .	555
DHCP Snooping . . . . .	556
Converged Enhanced Ethernet Configuration . . . . .	557
ETS Global Configuration . . . . .	558
ETS Global Priority Group Configuration. . . . .	558
Priority Flow Control Configuration. . . . .	560
Global Priority Flow Control Configuration. . . . .	560
Port-level 802.1p PFC Configuration . . . . .	561
DCBX Port Configuration . . . . .	562
Fibre Channel over Ethernet Configuration . . . . .	563
FIPS Port Configuration . . . . .	564
Remote Monitoring Configuration . . . . .	565
RMON History Configuration . . . . .	565
RMON Event Configuration . . . . .	566
RMON Alarm Configuration . . . . .	567
VMReady . . . . .	569
VM Policy Bandwidth Management. . . . .	570
VM Group Configuration . . . . .	571
VM Check Configuration . . . . .	574
VM Profile Configuration . . . . .	575
VMWare Configuration . . . . .	576
Miscellaneous VMready Configuration . . . . .	577
Virtual NIC Configuration. . . . .	578
Virtual NIC Group Configuration. . . . .	578
vNIC Port Configuration. . . . .	580
UFP Configuration . . . . .	581
Edge Virtual Bridge Configuration . . . . .	584
Edge Virtual Bridge Profile Configuration . . . . .	586
OpenFlow Configuration . . . . .	587
Static Flows Configuration . . . . .	597
Switch Partition (SPAR) Configuration . . . . .	600
Precision Time Protocol Configuration . . . . .	602
Service Location Protocol Configuration. . . . .	604
Configuration Dump . . . . .	605
Saving the Active Switch Configuration . . . . .	606
Restoring the Active Switch Configuration. . . . .	607

<b>Chapter 5. Operations Commands . . . . .</b>	<b>. 609</b>
Operations-Level Port Commands . . . . .	610
Operations-Level Port 802.1X Commands . . . . .	611
Operations-Level VRRP Commands. . . . .	612
Operations-Level BGP Commands . . . . .	613
Protected Mode Options. . . . .	614
VMware Operations . . . . .	616
VMware Distributed Virtual Switch Operations. . . . .	618
VMware Distributed Port Group Operations . . . . .	619
Edge Virtual Bridge Operations. . . . .	620
Feature on Demand Key Options . . . . .	621
<b>Chapter 6. Boot Options . . . . .</b>	<b>. 623</b>
Stacking Boot Options. . . . .	624
Scheduled Reboot. . . . .	627
Netboot Configuration . . . . .	628
Flexible Port Mapping. . . . .	629
QSFP Port Configuration . . . . .	630
SIOM Configuration . . . . .	631
Configuring the Number of Spanning Tree Groups . . . . .	632
Updating the Switch Software Image . . . . .	633
Loading New Software to Your Switch. . . . .	633
Selecting a Software Image to Run. . . . .	634
Uploading a Software Image from Your Switch . . . . .	634
Selecting a Configuration Block. . . . .	636
Rebooting the Switch . . . . .	637
Changing the Switch Profile . . . . .	638
Using the Boot Management Menu . . . . .	639
Boot Recovery Mode . . . . .	640
Recover from a Failed Image Upgrade using TFTP. . . . .	641
Recovering from a Failed Image Upgrade using XModem Download . . . . .	643
Physical Presence . . . . .	645
<b>Chapter 7. Maintenance Commands . . . . .</b>	<b>. 647</b>
Forwarding Database Maintenance . . . . .	649
Debugging Commands . . . . .	651
IP Security Debugging. . . . .	654
vLAG Debugging. . . . .	655
ARP Cache Maintenance. . . . .	656
IP Route Manipulation . . . . .	657
LLDP Cache Manipulation. . . . .	658
IGMP Group Maintenance . . . . .	659
IGMP Multicast Routers Maintenance . . . . .	660
IPv6 Neighbor Discovery Cache Manipulation . . . . .	662
IPv6 Route Maintenance. . . . .	663
Stacking Maintenance . . . . .	664
TFTP, SFTP or FTP System Dump Copy . . . . .	665
Clearing Dump Information . . . . .	666

<b>Appendix A. Enterprise NOS System Log Messages</b>	<b>667</b>
LOG_ALERT	668
LOG_CRIT	671
LOG_ERR	672
LOG_INFO	674
LOG_NOTICE	678
LOG_WARNING	682
<b>Appendix B. Getting help and technical assistance.</b>	<b>685</b>
<b>Appendix C. Notices</b>	<b>687</b>
Trademarks	689
Important Notes	690
Recycling Information.	691
Particulate Contamination.	692
Telecommunication Regulatory Statement	693
Electronic Emission Notices	694
Federal Communications Commission (FCC) Statement	694
Industry Canada Class A Emission Compliance Statement	694
Avis de Conformité à la Réglementation d'Industrie Canada	694
Australia and New Zealand Class A Statement	694
European Union - Compliance to the Electromagnetic Compatibility Directive	695
Germany Class A Statement	695
Japan VCCI Class A Statement	696
Japan Electronics and Information Technology Industries Association (JEITA) Statement	697
Korea Communications Commission (KCC) Statement	697
Russia Electromagnetic Interference (EMI) Class A Statement	697
People's Republic of China Class A electronic emission Statement	697
Taiwan Class A compliance Statement	697
<b>Index</b>	<b>699</b>

---

# Preface

The *Lenovo Flex System Fabric SI4093 System Interconnect Module ISCLI Command Reference* describes how to configure and use the Enterprise NOS 8.4 software with your Lenovo Flex System EN4093R 10Gb Ethernet Scalable Switch (referred to as EN4093R throughout this document). This guide lists each command, together with the complete syntax and a functional description, from the IS Command Line Interface (ISCLI).

For documentation on installing the switches physically, see the *Installation Guide* for your EN4093R. For details about the configuration and operation of the EN4093R, see the *Lenovo N/OS 8.4 Application Guide*.

---

## Who Should Use This Book

This book is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, the Spanning Tree Protocol and SNMP configuration parameters.



---

## How This Book Is Organized

[Chapter 1, “ISCLI Basics,”](#) describes how to connect to the switch and access the information and configuration commands. This chapter provides an overview of the command syntax, including command modes, global commands, and shortcuts.

[Chapter 2, “Information Commands,”](#) shows how to view switch configuration parameters.

[Chapter 3, “Statistics Commands,”](#) shows how to view switch performance statistics.

[Chapter 4, “Configuration Commands,”](#) shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing, Link Aggregation, and more.

[Chapter 5, “Operations Commands,”](#) shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The commands describe how to activate or deactivate optional software features.

[Chapter 6, “Boot Options,”](#) describes the use of the primary and alternate switch images, how to load a new software image, and how to reset the software to factory defaults.

[Chapter 7, “Maintenance Commands,”](#) shows how to generate and access a dump of critical switch state information, how to clear it, and how to clear part or all of the forwarding database.

[Appendix A, “Enterprise NOS System Log Messages,”](#) lists Enterprise NOS System Log Messages.

[Appendix B, “Getting help and technical assistance,”](#) contains information on how to get help, service, technical assistance, or more information about Lenovo products.

[Appendix C, “Notices,”](#) displays Lenovo legal information.

[“Index”](#) includes pointers to the description of the key words used throughout the book.

# Typographic Conventions

The following table describes the typographic styles used in this book.

**Table 1.** *Typographic Conventions*

Typeface or Symbol	Meaning
plain fixed-width text	This type is used for names of commands, files, and directories used within the text. For example:  View the <code>readme.txt</code> file.  It also depicts on-screen computer output and prompts.
<b>bold fixed-width text</b>	This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example:  <b>show sys-info</b>
<b>bold body text</b>	This bold type indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.
<i>italicized body text</i>	This italicized type indicates book titles, special terms, or words to be emphasized.
angle brackets < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command.  Example: If the command syntax is <b>ping</b> <IP address>  you enter <b>ping 192.32.10.12</b>
braces { }	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.  Example: If the command syntax is <b>show portchannel</b> {<1-128> hash information}  you enter: <b>show portchannel</b> <1-128>  or <b>show portchannel hash</b>  or <b>show portchannel information</b>

**Table 1.** *Typographic Conventions*

Typeface or Symbol	Meaning
brackets [ ]	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is <b>show interface ip [&lt;1-128&gt;]</b></p> <p>you enter <b>show interface ip</b></p> <p>or <b>show interface ip &lt;1-128&gt;</b></p>
vertical line	<p>Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is <b>show portchannel {&lt;1-128&gt; hash information}</b></p> <p>you must enter: <b>show portchannel &lt;1-128&gt;</b></p> <p>or <b>show portchannel hash</b></p> <p>or <b>show portchannel information</b></p>



---

# Chapter 1. ISCLI Basics

Your EN4093R 10Gb Ethernet Scalable Switch (EN4093R) is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

This guide describes the individual ISCLI commands available for the EN4093R.

The ISCLI provides a direct method for collecting switch information and performing switch configuration. Using a basic terminal, the ISCLI allows you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the IS Command Line Interface (ISCLI) for the switch.

## ISCLI Command Modes

The ISCLI has three major command modes listed in order of increasing privileges, as follows:

- **User EXEC mode**

This is the initial mode of access. By default, password checking is disabled for this mode, on console.

- **Privileged EXEC mode**

This mode is accessed from User EXEC mode. This mode can be accessed using the following command: **enable**

- **Global Configuration mode**

This mode allows you to make changes to the running configuration. If you save the configuration, the settings survive a reload of the EN4093R. Several sub-modes can be accessed from the Global Configuration mode. For more details, see [Table 1](#). This mode can be accessed using the following command: **configure terminal**

Each mode provides a specific set of commands. The command set of a higher-privilege mode is a superset of a lower-privilege mode—all lower-privilege mode commands are accessible when using a higher-privilege mode.

[Table 1](#) lists the ISCLI command modes.

**Table 1.** ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
User EXEC EN 4093>	Default mode, entered automatically on console Exit: <b>exit</b> or <b>logout</b>
Privileged EXEC EN 4093#	Enter Privileged EXEC mode, from User EXEC mode: <b>enable</b> Exit to User EXEC mode: <b>disable</b> Quit ISCLI: <b>exit</b> or <b>logout</b>
Global Configuration EN 4093(config)#	Enter Global Configuration mode, from Privileged EXEC mode: <b>configure terminal</b> Exit to Privileged EXEC: <b>end</b> or <b>exit</b>
Interface IP EN 4093(config-ip-if)#	Enter Interface IP Configuration mode, from Global Configuration mode: <b>interface ip</b> <interface number> Internal Management IP interface is reachable only by Management Module. Exit to Global Configuration mode: <b>exit</b> Exit to Privileged EXEC mode: <b>end</b>

**Table 1. ISCLI Command Modes (continued)**

Command Mode/Prompt	Command used to enter or exit
Interface Loopback EN 4093(config-ip-loopback)#	Enter Interface Loopback Configuration mode, from Global Configuration mode: <b>interface loopback</b> <1-5>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
Interface Port EN 4093(config-if)#	Enter Port Configuration mode, from Global Configuration mode: <b>interface port</b> <port number or alias>  Exit to Privileged EXEC mode: <b>exit</b>  Exit to Global Configuration mode: <b>end</b>
Interface PortChannel EN 4093(config-PortChannel)#	Enter PortChannel Configuration mode, from Global Configuration mode: <b>interface portchannel</b> {<portchannel number> lacp <key>}  Exit to Privileged EXEC mode: <b>exit</b>  Exit to Global Configuration mode: <b>end</b>
VLAN EN 4093(config-vlan)#	Enter VLAN Configuration mode, from Global Configuration mode: <b>vlan</b> <VLAN number>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
Router OSPF EN 4093(config-router-ospf)#	Enter OSPF Configuration mode, from Global Configuration mode: <b>router ospf</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
Router OSPFv3 EN 4093(config-router-ospf3)#	Enter OSPFv3 Configuration mode, from Global Configuration mode: <b>ipv6 router ospf</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
Router BGP EN 4093(config-router-bgp)#	Enter BGP Configuration mode, from Global Configuration mode: <b>router bgp</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>

**Table 1.** ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
Router RIP EN 4093(config-router-rip)#	Enter RIP Configuration mode, from Global Configuration mode: <b>router rip</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
Route Map EN 4093(config-route-map)#	Enter Route Map Configuration mode, from Global Configuration mode: <b>route-map</b> <1-32>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
Router VRRP EN 4093(config-vrrp)#	Enter VRRP Configuration mode, from Global Configuration mode: <b>router vrrp</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
IKEv2 Proposal EN 4093(config-ikev2-prop)#	Enter IKEv2 Proposal Configuration mode, from Global Configuration mode: <b>ikev2 proposal</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
MLD Configuration EN 4093(config-router-mld)#	Enter Multicast Listener Discovery Protocol Configuration mode, from Global Configuration mode: <b>ipv6 mld</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
MST Configuration EN 4093(config-mst)#	Enter Multiple Spanning Tree Protocol Configuration mode, from Global Configuration mode: <b>spanning-tree mst configuration</b>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
OpenFlow Instance EN 4093(config-openflow-instance)#	Enter OpenFlow Instance Configuration mode, from Global Configuration mode: <b>openflow instance</b> <1-2>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>



**Table 1. ISCLI Command Modes (continued)**

Command Mode/Prompt	Command used to enter or exit
VSI Database EN 4093(conf-vsldb)#	Enter Virtual Station Interface Database Configuration mode, from Global Configuration mode: <b>virt evb vsldb</b> <VSIDB_number>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
EVB Profile EN 4093(conf-evbprof)#	Enter Edge Virtual Bridging Profile Configuration mode, from Global Configuration mode: <b>virt evb profile</b> <1-16>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
UFP Virtual Port Configuration EN 4093(config_ufp_vport)#	Enter Unified Fabric Port Virtual Port Configuration mode, from Global Configuration mode: <b>ufp port</b> <port no.> <b>vport</b> <1-4>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>
SPAR Configuration EN 4093(config-spar)#	Enter Switch Partition Configuration mode, from Global Configuration mode: <b>spar</b> <1-8>  Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>

## Global Commands

Some basic commands are recognized throughout the ISCLI command modes. These commands are useful for obtaining online help, navigating through the interface, and for saving configuration changes.

For help on a specific command, type the command, followed by `help`.

**Table 2.** Description of Global Commands

Command	Action
<code>?</code>	Provides more information about a specific command or lists commands available at the current level.
<code>list</code>	Lists the commands available at the current level.
<code>exit</code>	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
<code>copy running-config startup-config</code>	Write configuration changes to non-volatile flash memory.
<code>logout</code>	Exit from the command line interface and log out.
<code>ping</code>	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre><b>ping</b> &lt;host name&gt;   &lt;IP address&gt; [-n &lt;tries (0-4294967295)&gt;] [-w &lt;msec delay (0-4294967295)&gt;] [-l &lt;length (0/32-65500/2080)&gt;] [-s &lt;IP source&gt;] [-v &lt;tos (0-255)&gt;] [-f] [-t]</pre> <p>Where:</p> <ul style="list-style-type: none"> <li>o <b>-n</b>: Sets the number of attempts (optional).</li> <li>o <b>-w</b>: Sets the number of milliseconds between attempts (optional).</li> <li>o <b>-l</b>: Sets the ping request payload size (optional).</li> <li>o <b>-s</b>: Sets the IP source address for the IP packet (optional).</li> <li>o <b>-v</b>: Sets the Type Of Service bits in the IP header.</li> <li>o <b>-f</b>: Sets the <i>don't fragment</i> bit in the IP header (only for IPv4 addresses).</li> <li>o <b>-t</b>: Pings continuously (same as <b>-n 0</b>).</li> </ul> <p>Where the <i>IP address</i> or <i>hostname</i> specify the target device. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Tries</i> (optional) is the number of attempts (1-32), and <i>msec delay</i> (optional) is the number of milliseconds between attempts.</p>

**Table 2.** Description of Global Commands (continued)

Command	Action
<b>traceroute</b>	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <p><b>traceroute</b> {&lt;hostname&gt; &lt;IP address&gt;} [&lt;max-hops (1-32)&gt; [&lt;msec-delay (1-4294967295)&gt;]]</p> <p>Where <i>hostname/IP address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-32 devices), and <i>msec-delay</i> (optional) is the number of milliseconds to wait for the response.</p> <p>As with ping, the DNS parameters must be configured if specifying hostnames.</p>
<b>telnet</b>	<p>This command is used to form a Telnet session between the switch and another network device. The format is as follows:</p> <p><b>telnet</b> {&lt;hostname&gt; &lt;IP address&gt;} [&lt;port&gt;]</p> <p>Where <i>IP address</i> or <i>hostname</i> specifies the target station. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Port</i> is the logical Telnet port or service number.</p>
<b>show history</b>	This command displays the last ten issued commands.
<b>show who</b>	Displays a list of users who are currently logged in.
<b>show line</b>	Displays a list of users who are currently logged in, in table format.

---

## Command Line Interface Shortcuts

The following shortcuts allow you to enter commands quickly and easily.

### CLI List and Range Inputs

For VLAN and port commands that allow an individual item to be selected from within a numeric range, lists and ranges of items can now be specified. For example, the `vlan` command permits the following options:

```
EN 4093(config)# vlan 1,3,4095           (access VLANs 1, 3, and 4095)
EN 4093(config)# vlan 1-20             (access VLANs 1 through 20)
EN 4093(config)# vlan 1-5,90-99,4090-4095 (access multiple ranges)
EN 4093(config)# vlan 1-5,19,20,4090-4095 (access a mix of lists and ranges)
```

The numbers in a range must be separated by a dash: *<start of range>-<end of range>*

Multiple ranges or list items are permitted using a comma: *<range or item 1>, <range or item 2>*

Do not use spaces within list and range specifications.

Ranges can also be used to apply the same command option to multiple items. For example, to access multiple ports with one command:

```
EN 4093(config)# interface port 1-4    (access ports 1 through 4)
```

### Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same mode. For example, consider the following full command and a valid abbreviation:

```
EN 4093(config)# show mac-address-table interface port 12
```

or:

```
EN 4093(config)# sh ma i p 12
```

### Tab Completion

By entering the first letter of a command at any prompt and pressing `<Tab>`, the ISCLI displays all available commands or options that begin with that letter. Entering additional letters further refines the list of commands or options displayed. If only one command fits the input text when `<Tab>` is pressed, that command is supplied on the command line, waiting to be entered.

---

## User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the EN4093R. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- **user**

Interaction with the switch is completely passive—nothing can be changed on the EN4093R. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.

- **oper**

Operators can make temporary changes on the EN4093R. These changes are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.

- **admin**

Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot or reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the EN4093R. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

**Note:** It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies.

**Table 3.** *User Access Levels*

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	
Operator	The Operator can make temporary changes that are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations.	
Administrator	The superuser Administrator has complete access to all command modes, information, and configuration commands on the EN4093R, including the ability to change both the user and administrator passwords.	admin

**Note:** With the exception of the “admin” user, access to each user level can be disabled by setting the password to an empty value.

---

## Idle Timeout

By default, the switch will disconnect your Telnet session after ten minutes of inactivity. This function is controlled by the following command, which can be set from 1 to 60 minutes, or disabled when set to 0:

**system idle** <0-60>

**Command mode:** Global Configuration

---

## Chapter 2. Information Commands

You can view configuration information for the switch in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch information.

**Table 4.** *Information Commands*

<b>Command Syntax and Usage</b>
<p><b>show interface status</b> <i>&lt;port alias or number&gt;</i></p> <p>Displays configuration information about the selected port(s), including:</p> <ul style="list-style-type: none"><li>○ Port alias and number</li><li>○ Port speed</li><li>○ Duplex mode (half, full, or auto)</li><li>○ Flow control for transmit and receive (no, yes, or both)</li><li>○ Link status (up, down, or disabled)</li></ul> <p>For details, see <a href="#">page 158</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show interface trunk</b> <i>&lt;port alias or number&gt;</i></p> <p>Displays port status information, including:</p> <ul style="list-style-type: none"><li>○ Port alias and number</li><li>○ Whether the port uses VLAN Tagging or not</li><li>○ Port VLAN ID (PVID)</li><li>○ Port name</li><li>○ VLAN membership</li><li>○ FDB Learning status</li><li>○ Flooding status</li></ul> <p>For details, see <a href="#">page 159</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show interface transceiver</b></p> <p>Displays the status of the port transceiver module on each external port. For details, see <a href="#">page 161</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show software-key</b></p> <p>Displays the enabled software features.</p> <p><b>Command mode:</b> All</p>

**Table 4.** *Information Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>show information-dump</b></p> <p>Dumps all switch information available (10K or more, depending on your configuration).</p> <p>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.</p> <p><b>Command mode:</b> All</p>



---

## System Information

The information provided by each command option is briefly described in [Table 5 on page 33](#), with pointers to where detailed information can be found.

**Table 5.** *System Information Commands*

Command Syntax and Usage
<p><b>show sys-info</b></p> <p>Displays system information, including:</p> <ul style="list-style-type: none"><li>o System date and time</li><li>o Switch model name and number</li><li>o Switch name and location</li><li>o Time of last boot</li><li>o MAC address of the switch management processor</li><li>o IP address of management interface</li><li>o Hardware version and part number</li><li>o Software image file and version number</li><li>o Configuration name</li><li>o Log-in banner, if one is configured</li><li>o Internal temperatures</li></ul> <p>For details, see <a href="#">page 45</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show logging [severity &lt;0-7&gt;] [reverse]</b></p> <p>Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the <b>show logging messages</b> command.</p> <p>For details, see <a href="#">page 47</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show access user</b></p> <p>Displays configured user names and their status.</p> <p><b>Command mode:</b> Privileged EXEC</p>

## CLI Display Information

These commands allow you to display information about the number of lines per screen displayed in the CLI.

**Table 6.** *CLI Display Information Options*

<b>Command Syntax and Usage</b>
<b>show terminal-length</b> Displays the number of lines per screen displayed in the CLI for the current session. A value of 0 means paging is disabled. <b>Command mode:</b> All
<b>show line console length</b> Displays the current line console length setting. For details, see <a href="#">page 322</a> . <b>Command mode:</b> All
<b>show line vty length</b> Displays the current line vty length setting. For details, see <a href="#">page 322</a> . <b>Command mode:</b> All

## Error Disable and Recovery Information

These commands allow you to display information about the Error Disable and Recovery feature for interface ports.

**Table 7.** *Error Disable Information Commands*

<b>Command Syntax and Usage</b>
<b>show errdisable [information]</b> Displays all Error Disable and Recovery information. <b>Command mode:</b> All
<b>show errdisable link-flap [information]</b> Displays the current Link Flap Dampening parameters. The <code>information</code> option displays ports that have been disabled due to excessive link flaps. <b>Command mode:</b> All
<b>show errdisable recovery</b> Displays a list of ports with their Error Recovery status. <b>Command mode:</b> All
<b>show errdisable timers</b> Displays a list of active recovery timers, if applicable. <b>Command mode:</b> All

## SNMPv3 System Information

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

**Table 8.** *SNMPv3 Commands*

Command Syntax and Usage
<b>show snmp-server v3 user</b> Displays User Security Model (USM) table information. To view the table, see <a href="#">page 37</a> . <b>Command mode:</b> All
<b>show snmp-server v3 view</b> Displays information about view, subtrees, mask and type of view. To view a sample, see <a href="#">page 38</a> . <b>Command mode:</b> All
<b>show snmp-server v3 access</b> Displays View-based Access Control information. To view a sample, see <a href="#">page 39</a> . <b>Command mode:</b> All
<b>show snmp-server v3 group</b> Displays information about the group, including the security model, user name, and group name. To view a sample, see <a href="#">page 40</a> . <b>Command mode:</b> All
<b>show snmp-server v3 community</b> Displays information about the community table information. To view a sample, see <a href="#">page 40</a> . <b>Command mode:</b> All
<b>show snmp-server v3 target-address</b> Displays the Target Address table information. To view a sample, see <a href="#">page 41</a> . <b>Command mode:</b> All
<b>show snmp-server v3 target-parameters</b> Displays the Target parameters table information. To view a sample, see <a href="#">page 42</a> . <b>Command mode:</b> All

**Table 8.** *SNMPv3 Commands (continued)*

<b>Command Syntax and Usage</b>
<b>show snmp-server v3 notify</b> Displays the Notify table information. To view a sample, see <a href="#">page 43</a> . <b>Command mode:</b> All
<b>show snmp-server v3</b> Displays all the SNMPv3 information. To view a sample, see <a href="#">page 44</a> . <b>Command mode:</b> All

## SNMPv3 USM User Table Information

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The following command displays SNMPv3 user information:

**show snmp-server v3 user**

**Command mode:** All

The USM user table contains the following information:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol

usmUser Table:	
User Name	Protocol
-----	-----
adminmd5	HMAC_MD5, DES PRIVACY
adminsha	HMAC_SHA, DES PRIVACY
v1v2only	NO AUTH, NO PRIVACY

**Table 9.** *USM User Table Information Parameters*

Field	Description
User Name	This is a string that represents the name of the user that you can use to access the switch.
Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. Enterprise NOS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

## SNMPv3 View Table Information

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

The following command displays the SNMPv3 View Table:

```
show snmp-server v3 view
```

**Command mode:** All

View Name	Subtree	Mask	Type
iso	1		included
v1v2only	1		included
v1v2only	1.3.6.1.6.3.15		excluded
v1v2only	1.3.6.1.6.3.16		excluded
v1v2only	1.3.6.1.6.3.18		excluded

**Table 10.** *SNMPv3 View Table Information Parameters*

Field	Description
View Name	Displays the name of the view.
Subtree	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
Mask	Displays the bit mask.
Type	Displays whether a family of view subtrees is included or excluded from the MIB view.

## SNMPv3 Access Table Information

The access control subsystem provides authorization services.

The `vacmAccessTable` maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

The following command displays SNMPv3 access information:

```
show snmp-server v3 access
```

**Command mode:** All

Group Name	Model	Level	ReadV	WriteV	NotifyV
v1v2grp	snmpv1	noAuthNoPriv	iso	iso	v1v2only
admingrp	usm	authPriv	iso	iso	iso

**Table 11.** *SNMPv3 Access Table Information*

Field	Description
Group Name	Displays the name of group.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, <code>noAuthNoPriv</code> , <code>authNoPriv</code> , or <code>authPriv</code> .
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

## SNMPv3 Group Table Information

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

The following command displays SNMPv3 group information:

```
show snmp-server v3 group
```

**Command mode:** All

Sec Model	User Name	Group Name
snmpv1	v1v2only	v1v2grp
usm	adminmd5	admingrp
usm	adminsha	admingrp
usm	adminshaaes	admingrp

**Table 12.** *SNMPv3 Group Table Information Parameters*

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.

## SNMPv3 Community Table Information

This command displays the community table information stored in the SNMP engine. The following command displays SNMPv3 community information:

```
show snmp-server v3 community
```

**Command mode:** All

Index	Name	User Name	Tag
trap1	public	v1v2only	v1v2trap

**Table 13.** *SNMPv3 Community Table Information Parameters*

Field	Description
Index	Displays the unique index value of a row in this table.
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.



## SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

```
show snmp-server v3 target-address
```

**Command mode:** All

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

Name	Transport Addr	Port	Taglist	Params
trap1	47.81.25.66	162	v1v2trap	v1v2param

**Table 14.** *SNMPv3 Target Address Table Information Parameters*

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry.
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

## SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

```
show snmp-server v3 target-parameters
```

**Command mode:** All

Name	MP Model	User Name	Sec Model	Sec Level
v1v2param	snmpv2c	v1v2only	snmpv1	noAuthNoPriv

**Table 15.** *SNMPv3 Target Parameters Table Information*

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this <code>snmpTargetParamsEntry</code> .
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the <code>securityName</code> , which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an <code>inconsistentValue</code> error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

## SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify table:

```
show snmp-server v3 notify
```

Command mode: All

Name	Tag
v1v2trap	v1v2trap

**Table 16.** *SNMPv3 Notify Table Information*

Field	Description
Name	The locally arbitrary, but unique identifier associated with this snmpNotifyEntry.
Tag	This represents a single tag value which is used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected.

## SNMPv3 Dump Information

The following command displays SNMPv3 information:

**show snmp-server v3**

**Command mode:** All

```

usmUser Table:
User Name                               Protocol
-----
adminmd5                                HMAC_MD5, DES PRIVACY
adminsha                                HMAC_SHA, DES PRIVACY
v1v2only                                NO AUTH, NO PRIVACY

vacmAccess Table:
Group Name Prefix Model Level Match ReadV WriteV NotifyV
-----
v1v2grp          snmpv1 noAuthNoPriv exact iso iso v1v2only
admingrp         usm authPriv exact iso iso iso

vacmViewTreeFamily Table:
View Name Subtree Mask Type
-----
iso          1 included
v1v2only    1 included
v1v2only    1.3.6.1.6.3.15 excluded
v1v2only    1.3.6.1.6.3.16 excluded
v1v2only    1.3.6.1.6.3.18 excluded

vacmSecurityToGroup Table:
All active SNMPv3 groups are listed below:
Sec Model User Name Group Name
-----
snmpv1    v1v2only v1v2grp
usm       adminmd5 admingrp
usm       adminsha admingrp

snmpCommunity Table:
Index Name User Name Tag
-----

snmpNotify Table:
Name Tag
-----

snmpTargetAddr Table:
Name Transport Addr Port Taglist Params
-----

snmpTargetParams Table:
Name MP Model User Name Sec Model Sec Level
-----

```

## General System Information

The following command displays system information:

**show sys-info**

**Command mode:** All

```
System Information at 14:26:16 Tue Mar 31, 2015
Time zone: No timezone configured
Daylight Savings Time Status: Disabled

Lenovo Flex System Fabric EN4093R 10Gb Scalable Switch

Switch has been up for 12 days, 1 hour, 48 minutes and 22 seconds.
Last boot: 11:40:13 Thu Mar 19, 2015 (reset by SNMP)

MAC address: 08:17:f4:0a:20:00 IP (If 2) address: 2000:0:0:0:0:0:7
Internal Management Port MAC Address: 08:17:f4:0a:20:ef
Internal Management Port IP Address (if 128): 10.241.37.7
External Management Port MAC Address: 08:17:f4:0a:20:fe
External Management Port IP Address (if 127): 10.241.38.34

Software Version 8.2.1 (FLASH image1), active configuration.
Boot kernel version 8.2.1

Chassis MTM                : 8721A1G
Chassis Serial Num         : 06MBGH0
Hardware Part Number       : 00FM516
Hardware Revision          : 05
Serial Number              : Y010CM28E863
Manufacturing Date (WWYY)  : 3712
PCBA Part Number           : 00D6166
PCBA Revision              : 0
PCBA Number                : 00
Board Revision             : 05
PLD Firmware Version       : 1.7

Temperature Warning        : 34 C (Warning at 66 C / Recover at 61 C)
Temperature Shutdown      : 35 C (Shutdown at 72 C / Recover at 67 C)
Temperature Inlet         : 31 C
Temperature Exhaust       : 36 C
Temperature Asic Max      : 38 C (Warning at 100 C / Shutdown at 108 C)

Power Consumption          : 47.400 W (12.236 V 3.861 A)

Switch is in I/O Module Bay 4
```

**Note:** The display of temperature will come up only if the temperature of any of the sensors exceeds the temperature threshold. There will be a warning from the software if any of the sensors exceeds this temperature threshold. The switch will shut down if the power supply overheats.

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- Software image file and version number, and configuration name.
- IP address of the management interface
- Hardware version and part number
- Log-in banner, if one is configured
- Internal temperatures

## Show Software Version Brief

[Table 17](#) lists commands used for displaying specific entries from the general system information screen.

**Table 17.** *Specific System Information Options*

<b>Command Syntax and Usage</b>
<b>show version brief</b> Displays the software version number, image file, and configuration name. <b>Command mode:</b> All

Sample output for command **show version brief**:

Software Version 8.2.1 (FLASH image2), active configuration.
--

Displays the software version number, image file, and configuration name.

## Show Recent Syslog Messages

The following command displays system log messages:

```
show logging [messages] [severity <0-7>] [reverse]
```

**Command mode:** All

```
Current syslog configuration:
 host 0.0.0.0 via MGT port, severity 7, facility 0
 host2 0.0.0.0 via MGT port, severity2 7, facility2 0
 console enabled
 severity level of console output 6
 severity level of write to flash 7
 syslogging all features
 Syslog source loopback interface not set
```

Date	Time	Criticality level	Message
Jul 8	17:25:41	NOTICE	system: link up on port INT1
Jul 8	17:25:41	NOTICE	system: link up on port INT8
Jul 8	17:25:41	NOTICE	system: link up on port INT7
Jul 8	17:25:41	NOTICE	system: link up on port INT2
Jul 8	17:25:41	NOTICE	system: link up on port INT1
Jul 8	17:25:41	NOTICE	system: link up on port INT4
Jul 8	17:25:41	NOTICE	system: link up on port INT3
Jul 8	17:25:41	NOTICE	system: link up on port INT6
Jul 8	17:25:41	NOTICE	system: link up on port INT5
Jul 8	17:25:41	NOTICE	system: link up on port EXT4
Jul 8	17:25:41	NOTICE	system: link up on port EXT1
Jul 8	17:25:41	NOTICE	system: link up on port EXT3
Jul 8	17:25:41	NOTICE	system: link up on port EXT2
Jul 8	17:25:41	NOTICE	system: link up on port INT3
Jul 8	17:25:42	NOTICE	system: link up on port INT2
Jul 8	17:25:42	NOTICE	system: link up on port INT4
Jul 8	17:25:42	NOTICE	system: link up on port INT3
Jul 8	17:25:42	NOTICE	system: link up on port INT6

Each syslog message has a severity level associated with it, included in text form as a prefix to the log message. One of eight different prefixes is used, depending on the condition for which the administrator is being notified.

- EMERG Indicates the system is unusable
- ALERT Indicates action should be taken immediately
- CRIT Indicates critical conditions
- ERR Indicates error conditions or errored operations
- WARNING Indicates warning conditions
- NOTICE Indicates a normal but significant condition
- INFO Indicates an information message
- DEBUG Indicates a debug-level message

The **severity** option filters only syslog messages with a specific severity level between 0 and 7, from EMERG to DEBUG correspondingly.

The **reverse** option displays the output in reverse order, from the newest entry to the oldest.

## Show Security Audit Log Messages

The following commands display security audit log messages:

**Table 18.** Security Audit Log Information Commands

Command Syntax and Usage
<p><b>show sal [reverse]</b></p> <p>Displays the most recent security audit log messages. The <code>reverse</code> option displays the output in reverse order, from the newest entry to the oldest.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>show sal sequence</b> &lt;sequence number or range&gt;</p> <p>Displays the security audit log messages associated with the specified sequence number or range.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>show sal severity</b> &lt;1-6&gt; [reverse]</p> <p>Displays only the security audit log messages with a specific severity level between 1 and 6, from FATAL to INFORMATION correspondingly. The <code>reverse</code> option displays the output in reverse order, from the newest entry to the oldest.</p> <p><b>Command mode:</b> All except User EXEC</p>

**Note:** Security Audit Log commands are not available in Stacking mode.

Command sample output for `show sal`:

<pre>2014 Jul 16 12:40:39 2000:30:0:0:0:2:95 000004DC 0x00000004 Warning 1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP: New Management IP Address 10.30.2.95 configured</pre>
<pre>2014 Jul 16 12:40:39 2000:30:0:0:0:2:95 000004DD 0x00000004 Warning 1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP: New Management Gateway 10.30.1.1 configured</pre>
<pre>2014 Jul 16 12:42:40 2000:30:0:0:0:2:95 000004DE 0x00000004 Warning 1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP: New Management IP Address 10.30.2.95 configured</pre>
<pre>2014 Jul 16 12:42:40 2000:30:0:0:0:2:95 000004DF 0x00000004 Warning 1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP: New Management Gateway 10.30.1.1 configured</pre>

Each security audit log message has a severity level associated with it, included in text form as a prefix to the log message. One of six different prefixes is used, depending on the condition for which the administrator is being notified.

- FATAL Indicates the system is unusable
- CRITICAL Indicates critical conditions
- MAJOR Indicates action should be taken immediately
- MINOR Indicates error conditions or errored operations
- WARNING Indicates warning conditions
- INFORMATION Indicates an information message



## User Status

The following command displays user status information:

**show access user**

**Command mode:** All except User EXEC

```
Username:
user    - disabled - offline
oper    - disabled - offline
admin   - enabled  - online    1 session.
Current User ID table:
1: name USERID , ena, cos admin , password valid, offline

Current strong password settings:
strong password status: disabled
```

This command displays the status of the configured usernames.

## LDAP Information

The following command displays LDAP server configuration information, for LDAP configured in LIOM mode:

### **show ldap-server**

**Command mode:** All except User EXEC

```
Current LDAP settings:
Primary LDAP Server (null) via MGT port
Secondary LDAP Server (null) via MGT port
Current LDAP server (null)
LDAP port 389, Retries 3, Timeout 5, LDAP server OFF, Backdoor access
disabled
LDAP domain name
LDAP user attribute uid
```

For LDAP configured in SIOM mode in CMM tool, use the following command to display LDAP server configuration information:

### **show ldap-server siom-configure**

**Command mode:** All except User EXEC

```
LDAP VPD DATA:
LDAP Search Order:                                LOCAL ONLY

CMM Bind Method: Login prompt
CMM Root DN: dc=ibmbase,dc=com
CMM Client DN:
CMM Client Password is empty.
CMM Connect type:                                LDAPS

CMM user attribute name: uid
CMM group attribute name: memberOf
CMM permission attribute name: ibm-chassisRole
CMM Server IP Address: fe80::211:25ff:fec3:e4b0:636
External Bind Method: Login prompt
External Root DN:
External Client DN:
External Client Password:
External Connect type:                            clear text

External user attribute name:
External group attribute name: memberOf
External permission attribute name: ibmChassisRole
External Server 1 IP Address: :0
External Server 2 IP Address: :0
External Server 3 IP Address: :0
External Server 4 IP Address: :0
AOM Mode: Disabled
SIOM Mode enabled
```

---

## Stacking Information

Table 19 lists the Stacking information options.

**Table 19.** *Stacking Information Commands*

Command Syntax and Usage
<p><b>show sys-info swn</b> &lt;attached switch number (1-16)&gt;</p> <p>Displays system information for the specified attached switch, including:</p> <ul style="list-style-type: none"><li>o System date and time</li><li>o Switch model name and number</li><li>o Switch name and location</li><li>o Time of last boot</li><li>o MAC address of the switch management processor</li><li>o IP address of management interface</li><li>o Hardware version and part number</li><li>o Software image file and version number</li><li>o Configuration name</li><li>o Log-in banner, if one is configured</li><li>o Internal temperatures</li><li>o Fan status</li><li>o Power supply status</li></ul> <p><b>Note:</b> This command is available only on the master switch.</p> <p><b>Command mode:</b> All</p>
<p><b>show processes [cpu memory thread] swn</b> &lt;attached switch number (1-8)&gt;</p> <p>Displays process information for the specified attached switch, including:</p> <ul style="list-style-type: none"><li>o CPU usage</li><li>o memory usage</li><li>o thread statistics</li></ul>
<p><b>show stack switch</b></p> <p>Displays information about each switch in the stack, including:</p> <ul style="list-style-type: none"><li>o Configured Switch Number (csnum)</li><li>o Attached Switch Number (asnum) when run on master switch</li><li>o MAC address</li><li>o Stacking state</li><li>o UUID</li><li>o Bay number</li></ul> <p><b>Command mode:</b> All</p>

**Table 19.** *Stacking Information Commands*

<b>Command Syntax and Usage</b>
<b>show stack attached-switches</b> Displays information about each attached switch in the stack. Available only on the master switch. <b>Command mode:</b> All
<b>show stack link</b> Displays link information for each switch in the stack, listed by attached switch number. <b>Command mode:</b> All
<b>show stack name</b> Displays the name of the stack. <b>Command mode:</b> All
<b>show stack backup</b> Displays the csnum (configured switch number) of the backup switch. <b>Command mode:</b> All
<b>show stack version</b> Displays the firmware version number for all attached switches. <b>Command mode:</b> All
<b>show stack path-map [csnum &lt;1-8&gt;]</b> Displays the path used to send known unicast packets from one switch of the stack to another. <b>Command mode:</b> All
<b>show stack push-status</b> Displays the status of the most recent firmware and configuration file push from the master to member switches. <b>Command mode:</b> All
<b>show stack dynamic</b> Displays all stacking information. <b>Command mode:</b> All

## Stacking Switch Information

The following command displays Stacking switch information:

**show stack switch**

**Command mode:** All

```
Stack name: STK
Local switch is the master.

Local switch:
  csnum           - 1
  MAC             - 74:99:75:21:8d:00
  UUID           - 534c8ca1605846299148305adc9a1f6d
  Bay Number     - 1
  Switch Type    - 14
  Chassis Type   - 6 (Flex Enterprise)
  Switch Mode (cfg) - Master
  Priority       - 250
  Stack MAC     - 74:99:75:21:8d:1f

Master switch:
  csnum           - 1
  MAC             - 74:99:75:21:8d:00
  UUID           - 534c8ca1605846299148305adc9a1f6d
  Bay Number     - 1

Backup switch:
  csnum           - 5
  MAC             - 74:99:75:21:8c:00
  UUID           - 98c587636548429aba5010f8c62d4e27
  Bay Number     - 1

Configured Switches:
-----
csnum           UUID                               Bay      MAC                               asnum
-----
C1  534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  A1
C2  534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  A3
C3  534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  A2
C4  534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  A4
C5  98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  A5

Attached Switches in Stack:
-----
asnum           UUID                               Bay      MAC                               csnum  State
-----
A1  534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  C1  IN_STACK
A2  534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  C3  IN_STACK
A3  534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  C2  IN_STACK
A4  534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  C4  IN_STACK
A5  98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  C5  IN_STACK
```

Stack switch information includes the following:

- Stack name
- Details about the local switch from which the command was issued
- Configured switch number and MAC of the Stack Master and Stack Backup
- Configured switch numbers and their associated assigned switch numbers
- Attached switch numbers and their associated configured switch numbers

## Attached Switches Information

The following command displays information about attached switches, when run on master switch:

**show stack attached-switches**

**Command mode:** All

Attached Switches in Stack						
asnum	UUID	Bay	MAC	cnum	State	
A1	534c8ca1605846299148305adc9a1f6d	1	74:99:75:21:8d:00	C1	IN_STACK	
A2	534c8ca1605846299148305adc9a1f6d	3	08:17:f4:0a:2d:00	C3	IN_STACK	
A3	534c8ca1605846299148305adc9a1f6d	2	08:17:f4:84:34:00	C2	IN_STACK	
A4	534c8ca1605846299148305adc9a1f6d	4	74:99:75:1c:77:00	C4	IN_STACK	
A5	98c587636548429aba5010f8c62d4e27	1	74:99:75:21:8c:00	C5	IN_STACK	

## Stack Name Information

The following command displays the name of the stack:

**show stack name**

**Command mode:** All

```
Stack name: STK
```

## Stack Backup Switch Information

The following command displays the cnum (configured switch number) for the backup switch:

**show stack backup**

**Command mode:** All

```
Current config Backup unit number = 5
```

## Stack Version Information

The following command displays firmware version information for each switch in the stack:

**show stack version**

**Command mode:** All

Switch Firmware Versions:						
asnum	csnum	MAC	S/W	Version	Serial #	
A1	C1	74:99:75:21:8d:00	image1	8.3.7.49	Y250CM28Y653	
A2	C2	34:40:b5:73:8a:00	image1	8.3.7.49	Y010CM223620	
A3	C4	34:40:b5:77:65:00	image1	8.3.7.49	Y250VT21X302	
A4	C5	74:99:75:1c:68:00	image1	8.3.7.49	Y010CM28E870	
A5	C3	74:99:75:21:8c:00	image1	8.3.7.49	Y250CM28Y639	
A6	C6	08:17:f4:5f:39:00	image1	8.3.7.49	Y010CM003E00	

## Stack Packet Path Information

The following command displays information about the path used to send known unicast packets between the switches of a stack.

**show stack path-map**

**Command mode:** All

Packet path Information:									
To->	Swu 1	Swu 2	Swu 3	Swu 4	Swu 5	Swu 6	Swu 7	Swu 8	
Swu 1	0	1:45	1:45	1:49	1:49	0	0	0	
Swu 2	2:61	0	2:61	2:57	2:57	0	0	0	
Swu 3	3:57	3:61	0	3:57	3:61	0	0	0	
Swu 4	4:57	4:61	4:57	0	4:61	0	0	0	
Swu 5	5:45	5:49	5:49	5:45	0	0	0	0	
Swu 6	0	0	0	0	0	0	0	0	
Swu 7	0	0	0	0	0	0	0	0	
Swu 8	0	0	0	0	0	0	0	0	

## Stack Push Status Information

The following command displays the status of the most recent firmware and configuration file push from the master to member switches:

### **show stack push-status**

**Command mode:** All

```
Image 1 transfer status info:
  Switch 08:17:f4:0a:2d:00:
    not received - file not sent or transfer in progress
  Switch 08:17:f4:84:34:00:
    not received - file not sent or transfer in progress
  Switch 74:99:75:1c:77:00:
    not received - file not sent or transfer in progress
  Switch 74:99:75:21:8c:00:
    not received - file not sent or transfer in progress

Image 2 transfer status info:
  Switch 08:17:f4:0a:2d:00:
    not received - file not sent or transfer in progress
  Switch 08:17:f4:84:34:00:
    not received - file not sent or transfer in progress
  Switch 74:99:75:1c:77:00:
    not received - file not sent or transfer in progress
  Switch 74:99:75:21:8c:00:
    not received - file not sent or transfer in progress

Boot image transfer status info:
  Switch 08:17:f4:0a:2d:00:
    not received - file not sent or transfer in progress
  Switch 08:17:f4:84:34:00:
    not received - file not sent or transfer in progress
  Switch 74:99:75:1c:77:00:
    not received - file not sent or transfer in progress
  Switch 74:99:75:21:8c:00:
    not received - file not sent or transfer in progress

Config file transfer status info:
  Switch 08:17:f4:0a:2d:00:
    last receive successful
  Switch 08:17:f4:84:34:00:
    last receive successful
  Switch 74:99:75:1c:77:00:
    last receive successful
  Switch 74:99:75:21:8c:00:
    last receive successful
```



---

## Layer 2 Information

The following commands display Layer 2 information.

**Table 20.** *Layer 2 Information Commands*

Command Syntax and Usage
<p><b>show dot1x information</b></p> <p>Displays 802.1X Information. For details, see <a href="#">page 75</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show spanning-tree</b></p> <p>Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership.</p> <p>In addition to seeing if spanning tree groups (STGs) are enabled or disabled, you can view the following STG bridge information:</p> <ul style="list-style-type: none"><li>o Priority</li><li>o Hello interval</li><li>o Maximum age value</li><li>o Forwarding delay</li><li>o Aging time</li></ul> <p>You can also see the following port-specific STG information:</p> <ul style="list-style-type: none"><li>o Port alias and priority</li><li>o Cost</li><li>o State</li></ul> <p>For details, see <a href="#">page 77</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show spanning-tree stp &lt;STP instance or range&gt; information</b></p> <p>Displays information about a specific Spanning Tree Group. For details, see <a href="#">page 82</a>.</p> <p><b>Command mode:</b> All</p>

**Table 20.** *Layer 2 Information Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>show spanning-tree mst</b> <i>&lt;MST instance or range&gt;</i> [<b>information</b>]</p> <p>Displays Multiple Spanning Tree Protocol (MSTP) information for the specified instance, including the MSTP digest and VLAN membership. MSTP port information includes:</p> <ul style="list-style-type: none"><li>o Port number and priority</li><li>o Cost</li><li>o State</li><li>o Role</li><li>o Designated bridge and port</li><li>o Type</li></ul> <p>For details, see <a href="#">page 86</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show spanning-tree mst configuration</b></p> <p>Displays the current MSTP settings.</p> <p><b>Command mode:</b> All</p>
<p><b>show portchannel information</b></p> <p>Displays the state of each port in the various Link Aggregation Groups (LAGs). For details, see <a href="#">page 88</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show vlan</b></p> <p>Displays VLAN configuration information for all configured VLANs, including:</p> <ul style="list-style-type: none"><li>o VLAN Number</li><li>o VLAN Name</li><li>o Status</li><li>o Port membership of the VLAN</li></ul> <p>For details, see <a href="#">page 89</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show failover trigger</b> [<i>&lt;trigger number&gt;</i>]<b>information</b></p> <p>Displays Layer 2 Failover information. For details, see <a href="#">page 64</a>.</p> <p><b>Command mode:</b> All</p>

**Table 20.** *Layer 2 Information Commands (continued)*

<b>Command Syntax and Usage</b>
<b>show hotlinks information</b> Displays Hot Links information. For details, see <a href="#">page 66</a> . <b>Command mode:</b> All
<b>show layer2 information</b> Dumps all Layer 2 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. <b>Command mode:</b> All

## FDB Information

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

**Note:** The master forwarding database supports up to 128K MAC address entries on the MP per switch.

**Table 21.** *FDB Information Commands*

Command Syntax and Usage
<p><b>show mac-address-table</b></p> <p>Displays all entries in the Forwarding Database.</p> <p><b>Command mode:</b> All</p> <p>For more information, see <a href="#">page 61</a>.</p>
<p><b>show mac-address-table address</b> &lt;MAC address&gt;</p> <p>Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, xx:xx:xx:xx:xx:xx. For example, 08:00:20:12:34:56.</p> <p>You can also enter the MAC address using the format, xxxxxxxxxxxx. For example, 080020123456.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table all</b></p> <p>Displays both unicast (static and dynamic) and multicast (static) entries in the Forwarding Database.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table configured-static</b></p> <p>Displays all configured static MAC entries in the FDB.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table interface port</b> &lt;port alias or number&gt;</p> <p>Displays all FDB entries for a particular port.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table multicast</b></p> <p>Displays all Multicast MAC entries in the FDB.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table portchannel</b> &lt;LAG number&gt;</p> <p>Displays all FDB entries for a particular Link Aggregation Group (LAG).</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table private-vlan</b> &lt;VLAN number&gt;</p> <p>Displays all FDB entries on a single private VLAN.</p> <p><b>Command mode:</b> All</p>

**Table 21.** *FDB Information Commands (continued)*

<b>Command Syntax and Usage</b>
<b>show mac-address-table state {unknown forward trunk}</b> Displays all FDB entries for a particular state. <b>Command mode:</b> All
<b>show mac-address-table static</b> Displays all static MAC entries in the FDB. <b>Command mode:</b> All
<b>show mac-address-table vlan &lt;VLAN number&gt;</b> Displays all FDB entries on a single VLAN. <b>Command mode:</b> All

### Show All FDB Information

The following command displays Forwarding Database information:

**show mac-address-table**

**Command mode:** All

MAC address	VLAN	Port	Trnk	State	Permanent
-----	----	----	----	-----	-----
00:04:38:90:54:18	1	EXT4		FWD	
00:09:6b:9b:01:5f	1	INT13		FWD	
00:09:6b:ca:26:ef	4095	MGT1		FWD	
00:0f:06:ec:3b:00	4095	MGT1		FWD	
00:11:43:c4:79:83	1	EXT4		FWD	P

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the aggregation (TRK) state, the port field represents the Link Aggregation Group (LAG) number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address.

When an address is in the unknown state, no outbound port is indicated, although ports that reference the address as a destination will be listed under "Reference ports".

## Show FDB Multicast Address Information

The following commands display Multicast Forwarding Database information:

**Table 22.** Multicast FDB Information Commands

Command Syntax and Usage
<b>show mac-address-table multicast</b> Displays all Multicast MAC entries in the FDB. <b>Command mode:</b> All
<b>show mac-address-table multicast address</b> <MAC address> Displays a single FDB multicast entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, xx:xx:xx:xx:xx:xx. For example, 03:00:20:12:34:56. You can also enter the MAC address using the format, xxxxxxxxxxxx. For example, 030020123456. <b>Command mode:</b> All
<b>show mac-address-table multicast interface port</b> <port alias or number> Displays all FDB multicast entries for a particular port. <b>Command mode:</b> All
<b>show mac-address-table multicast vlan</b> <VLAN number> Displays all FDB multicast entries on a single VLAN. <b>Command mode:</b> All

## Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to [“Forwarding Database Maintenance” on page 649](#).

## Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the EN4093R.

**Table 23.** *LACP Information Commands*

Command Syntax and Usage
<p><b>show lacp aggregator</b> &lt;aggregator ID&gt;</p> <p>Displays detailed information about the LACP aggregator.</p> <p><b>Command mode:</b> All</p>
<p><b>show lacp information</b></p> <p>Displays a summary of LACP information. For details, see <a href="#">page 63</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show interface port</b> &lt;port alias or number&gt; <b>lacp information</b></p> <p>Displays LACP information about the selected port.</p> <p><b>Command mode:</b> All</p>

### Link Aggregation Control Protocol

The following command displays LACP information:

**show lacp information**

**Command mode:** All

port	mode	adminkey	operkey	selected	prio	aggr	trunk	status	minlinks
1	active	1000	1000	individual	32768	--	--	down	1
2	active	2000	2000	suspended	32768	--	--	down	1
3	active	3000	2000	yes	32768	1	65*	up	1
4	active	3000	2000	suspended	32768	--	65*	down	1
...									

(\*) LACP PortChannel is statically bound to the admin key

LACP dump includes the following information for each external port in the EN4093R:

- **mode** Displays the port's LACP mode (active, passive, or off).
- **adminkey** Displays the value of the port's *adminkey*.
- **operkey** Shows the value of the port's operational key.
- **selected** Indicates whether the port has been selected to be part of a Link Aggregation Group (LAG).
- **prio** Shows the value of the port priority.
- **aggr** Displays the aggregator associated with each port.
- **trunk** This value represents the LACP LAG number.
- **status** Displays the status of LACP on the port (up, down or standby).
- **minlinks** Displays the minimum number of active links in the LACP LAG.

## Layer 2 Failover Information Commands

The following command displays Layer 2 Failover information:

**Table 24.** *Layer 2 Failover Information Commands*

Command Syntax and Usage
<b>show failover trigger</b> <trigger number> [ <b>information</b> ] Displays detailed information about the selected Layer 2 Failover trigger. <b>Command mode:</b> All
<b>show failover trigger</b> [ <b>information</b> ] Displays a summary of Layer 2 Failover information. For details, see <a href="#">page 64</a> . <b>Command mode:</b> All

### *Layer 2 Failover Information*

The following command displays Layer 2 Failover information:

**show failover trigger**

**Command mode:** All

```
trunk 1
  EXT2      Operational
  EXT3      Operational

Control State: Auto Disabled
Member      Status
-----
  INT1      Operational
  INT2      Operational
  INT3      Operational
  INT4      Operational

Trigger 2 Manual Monitor: Enabled
Trigger 2 limit: 0
Monitor State: Down
Member      Status
-----
adminkey 62
  EXT20     Failed
Control State: Auto Disabled
Member      Status
-----

Physical ports
  INTC1     Failed
Virtual ports
  INTB1.2   Failed
  INTB2.2   Failed
  INTB3.2   Failed
  INTB4.2   Failed
  INTB5.2   Failed
...
```



A monitor port's Failover status is **Operational** only if all the following conditions hold true:

- Port link is up.
- If Spanning-Tree is enabled, the port is in the **Forwarding** state.
- If the port is a member of an LACP Link Aggregation Group (LAG), the port is aggregated.

If any of these conditions are not true, the monitor port is considered to be failed.

A control port is considered to be operational if the monitor trigger state is **Up**. Even if a port's link status is **Down**, Spanning-Tree status is **Blocking**, and the LACP status is **Not Aggregated**, from a teaming perspective the port status is **Operational**, since the trigger is **Up**.

A control port's status is displayed as **Failed** when the monitor trigger state is **Down** or when the controlled port is a vPort which is not properly configured (UFP feature is not enabled in switch, port is not configured as a UFP port, vport is not enabled or physical port is not enabled).

## Hot Links Information

The following command displays Hot Links information:

**show hotlinks information**

**Command mode:** All

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
Hot Links BPDU flood: disabled
Hot Links FDB update: disabled
FDB update rate (pps): 500

Current Trigger 12 setting: enabled
name "TG-12", preempt enabled, fdelay 30 sec

Active state: None

Master settings:
    port EXT2
Backup settings:
    port EXT3
```

Hot Links information includes the following:

- Hot Links status (on or off)
- Status of BPDU flood option
- Status of FDB send option
- Status and configuration of each Hot Links trigger

## Edge Control Protocol Information

The following commands display Edge Control Protocol (ECP) information.

**Table 25.** *ECP Information Options*

<b>Command Syntax and Usage</b>
<b>show ecp channels</b> Displays all Edge Control Protocol (ECP) channels. <b>Command mode:</b> All
<b>show ecp retransmit-interval</b> Displays Edge Control Protocol (ECP) retransmit interval. <b>Command mode:</b> All
<b>show ecp upper-layer-protocols</b> Displays all registered Upper-Level Protocols (ULPs). <b>Command mode:</b> All

## LLDP Information

The following commands display LLDP information.

**Table 26.** *LLDP Information Commands*

Command Syntax and Usage
<b>show lldp [information]</b> Displays LLDP information. <b>Command mode:</b> All
<b>show lldp port [&lt;port number or range&gt;]</b> Displays Link Layer Discovery Protocol (LLDP) port information. <b>Command mode:</b> All
<b>show lldp port &lt;1-16&gt; tlv evb</b> Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information. <b>Command mode:</b> All
<b>show lldp port &lt;1-16&gt; vport &lt;1-4&gt; tlv evb</b> Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information for the specific virtual port. <b>Command mode:</b> All
<b>show lldp receive</b> Displays information about the LLDP receive state machine. <b>Command mode:</b> All
<b>show lldp remote-device [&lt;1-256&gt; detail]  port [&lt;port number or range&gt;]]</b> Displays information received from LLDP-capable devices. To view a sample display, see <a href="#">page 69</a> . <b>Command mode:</b> All
<b>show lldp transmit</b> Displays information about the LLDP transmit state machine. <b>Command mode:</b> All

## LLDP Remote Device Information

The following command displays LLDP remote device information:

```
show lldp remote-device [<1-256>|detail|port [<port number>]]
```

Command mode: All

```
LLDP Remote Devices Information
Legend(possible values in DMAC column) :
NB   - Nearest Bridge           - 01-80-C2-00-00-0E
NnTB - Nearest non-TPMR Bridge - 01-80-C2-00-00-03
NCB  - Nearest Customer Bridge - 01-80-C2-00-00-00
Total number of current entries: 1

LocalPort|Index|Remote Chassis ID|Remote Port|Remote System Name|DMAC
-----|-----|-----|-----|-----|-----
EXTM     | 1   |74 99 75 df 88 00|2         |G8052-11         |NB
```

LLDP remote device information provides a summary of information about remote devices connected to the switch. To view detailed information about a device, as shown below, follow the command with the index number of the remote device. To view detailed information about all devices, use the `detail` option.

```
Local Port Alias: EXT1
Remote Device Index      : 15
Remote Device TTL       : 99
Remote Device RxChanges : false
Chassis Type            : Mac Address
Chassis Id              : 00-18-b1-33-1d-00
Port Type               : Locally Assigned
Port Id                 : 23
Port Description        : EXT1

System Name             :
System Description     : Lenovo Networking Operating System
RackSwitch G8264, Lenovo Networking OS: version 7.8.0.24,
Boot image: version 7.8.0.24

System Capabilities Supported : bridge, router
System Capabilities Enabled   : bridge, router

Remote Management Address:
Subtype                    : IPV4
Address                     : 10.100.120.181
Interface Subtype          : ifIndex
Interface Number           : 128
Object Identifier          :
```

## Unidirectional Link Detection Information

The following commands show unidirectional link detection information.

**Table 27.** *UDLD Information Commands*

Command Syntax and Usage
<b>show interface port</b> <port alias or number> <b>udld</b> Displays UDLD information about the selected port. <b>Command mode:</b> All
<b>show udld</b> Displays all UDLD information. <b>Command mode:</b> All

### UDLD Port Information

The following command displays UDLD information for the selected port:

**show interface port** <port alias or number> **udld**

Command mode: All

```
UDLD information on port EXT1
Port enable administrative configuration setting: Enabled
Port administrative mode: normal
Port enable operational state: link up
Port operational state: advertisement
Port bidirectional status: bidirectional
Message interval: 15
Time out interval: 5
Neighbor cache: 1 neighbor detected

Entry #1
Expiration time: 31 seconds
Device Name:
Device ID: 00:da:c0:00:04:00
Port ID: EXT1
```

UDLD information includes the following:

- Status (enabled or disabled)
- Mode (normal or aggressive)
- Port state (link up or link down)
- Bi-directional status (unknown, unidirectional, bidirectional, TX-RX loop, neighbor mismatch)

## OAM Discovery Information

The following commands display OAM Discovery information.

**Table 28.** *OAM Discovery Information Commands*

Command Syntax and Usage
<b>show interface port</b> <port alias or number> <b>oam</b> Displays OAM information about the selected port. <b>Command mode:</b> All
<b>show oam</b> Displays all OAM information. <b>Command mode:</b> All

## OAM Port Information

The following command displays OAM information for the selected port:

**show interface port** <port alias or number> **oam**

Command mode: All

```
OAM information on port EXT1
State enabled
Mode active
Link up
Satisfied Yes
Evaluating No

Remote port information:
Mode active
MAC address 00:da:c0:00:04:00
Stable Yes
State valid Yes
Evaluating No
```

OAM port display shows information about the selected port and the peer to which the link is connected.

## vLAG Information

The following table lists the information commands for Virtual Link Aggregation Group (vLAG) protocol.

**Table 29.** *vLAG Information Options*

Command Syntax and Usage
<b>show vlag adminkey</b> <1-65535> Displays vLAG LACP information. <b>Command mode:</b> All
<b>show vlag peer-gateway</b> Displays the current state of the vLAG peer gateway. For details, see <a href="#">page 73</a> . <b>Command mode:</b> All
<b>show vlag portchannel</b> <LAG number> Displays vLAG static Link Aggregation Group (LAG) information. <b>Command mode:</b> All
<b>show vlag isl</b> Displays vLAG Inter-Switch Link (ISL) information. <b>Command mode:</b> All
<b>show vlag information</b> Displays all vLAG information. <b>Command mode:</b> All
<b>show vlag vrrp</b> Displays current vLAG related VRRP information. <b>Command mode:</b> All

### *vLAG Aggregation Information*

The following command displays vLAG information for the Link Aggregation Group (LAG):

**show vlag portchannel** <LAG number>

**Command mode:** All

vLAG is enabled on trunk 3 Protocol - Static Current settings: enabled ports: 60 Current L2 trunk hash settings: smac Current L3 trunk hash settings: sip dip Current ingress port hash: disabled Current L4 port hash: disabled
---



## *vLAG Peer Gateway Information*

The following command displays the current state of the vLAG peer gateway.

**show vlag peer-gateway**

**Command mode:** All

```
Current peer gateway state: disabled
```

## *vLAG VRRP Information*

The following command displays vLAG related VRRP information:

**show vlag vrrp**

**Command mode:** All

```
vLAG VRRP mode: Active
vLAG related VRRP information:
  1: vrid  1, local role master, peer role backup
 10: vrid  1, local role backup, peer role backup
100: vrid  1, local role backup, peer role master
```

```
vLAG VRRP mode: Passive
vLAG related VRRP information:
  1: vrid  1, local role master, peer role init
 10: vrid  1, local role backup, peer role init
100: vrid  1, local role backup, peer role init
```

## 802.1X Information

The following command displays 802.1X information:

**show dot1x information**

**Command mode:** All

```

System capability : Authenticator
System status    : disabled
Protocol version : 1
Guest VLAN status : disabled
Guest VLAN      : none

```

Port	Auth Mode	Auth Status	Authenticator PAE State	Backend Auth State	Assigned VLAN
*INT1	force-auth	unauthorized	initialize	initialize	none
*INT2	force-auth	unauthorized	initialize	initialize	none
INT3	force-auth	unauthorized	initialize	initialize	none
*INT4	force-auth	unauthorized	initialize	initialize	none
*INT5	force-auth	unauthorized	initialize	initialize	none
*INT6	force-auth	unauthorized	initialize	initialize	none
*INT7	force-auth	unauthorized	initialize	initialize	none
INT8	force-auth	unauthorized	initialize	initialize	none
INT9	force-auth	unauthorized	initialize	initialize	none
*INT10	force-auth	unauthorized	initialize	initialize	none
*INT11	force-auth	unauthorized	initialize	initialize	none
*INT12	force-auth	unauthorized	initialize	initialize	none
EXT1	force-auth	unauthorized	initialize	initialize	none
EXT2	force-auth	unauthorized	initialize	initialize	none
*EXT3	force-auth	unauthorized	initialize	initialize	none
*EXT4	force-auth	unauthorized	initialize	initialize	none
*EXT11	force-auth	unauthorized	initialize	initialize	none

\* - Port down or disabled

**Note:** The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Lenovo Switch that you are using and the firmware versions and options that are installed.

The following table describes the IEEE 802.1X parameters.

**Table 30.** 802.1X Parameter Descriptions

Parameter	Description
Port	Displays each port's alias.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: <ul style="list-style-type: none"> <li>o force-unauth</li> <li>o auto</li> <li>o force-auth</li> </ul>
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.

**Table 30.** 802.1X Parameter Descriptions (continued)

Parameter	Description
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: <ul style="list-style-type: none"><li>o initialize</li><li>o disconnected</li><li>o connecting</li><li>o authenticating</li><li>o authenticated</li><li>o aborting</li><li>o held</li><li>o forceAuth</li></ul>
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: <ul style="list-style-type: none"><li>o initialize</li><li>o request</li><li>o response</li><li>o success</li><li>o fail</li><li>o timeout</li><li>o idle</li></ul>

## Spanning Tree Information

The following command displays Spanning Tree information:

**show spanning-tree**

**Command mode:** All

**Note:** Based on the Spanning Tree mode enabled, the command output differs:

- VLAN Rapid Spanning Tree mode (pvrst):

```

Max PVRST Instances: 256
Pvst+ compatibility mode enabled
-----
Spanning Tree Group 2: On (PVRST)
VLANs: 4000

Current Root:          Path-Cost  Port  Hello  MaxAge  FwdDel
8002 74:99:75:bd:b6:00      0      0      2      20      15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging  Topology  Change  Counts
              32770    2      20      15      300           0

      Port  Prio  Cost  State Role Designated Bridge      Des Port Type
-----
EXT13      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8036 P2P
EXT14      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8036 P2P
EXT15      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8036 P2P
EXT16      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8036 P2P
EXT17      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
EXT20      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
EXT21      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
EXT22      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
-----

Spanning Tree Group 32: On (PVRST)
VLANs: 1

Current Root:          Path-Cost  Port  Hello  MaxAge  FwdDel
8020 74:99:75:bd:b6:00      0      0      2      20      15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging  Topology  Change  Counts
              32800    2      20      15      300           0

      Port  Prio  Cost  State Role Designated Bridge      Des Port Type
-----

Note: There is no active STP port in Spanning Tree Group 32.
-----

Spanning Tree Group 128: Off (PVRST), FDB aging timer 300
VLANs: 4095

      Port  Prio  Cost  State Role Designated Bridge      Des Port Type
-----
MGT1          0      0  FWD  *
* = STP turned off for this port.

```

- Rapid Spanning Tree mode (rstp)

```

Max PVRST Instances: 256
Pvst+ compatibility mode enabled

-----
Spanning Tree Group 1: On (RSTP)
VLANs: 1 4000 4095

Current Root:          Path-Cost  Port  Hello  MaxAge  FwdDel
0000 74:99:75:bd:c4:00    990   EXT15   2      20      15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging  Topology  Change Counts
              32768    2      20      15      300    1

      Port  Prio  Cost  State Role Designated Bridge      Des Port Type
-----
EXT13      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8036 P2P
EXT14      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8036 P2P
EXT15      128   990!+ FWD  ROOT 0000-74:99:75:bd:c4:00  8046 P2P
EXT16      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8036 P2P
EXT17      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
EXT20      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
EXT21      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
EXT22      128  4990!+ DISC  DESG 8002-74:99:75:bd:b6:00  8047 P2P
MGT1       0      0  FWD  *
* = STP turned off for this port.
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.

```

• Multiple Spanning Tree mode (mstp)

```

Max PVRST Instances: 256
Pvst+ compatibility mode enabled

Mstp Digest: 0x5e5b21c3e2cb4f144cab50e88b9bdea

Common Internal Spanning Tree:

VLANs MAPPED: 2-3999 4001-4094
VLANs: 4095

Current Root:          Path-Cost  Port  MaxAge  FwdDel
0000 74:99:75:bd:c4:00      0    EXT15    20     15

Cist Regional Root:    Path-Cost
0000 74:99:75:bd:c4:00      990

Parameters:  Priority  MaxAge  FwdDel  Hops
              4096      20      15      20
  Port  Prio  Cost  State Role Designated Bridge  Des Port Hello Type
-----
EXT13   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8056   2  P2P
EXT14   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8056   2  P2P
EXT15   128   990!+ FWD  ROOT 0000-74:99:75:bd:c4:00  8046   2  P2P
EXT16   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8056   2  P2P
EXT17   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   2  P2P
EXT20   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   2  P2P
EXT21   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   2  P2P
EXT22   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   2  P2P
MGT1    0       0    FWD  *
* = STP turned off for this port.
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.

-----
Spanning Tree Group 2: On (MSTP)
VLANs MAPPED: 4000
VLANs: 4000

Current Root:          Path-Cost  Port
8000 74:99:75:bd:b6:00      0      0

Parameters:  Priority  Aging  Topology Change Counts
              32768    300    3
  Port  Prio  Cost  State Role Designated Bridge  Des Port Type
-----
EXT13   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8056   P2P
EXT14   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8056   P2P
EXT15   128   990!+ FWD  ROOT 0000-74:99:75:bd:c4:00  8046   P2P
EXT16   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8056   P2P
EXT17   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   P2P
EXT20   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   P2P
EXT21   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   P2P
EXT22   128   200!+ FWD  DESG 1000-74:99:75:bd:b6:00  8066   P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.

```

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view the following CIST bridge information:

**Table 31.** *CIST Parameter Descriptions*

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding to learning and from learning state to forwarding state.
Hops	The maximum number of bridge hops a packet can traverse before it is dropped. The default value is 20.

The following port-specific CIST information is also displayed:

**Table 32.** *CIST Parameter Descriptions*

Parameter	Description
Prio (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The state field shows the current state of the port. The state field can be either Discarding (DISC), Learning (LRN), or Forwarding (FWD).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Disabled (DSB), Master (MAST), or Unknown (UNK).



**Table 32.** *CIST Parameter Descriptions (continued)*

<b>Parameter</b>	<b>Description</b>
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are <b>AUTO</b> , <b>P2P</b> , or <b>SHARED</b> .

## RSTP/PVRST Information

The following command displays RSTP/PVRST information:

```
show spanning-tree stp <STP instance or range> information
```

**Command mode:** All

```
Spanning Tree Group 1: On (RSTP)
VLANs: 1

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
ffff 00:13:0a:4f:7d:d0      0    EXT4    2    20    15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              61440    2      20      15      300

Port  Prio  Cost    State  Role Designated Bridge      Des Port  Type
-----
INT1   0      0      DSB *
INT2   0      0      DSB *
INT3   0      0      FWD *
INT4   0      0      DSB *
INT5   0      0      DSB *
INT6   0      0      DSB *
INT7   0      0      DSB *
INT8   0      0      DSB *
INT9   0      0      DSB *
INT10  0      0      DSB *
INT11  0      0      DSB *
INT12  0      0      DSB *
INT13  0      0      DSB *
INT14  0      0      DSB *
EXT1  128    2000  FWD  DESG 8000-00:11:58:ae:39:00  8011  P2P
EXT2  128    2000  DISC BKUP 8000-00:11:58:ae:39:00  8011  P2P
EXT3  128    2000  FWD  DESG 8000-00:11:58:ae:39:00  8013  P2P
EXT4  128   20000  DISC BKUP 8000-00:11:58:ae:39:00  8013  Shared
...
* = STP turned off for this port.
```

**Note:** The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System unit that you are using and the firmware versions and options that are installed.

You can configure the switch software to use the IEEE 802.1D (2004) Rapid Spanning Tree Protocol (RSTP), Per VLAN Rapid Spanning Tree Protocol (PVRST) or IEEE 802.1Q (2003) Multiple Spanning Tree Protocol (MSTP).

If RSTP/PVRST is turned on, you can view the following bridge information for the Spanning Tree Group:

**Table 33.** *RSTP/PVRST Bridge Parameter Descriptions*

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and the MAC address of the root.
Priority (bridge)	The Bridge Priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The Hello Time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The Maximum Age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding to learning and from learning state to forwarding state.
Aging	The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.

The following port-specific information is also displayed:

**Table 34.** *RSTP/PVRST Port Parameter Descriptions*

Parameter	Description
Prio (port)	The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port Path Cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The State field shows the current state of the port. The State field in RSTP mode can be one of the following: Discarding (DISC), Learning (LRN), Forwarding (FWD), or Disabled (DSB).

**Table 34.** RSTP/PVRST Port Parameter Descriptions (continued)

Parameter	Description
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Disabled (DSB).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

## Spanning Tree Bridge Information

The following command displays Spanning Tree bridge information:

**show spanning-tree [vlan <VLAN ID>] bridge**

**Command mode:** All

Vlan	Priority	Hello	MaxAge	FwdDel	Protocol
-----	-----	-----	-----	-----	-----
1	61440	2	20	15	PVRST

**Table 35.** Bridge Parameter Descriptions

Parameter	Description
VLANs	VLANs that are part of the Spanning Tree Group.
Priority	The bridge priority parameter controls which bridge on the network will become the STP root bridge. The lower the value, the higher the priority.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding to learning and from learning state to forwarding state.
Protocol	The STP protocol run by the Spanning Tree Group.

## Spanning Tree Root Information

The following command displays information about the root switches in every STP group:

**show spanning-tree root**

**Command mode:** All

Instance	Root ID	Path-Cost	Hello	MaxAge	FwdDel	Root Port
1	8001 08:17:f4:32:95:00	0	2	20	15	0
3	8003 08:17:f4:32:95:00	0	2	20	15	0
6	8001 08:17:f4:fb:d8:00	20000	2	20	15	27
17	8011 08:17:f4:32:95:00	0	2	20	15	0

**Table 36.** Bridge Parameter Descriptions

Parameter	Description
Instance	Spanning Tree instance
Root ID	Indicates the root switch MAC address and port number.
Path-Cost	The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding to learning and from learning state to forwarding state.
Root Port	Port number allocated to the STP instance on the root switch.

## Multiple Spanning Tree Information

The following command displays Multiple Spanning Tree (MSTP) information:

**show spanning-tree mst <MST instance or range> information**

**Command mode:** All

```
Mstp Digest: 0x5e5b21c3e2cb4f144cab50e88b9bdea
-----
Spanning Tree Group 2: On (MSTP)
VLANs MAPPED: 4000
VLANs: 4000

Current Root:          Path-Cost  Port
8000 74:99:75:bd:b6:00      0      0

Parameters: Priority Aging Topology Change Counts
              32768    300              3

   Port   Prio   Cost   State Role Designated Bridge      Des Port Type
-----
EXT13    128    200!+ FWD   DESG 1000-74:99:75:bd:b6:00    8056 P2P
EXT14    128    200!+ FWD   DESG 1000-74:99:75:bd:b6:00    8056 P2P
EXT15    128    990!+ FWD   ROOT 0000-74:99:75:bd:c4:00    8046 P2P
EXT16    128    200!+ FWD   DESG 1000-74:99:75:bd:b6:00    8056 P2P
EXT17    128    200!+ FWD   DESG 1000-74:99:75:bd:b6:00    8066 P2P
EXT20    128    200!+ FWD   DESG 1000-74:99:75:bd:b6:00    8066 P2P
EXT21    128    200!+ FWD   DESG 1000-74:99:75:bd:b6:00    8066 P2P
EXT22    128    200!+ FWD   DESG 1000-74:99:75:bd:b6:00    8066 P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

The following port-specific MSTP information is also displayed:

**Table 37.** MSTP Parameter Descriptions

Parameter	Description
Prio (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The state field shows the current state of the port. The state field can be either Discarding (DISC), Learning (LRN), or Forwarding (FWD).

**Table 37.** *MSTP Parameter Descriptions (continued)*

<b>Parameter</b>	<b>Description</b>
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Disabled (DSB), Master (MAST), or Unknown (UNK).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

## LAG Information

The following command displays Link Aggregation Group (LAG) information:

**show portchannel information**

**Command mode:** All

```
Trunk group 1: Enabled
Protocol - Static
Port state:
  EXT1: STG 1 forwarding
  EXT2: STG 1 forwarding
```

When LAGs are configured, you can view the state of each port in the various LAGs.

**Note:** If Spanning Tree Protocol on any port in the LAG is set to forwarding, the remaining ports in the LAG will also be set to forwarding.



## VLAN Information

The following commands display VLAN information.

**Table 38.** *VLAN Information Commands*

<b>Command Syntax and Usage</b>
<b>show vlan &lt;VLAN number&gt; [information]</b> Displays general VLAN information.
<b>show vlan private-vlan [type]</b> Displays private VLAN information. The <code>type</code> option lists only the VLAN type for each private VLAN: <code>community</code> , <code>isolated</code> or <code>primary</code> . <b>Command mode:</b> All
<b>show vlan information</b> Displays information about all VLANs, including: <ul style="list-style-type: none"><li>○ VLAN number and name</li><li>○ Port membership</li><li>○ VLAN status (enabled or disabled)</li><li>○ Protocol VLAN status</li><li>○ Private VLAN status</li><li>○ Spanning Tree membership</li><li>○ VMAP configuration</li><li>○ Virtual ports</li></ul> <b>Command mode:</b> All
<b>show protocol-vlan &lt;protocol number&gt;</b> Displays protocol VLAN information. <b>Command mode:</b> All

The following command displays VLAN information:

**show vlan** [<VLAN number>]

**Command mode:** All

VLAN	Name	Status	MGT	Ports
1	Default VLAN	ena	dis	INTA1-EXT22
10	VLAN 10	ena	dis	empty
4095	Mgmt VLAN	ena	ena	EXTM MGT1

Primary	Secondary	Type	Ports	vPorts
-----	-----	-----	-----	-----

**Note:** The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Lenovo Switch that you are using and the firmware versions and options that are installed.

This information display includes all configured VLANs and all member ports that have an active link state. Port membership is represented in slot/port format.

VLAN information includes:

- VLAN Number
- VLAN Type
- VLAN Name
- Status
- Management status of the VLAN
- Port membership of the VLAN
- Protocol-based VLAN information
- Private VLAN configuration

---

## Layer 3 Information

The following commands display Layer 3 information.

**Table 39.** *Layer 3 Information Commands*

Command Syntax and Usage
<b>show arp</b> Displays Address Resolution Protocol (ARP) information. For details, see <a href="#">page 97</a> . <b>Command mode:</b> All
<b>show interface ip</b> [ <i>&lt;interface number&gt;</i> ] Displays IPv4 interface information. For details, see <a href="#">page 125</a> . <b>Command mode:</b> All
<b>show ikev2</b> Displays IKEv2 information. For more information options, see <a href="#">page 129</a> . <b>Command mode:</b> All
<b>show ip bgp information</b> [ <i>&lt;IPv4 address&gt;</i> ] [ <i>&lt;IPv4 mask&gt;</i> ] Displays Border Gateway Protocol (BGP) information. For details, see <a href="#">page 101</a> . <b>Command mode:</b> All
<b>show ip dhcp snooping</b> Displays DHCP Snooping information. For details, see <a href="#">page 133</a> . <b>Command mode:</b> All
<b>show ip dns</b> Displays the current Domain Name System settings. <b>Command mode:</b> All
<b>show ip ecmp</b> Displays ECMP static route information. For details, see <a href="#">page 116</a> . <b>Command mode:</b> All
<b>show ip gateway</b> <1-4> Displays the current gateway settings. <b>Command mode:</b> All
<b>show ip igmp</b> Displays IGMP Information. For more IGMP information options, see <a href="#">page 117</a> . <b>Command mode:</b> All

**Table 39.** *Layer 3 Information Commands (continued)*

<b>Command Syntax and Usage</b>
<b>show ip information</b> Displays all IP information. <b>Command mode:</b> All
<b>show ip interface brief</b> Displays IP Information. For details, see <a href="#">page 128</a> . IP information, includes: <ul style="list-style-type: none"><li>o IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.</li><li>o Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status.</li><li>o IP forwarding settings, network filter settings, route map settings.</li></ul> <b>Command mode:</b> All
<b>show ip ospf information</b> Displays OSPF information. For more OSPF information options, see <a href="#">page 102</a> . <b>Command mode:</b> All
<b>show ip pim component [&lt;1-2&gt;]</b> Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see <a href="#">page 134</a> . <b>Command mode:</b> All
<b>show ip rip interface</b> Displays RIP user's configuration. For details, see <a href="#">page 111</a> . <b>Command mode:</b> All
<b>show ip route</b> Displays all routes configured on the switch. For details, see <a href="#">page 95</a> . <b>Command mode:</b> All
<b>show ip slp</b> Displays information about the Service Location Protocol (SLP) configuration. For command options, see <a href="#">page 179</a> . <b>Command mode:</b> All
<b>show ip vrrp information</b> Displays VRRP information. For details, see <a href="#">page 124</a> . <b>Command mode:</b> All
<b>show ipsec manual-policy</b> Displays information about manual key management policy for IP security. For more information options, see <a href="#">page 131</a> . <b>Command mode:</b> All

**Table 39.** Layer 3 Information Commands (continued)

Command Syntax and Usage
<b>show ipv6 gateway6</b> <1,3-4> Displays the current IPv6 default gateway configuration. <b>Command mode:</b> All
<b>show ipv6 interface</b> [<interface number>] Displays IPv6 interface information. For details, see <a href="#">page 126</a> . <b>Command mode:</b> All
<b>show ipv6 mld groups</b> Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see <a href="#">page 122</a> . <b>Command mode:</b> All
<b>show ipv6 neighbors</b> Displays IPv6 Neighbor Discovery cache information. For more information options, see <a href="#">page 114</a> . <b>Command mode:</b> All
<b>show ipv6 ospf information</b> Displays OSPFv3 information. For more OSPFv3 information options, see <a href="#">page 107</a> . <b>Command mode:</b> All
<b>show ipv6 pmtu</b> [<destination IPv6 address>] Displays IPv6 Path MTU information. For details, see <a href="#">page 127</a> . <b>Command mode:</b> All
<b>show ipv6 prefix</b> Displays IPv6 Neighbor Discovery prefix information. For details, see <a href="#">page 115</a> . <b>Command mode:</b> All
<b>show ipv6 route</b> Displays IPv6 routing information. For more information options, see <a href="#">page 112</a> . <b>Command mode:</b> All
<b>show layer3</b> Dumps all Layer 3 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. <b>Command mode:</b> All

## IP Routing Information

Using the commands listed below, you can display all or a portion of the IP routes currently held in the switch.

**Table 40.** *Route Information Commands*

Command Syntax and Usage
<b>show ip route [all]</b> Displays all routes configured in the switch. For more information, see <a href="#">page 95</a> . <b>Command mode:</b> All
<b>show ip route address &lt;IP address&gt;</b> Displays a single route by destination IP address. <b>Command mode:</b> All
<b>show ip route ecmphash</b> Displays the current ECMP hashing mechanism. <b>Command mode:</b> All
<b>show ip route gateway &lt;IP address&gt;</b> Displays routes to a single gateway. <b>Command mode:</b> All
<b>show ip route interface &lt;interface number&gt;</b> Displays routes on a single interface. <b>Command mode:</b> All
<b>show ip route static</b> Displays static routes configured on the switch. <b>Command mode:</b> All
<b>show ip route tag {address bgp broadcast fixed martian multicast ospf rip static}</b> Displays routes of a single tag. For a description of IP routing tags, see <a href="#">Table 42 on page 95</a> . <b>Command mode:</b> All
<b>show ip route type {broadcast direct indirect local martian multicast}</b> Displays routes of a single type. For a description of IP routing types, see <a href="#">Table 41 on page 95</a> . <b>Command mode:</b> All

## Show All IP Route Information

The following command displays IP route information:

**show ip route**

**Command mode:** All

Destination	Mask	Gateway	Type	Tag	Metric	If
* 12.0.0.0	255.0.0.0	11.0.0.1	direct	fixed	128	
* 12.0.0.1	255.255.255.255	11.0.0.1	local	addr	128	
* 12.255.255.255	255.255.255.255	11.255.255.255	broadcast	broadcast	128	
* 12.0.0.0	255.0.0.0	12.0.0.1	direct	fixed	12	
* 12.0.0.1	255.255.255.255	12.0.0.1	local	addr	12	
* 255.255.255.255	255.255.255.255	12.255.255.255	broadcast	broadcast	2	
* 224.0.0.0	224.0.0.0	0.0.0.0	martian	martian		
* 224.0.0.5	255.255.255.255	0.0.0.0	multicast	addr		

The following table describes the Type parameters.

**Table 41.** IP Routing Type Parameters

Parameter	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the Gateway address.
direct	Packets will be delivered to a destination host or subnet attached to the switch.
local	Indicates a route to one of the switch's IP interfaces.
broadcast	Indicates a broadcast route.
martian	The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded.
multicast	Indicates a multicast route.

The following table describes the Tag parameters.

**Table 42.** IP Routing Tag Parameters

Parameter	Description
fixed	The address belongs to a host or subnet attached to the switch.
static	The address is a static route which has been configured on the EN4093R 10Gb Ethernet Scalable Switch.
address	The address belongs to one of the switch's IP interfaces.
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
bgp	The address was learned via Border Gateway Protocol (BGP).

**Table 42.** *IP Routing Tag Parameters (continued)*

<b>Parameter</b>	<b>Description</b>
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.



## ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags (see [Table 44 on page 98](#)), VLAN and port for the address, and port referencing information.

**Table 43.** *ARP Information Commands*

Command Syntax and Usage
<p><b>show [ip] arp [all]</b></p> <p>Displays all ARP entries, including:</p> <ul style="list-style-type: none"><li>o IP address and MAC address of each entry</li><li>o Address status flag (see below)</li><li>o The VLAN and port to which the address belongs</li><li>o The elapsed time (in seconds) since the ARP entry was learned</li></ul> <p>For more information, see <a href="#">page 98</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show [ip] arp find &lt;IP address&gt;</b></p> <p>Displays a single ARP entry by IP address.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip arp inspection</b></p> <p>Displays the current Dynamic ARP Inspection (DAI) configuration settings. For details, see <a href="#">page 99</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show [ip] arp interface port &lt;port alias or number&gt;</b></p> <p>Displays the ARP entries on a single port.</p> <p><b>Command mode:</b> All</p>
<p><b>show [ip] arp reply</b></p> <p>Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.</p> <p><b>Command mode:</b> All</p>
<p><b>show [ip] arp static</b></p> <p>Displays all static ARP entries.</p> <p><b>Command mode:</b> All</p>
<p><b>show [ip] arp vlan &lt;VLAN number&gt;</b></p> <p>Displays the ARP entries on a single VLAN.</p> <p><b>Command mode:</b> All</p>

## Show All ARP Entry Information

The following command displays ARP information:

**show arp**

**Command mode:** All

IP address	Flags	MAC address	VLAN	Age	Port
12.20.1.1		00:15:40:07:20:42	4095	0	INT8
12.20.20.16		00:30:13:e3:44:14	4095	2	INT8
12.20.20.18		00:30:13:e3:44:14	4095	2	INT6
12.20.23.111		00:1f:29:95:f7:e5	4095	6	INT6

The Port field shows the target port of the ARP entry.

The Flags field is interpreted as follows:

**Table 44.** ARP Dump Flag Parameters

Flag	Description
P	Permanent entry created for switch IP interface.
R	Indirect route entry.
U	Unresolved ARP entry. The MAC address has not been learned.

## ARP Address List Information

The following command displays owned ARP address list information:

**show arp reply**

**Command mode:** All

IP address	IP mask	MAC address	VLAN	Pass-Up
205.178.18.66	255.255.255.255	00:70:cf:03:20:04		P
205.178.50.1	255.255.255.255	00:70:cf:03:20:06	1	
205.178.18.64	255.255.255.255	00:70:cf:03:20:05	1	

## Dynamic ARP Inspection Information

The following commands display Dynamic ARP Inspection (DAI) information:

**Table 45.** *Dynamic ARP Inspection Information Options*

Command Syntax and Usage
<b>show ip arp inspection</b> Displays the current DAI configuration settings. <b>Command mode:</b> All
<b>show ip arp inspection interfaces</b> [ <i>&lt;port alias or number&gt;</i> ] Displays the current DAI configuration settings for the selected interfaces. <b>Command mode:</b> All
<b>show ip arp inspection vlan</b> [ <i>&lt;VLAN ID (1-4094)&gt;</i> ] Displays the current DAI configuration settings for the selected VLANs. <b>Command mode:</b> All

**show ip arp inspection interfaces** [*<port alias or number>*]

**Command mode:** All

Interface	Trust State
-----	-----
1	Trusted
2	Trusted
3	Untrusted
4	Untrusted
...	

**show ip arp inspection vlan** [*<VLAN ID (1-4094)>*]

**Command mode:** All

Vlan	Configuration
----	-----
2	Enabled

## BGP Information

The following commands display BGP information.

**Table 46.** *BGP Peer Information Commands*

Command Syntax and Usage
<b>show ip bgp aggregate-address</b> Displays BGP peer routes. See <a href="#">page 101</a> for a sample output. <b>Command mode:</b> All
<b>show ip bgp information</b> Displays the BGP routing table. See <a href="#">page 101</a> for a sample output. <b>Command mode:</b> All
<b>show ip bgp neighbor information</b> Displays BGP peer information. See <a href="#">page 100</a> for a sample output. <b>Command mode:</b> All
<b>show ip bgp neighbor summary</b> Displays peer summary information such as AS, message received, message sent, up/down, state. See <a href="#">page 101</a> for a sample output. <b>Command mode:</b> All

### *BGP Peer information*

Following is an example of the information provided by the following command:

**show ip bgp neighbor information**

**Command mode:** All

<pre>BGP Peer Information:  3: 2.1.1.1          , version 4, TTL 225   Remote AS: 100, Local AS: 100, Link type: IBGP   Remote router ID: 3.3.3.3,   Local router ID: 1.1.201.5   BGP status: idle, Old status: idle   Total received packets: 0, Total sent packets: 0   Received updates: 0, Sent updates: 0   Keepalive: 60, Holdtime: 180, MinAdvTime: 60   LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)   Established state transitions: 1  4: 2.1.1.4          , version 4, TTL 225   Remote AS: 100, Local AS: 100, Link type: IBGP   Remote router ID: 4.4.4.4,   Local router ID: 1.1.201.5   BGP status: idle, Old status: idle   Total received packets: 0, Total sent packets: 0   Received updates: 0, Sent updates: 0   Keepalive: 60, Holdtime: 180, MinAdvTime: 60   LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)   Established state transitions: 1</pre>
--

## BGP Summary Information

Following is an example of the information provided by the following command:

**show ip bgp neighbor summary**

**Command mode:** All

BGP Peer Summary Information:							
Peer	V	AS	MsgRcvd	MsgSent	Up/Down	State	
1: 205.178.23.142	4	142	113	121	00:00:28	established	
2: 205.178.15.148	0	148	0	0	never	connect	

## BGP Aggregation Information

Following is an example of the information provided by the following command:

**show ip bgp aggregate-address**

**Command mode:** All

Current BGP aggregation settings:	
1: addr 4.2.0.0, mask 255.0.0.0, enabled	
2: addr 5.5.0.0, mask 255.255.0.0, enabled	

## Dump BGP Information

Following is an example of the information provided by the following command:

**show ip bgp information [<IPv4 network> <IPv4 mask>]**

**Command mode:** All

Status codes: * valid, > best, i - internal							
Origin codes: i - IGP, e - EGP, ? - incomplete							
Network	Mask	Next Hop	Metr	LcPrf	Wght	Path	
*> 1.1.1.0	255.255.255.0	0.0.0.0			0	?	
*> 10.100.100.0	255.255.255.0	0.0.0.0			0	?	
*> 10.100.120.0	255.255.255.0	0.0.0.0			0	?	

The 13.0.0.0 is filtered out by rrmmap; or, a loop detected.

The IPv4 network and mask options restrict the output to a specific network in the BGP routing table.

## OSPF Information

The following commands display OSPF information.

**Table 47.** *OSPF Information Commands*

Command Syntax and Usage
<b>show ip ospf area</b> <0-2> Displays area information for a particular area index. <b>Command mode:</b> All
<b>show ip ospf area information</b> Displays area information for all areas. <b>Command mode:</b> All
<b>show ip ospf area-virtual-link information</b> Displays information about all the configured virtual links. <b>Command mode:</b> All
<b>show ip ospf general-information</b> Displays general OSPF information. See <a href="#">page 103</a> for a sample output. <b>Command mode:</b> All
<b>show ip ospf information</b> Displays OSPF information. <b>Command mode:</b> All
<b>show ip ospf interface</b> <interface number> Displays OSPF information for a particular IP interface. See <a href="#">page 104</a> for a sample output. <b>Command mode:</b> All
<b>show ip ospf interface loopback</b> <1-5> Displays loopback information for a particular interface. If no parameter is supplied, it displays loopback information for all the interfaces. See <a href="#">page 104</a> for a sample output. <b>Command mode:</b> All
<b>show ip ospf neighbor</b> Displays the status of all the current neighbors. <b>Command mode:</b> All
<b>show ip ospf routes</b> Displays OSPF routing table. See <a href="#">page 109</a> for a sample output. <b>Command mode:</b> All

**Table 47.** *OSPF Information Commands (continued)*

<b>Command Syntax and Usage</b>
<b>show ip ospf summary-range &lt;0-2&gt;</b> Displays the list of summary ranges belonging to non-NSSA areas. <b>Command mode:</b> All
<b>show ip ospf summary-range-nssa &lt;0-2&gt;</b> Displays the list of summary ranges belonging to NSSA areas. <b>Command mode:</b> All

## *OSPF General Information*

The following command displays general OSPF information:

**show ip ospf general-information**

**Command mode:** All

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                                2 are >=INIT state,
                                2 are >=EXCH state,
                                2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa
  Area Id : 0.0.0.0
  Authentication : none
  Import ASExtern : yes
  Number of times SPF ran : 8
  Area Border Router count : 2
  AS Boundary Router count : 0
  LSA count : 5
  LSA Checksum sum : 0x2237B
  Summary : noSummary
```

## OSPF Interface Loopback Information

The following command displays OSPF interface loopback information:

```
show ip ospf interface loopback <interface number>
```

**Command mode:** All

```
Ip Address 5.5.5.5, Area 0.0.0.1, Passive interface, Admin Status UP
Router ID 1.1.1.2, State Loopback, Priority 1
Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
Backup Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
Timer intervals, Hello 10, Dead 40, Wait 40, Retransmit 5, Transit delay 1
Neighbor count is 0 If Events 1, Authentication type none
```

## OSPF Interface Information

The following command displays OSPF interface information:

```
show ip ospf interface <interface number>
```

**Command mode:** All

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
Router ID 10.10.10.1, State DR, Priority 1
Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
Neighbor count is 1 If Events 4, Authentication type none
```

## OSPF Information Route Codes

The following command displays OSPF route information:

```
show ip ospf routes
```

**Command mode:** All

```
Codes: 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
IA 10.10.0.0/16 via 200.1.1.2
IA 40.1.1.0/28 via 20.1.1.2
IA 80.1.1.0/24 via 200.1.1.2
IA 100.1.1.0/24 via 20.1.1.2
IA 140.1.1.0/27 via 20.1.1.2
IA 150.1.1.0/28 via 200.1.1.2
E2 172.18.1.1/32 via 30.1.1.2
E2 172.18.1.2/32 via 30.1.1.2
E2 172.18.1.3/32 via 30.1.1.2
E2 172.18.1.4/32 via 30.1.1.2
E2 172.18.1.5/32 via 30.1.1.2
E2 172.18.1.6/32 via 30.1.1.2
E2 172.18.1.7/32 via 30.1.1.2
E2 172.18.1.8/32 via 30.1.1.2
```



## OSPF Database Information

The following commands display OSPF Database information.

**Table 48.** *OSPF Database Information Commands*

<p><b>Command Syntax and Usage</b></p>
<p><b>show ip ospf database</b></p> <p>Displays all the LSAs.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database advertising-router &lt;router ID&gt;</b></p> <p>Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database asbr-summary [advertising-router &lt;router ID&gt; link-state-id &lt;A.B.C.D&gt; self]</b></p> <p>Displays ASBR summary LSAs. The use of this command is as follows:</p> <ul style="list-style-type: none"> <li>o asbr-summary advertising-router 20.1.1.1 displays ASBR summary LSAs having the advertising router 20.1.1.1.</li> <li>o asbr-summary link-state-id 10.1.1.1 displays ASBR summary LSAs having the link state ID 10.1.1.1.</li> <li>o asbr-summary self displays the self advertised ASBR summary LSAs.</li> <li>o asbr-summary with no parameters displays all the ASBR summary LSAs.</li> </ul> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database database-summary</b></p> <p>Displays the following information about the LS database in a table format:</p> <ul style="list-style-type: none"> <li>o Number of LSAs of each type in each area.</li> <li>o Total number of LSAs for each area.</li> <li>o Total number of LSAs for each LSA type for all areas combined.</li> <li>o Total number of LSAs for all LSA types for all areas combined.</li> </ul> <p>No parameters are required.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database external [advertising-router &lt;router ID&gt; link-state-id &lt;A.B.C.D&gt; self]</b></p> <p>Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database network [advertising-router &lt;router ID&gt; link-state-id &lt;A.B.C.D&gt; self]</b></p> <p>Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database.</p> <p><b>Command mode:</b> All</p>

**Table 48.** *OSPF Database Information Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>show ip ospf database nssa</b></p> <p>Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database router [advertising-router &lt;router ID&gt; link-state-id &lt;A.B.C.D&gt; self]</b></p> <p>Displays the router (type 1) LSAs with detailed information of each field of the LSAs.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database self</b></p> <p>Displays all the self-advertised LSAs. No parameters are required.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip ospf database summary [advertising-router &lt;router ID&gt; link-state-id &lt;A.B.C.D&gt; self]</b></p> <p>Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs.</p> <p><b>Command mode:</b> All</p>

## OSPFv3 Information

The following commands display OSPFv3 information.

**Table 49.** *OSPFv3 Information Options*

Command Syntax and Usage
<b>show ipv6 ospf area</b> <area index (0-2)> Displays the area information. <b>Command mode:</b> All
<b>show ipv6 ospf areas</b> Displays the OSPFv3 Area Table. <b>Command mode:</b> All
<b>show ipv6 ospf area-range information</b> Displays OSPFv3 summary ranges. <b>Command mode:</b> All
<b>show ipv6 ospf area-virtual-link</b> Displays information about all the configured virtual links. <b>Command mode:</b> All
<b>show ipv6 ospf border-routers</b> Displays OSPFv3 routes to an ABR or ASBR. <b>Command mode:</b> All
<b>show ipv6 ospf host</b> Displays OSPFv3 host configuration information. <b>Command mode:</b> All
<b>show ipv6 ospf information</b> Displays all OSPFv3 information. To view a sample display, see <a href="#">page 108</a> . <b>Command mode:</b> All
<b>show ipv6 ospf interface</b> <interface number> Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. To view a sample display, see <a href="#">page 109</a> . <b>Command mode:</b> All
<b>show ipv6 ospf neighbor</b> <nbr router-id (A.B.C.D)> Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors. <b>Command mode:</b> All

**Table 49.** *OSPFv3 Information Options*

<b>Command Syntax and Usage</b>
<b>show ipv6 ospf redist-config</b> Displays OSPFv3 redistribution information to be applied to routes learned from the route table. <b>Command mode:</b> All
<b>show ipv6 ospf request-list</b> <nbr router-id (A.B.C.D)> Displays the OSPFv3 request list. If no router ID is supplied, it displays the information about all the current neighbors. <b>Command mode:</b> All
<b>show ipv6 ospf retrans-list</b> <nbr router-id (A.B.C.D)> Displays the OSPFv3 retransmission list. If no router ID is supplied, it displays the information about all the current neighbors. <b>Command mode:</b> All
<b>show ipv6 ospf routes</b> Displays OSPFv3 routing table. To view a sample display, see <a href="#">page 109</a> . <b>Command mode:</b> All
<b>show ipv6 ospf summary-prefix</b> <area index (0-2)> Displays the OSPFv3 external summary-address configuration information. <b>Command mode:</b> All

## OSPFv3 Information Dump

The following command displays OSPFv3 information:

**show ipv6 ospf information**

**Command mode:** All

Router Id: 1.0.0.1	ABR Type: Standard ABR	
SPF schedule delay: 5 secs	Hold time between two SPF: 10 secs	
Exit Overflow Interval: 0	Ref BW: 100000	Ext Lsdb Limit: none
Trace Value: 0x00008000	As Scope Lsa: 2	Checksum Sum: 0xfe16
Passive Interface: Disable		
Nssa Asbr Default Route Translation: Disable		
Autonomous System Boundary Router		
Redistributing External Routes from connected, metric 10, metric type asExtType1, no tag set		
Number of Areas in this router	1	
	Area	0.0.0.0
Number of interfaces in this area is	1	
Number of Area Scope Lsa:	7	Checksum Sum: 0x28512
Number of Indication Lsa:	0	SPF algorithm executed: 2 times

## OSPFv3 Interface Information

The following command displays OSPFv3 interface information:

**show ipv6 ospf interface**

**Command mode:** All

```
OspfV3 Interface Information
Interface Id: 1      Instance Id: 0      Area Id: 0.0.0.0
Local Address: fe80::222:ff:fe7d:5d00  Router Id: 1.0.0.1
Network Type: BROADCAST  Cost: 1      State: BACKUP

Designated Router Id: 2.0.0.2      local address:
fe80::218:b1ff:fea1:6c01

Backup Designated Router Id: 1.0.0.1      local address:
fe80::222:ff:fe7d:5d00

Transmit Delay: 1 sec  Priority: 1      IfOptions: 0x0
Timer intervals configured:
Hello: 10, Dead: 40, Retransmit: 5
Hello due in 6 sec
Neighbor Count is: 1, Adjacent neighbor count is: 1
Adjacent with neighbor 2.0.0.2
```

## OSPFv3 Routes Information

The following command displays OSPFv3 route information:

**show ipv6 ospf routes**

**Command mode:** All

Dest/ Prefix-Length	NextHop/ IfIndex	Cost	Rt. Type	Area
3ffe::10:0:0:0 /80	fe80::290:69ff fe90:b4bf /vlan1	30	interArea	0.0.0.0
3ffe::20:0:0:0 /80	fe80::290:69ff fe90:b4bf /vlan1	20	interArea	0.0.0.0
3ffe::30:0:0:0 /80	:: /vlan2	10	intraArea	0.0.0.0
3ffe::60:0:0:6 /128	fe80::211:22ff fe33:4426 /vlan2	10	interArea	0.0.0.0

## OSPFv3 Database Information

The following commands display OSPFv3 Database information.

**Table 50.** *OSPFv3 Database Information Options*

Command Syntax and Usage
<b>show ipv6 ospf database [detail hex]</b> Displays all the LSAs. <b>Command mode:</b> All
<b>show ipv6 ospf database as-external [detail hex]</b> Displays AS-External LSAs database information. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All
<b>show ipv6 ospf database inter-prefix [detail hex]</b> Displays Inter-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All
<b>show ipv6 ospf database inter-router [detail hex]</b> Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All
<b>show ipv6 ospf database intra-prefix [detail hex]</b> Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All
<b>show ipv6 ospf database link [detail hex]</b> Displays Link LSAs database information. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All
<b>show ipv6 ospf database network [detail hex]</b> Displays Network LSAs database information. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All
<b>show ipv6 ospf database router [detail hex]</b> Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All
<b>show ipv6 ospf database nssa [detail hex]</b> Displays Type-7 (NSSA) LSA database information. If no parameter is supplied, it displays condensed information. <b>Command mode:</b> All

## Routing Information Protocol

The following commands display Routing Information Protocol (RIP) information.

**Table 51.** *Routing Information Protocol Commands*

Command Syntax and Usage
<b>show ip rip routes</b> Displays RIP routes. For more information, see <a href="#">page 111</a> . <b>Command mode:</b> All
<b>show interface ip &lt;interface number&gt; rip</b> Displays RIP user's configuration. For more information, see <a href="#">page 111</a> . <b>Command mode:</b> All

### *RIP Routes Information*

The following command displays RIP route information:

**show ip rip routes**

**Command mode:** All

```
>> IP Routing#  
  
30.1.1.0/24 directly connected  
3.0.0.0/8 via 30.1.1.11 metric 4  
4.0.0.0/16 via 30.1.1.11 metric 16  
10.0.0.0/8 via 30.1.1.2 metric 3  
20.0.0.0/8 via 30.1.1.2 metric 2
```

This table contains all dynamic routes learned through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain locally configured static routes.

### *RIP Interface Information*

The following command displays RIP user information:

**show ip rip interface <interface number>**

**Command mode:** All

```
RIP USER CONFIGURATION :  
  RIP: ON, update 30  
  RIP on Interface 49 : 101.1.1.10, enabled  
  version 2, listen enabled, supply enabled, default none  
  poison disabled, split horizon enabled, trigg enabled, mcast  
  enabled, metric 1  
  auth none, key none
```

## IPv6 Routing Information

Table 52 describes the IPv6 Routing information options.

**Table 52.** *IPv6 Routing Information Commands*

Command Syntax and Usage
<b>show ipv6 route</b> Displays all IPv6 routing information. For more information, see <a href="#">page 113</a> . <b>Command mode:</b> All
<b>show ipv6 route address</b> <IPv6 address> Displays a single route by destination IP address. <b>Command mode:</b> All
<b>show ipv6 route gateway</b> <default gateway address> Displays routes to a single gateway. <b>Command mode:</b> All
<b>show ipv6 route interface</b> <interface number> Displays routes on a single interface. <b>Command mode:</b> All
<b>show ipv6 route static</b> Displays all static IPv6 routes. <b>Command mode:</b> All
<b>show ipv6 route type</b> {connected static ospf} Displays routes of a single type. <b>Command mode:</b> All
<b>show ipv6 route summary</b> Displays a summary of IPv6 routing information, including inactive routes. <b>Command mode:</b> All



## IPv6 Routing Table

The following command displays IPv6 routing information:

**show ipv6 route**

**Command mode:** All

```
IPv6 Routing Table - 3 entries
Codes : C - Connected, S - Static
        O - OSPF
        D - Data Gateway from RA
        M - Management Gateway, E - Ext-Management Gateway
        N - Management Gateway from RA
        F - Ext-Management Gateway from RA

S  ::/0 [1/20]
   via 2001:2:3:4::1, Interface 2
C  2001:2:3:4::/64 [1/1]
   via ::, Interface 2
C  fe80::20f:6aff:feec:f701/128 [1/1]
   via ::, Interface 2
```

**Note:** The first number inside the brackets represents the metric and the second number represents the preference for the route.

## IPv6 Neighbor Discovery Cache Information

The following commands display IPv6 Neighbor Discovery Cache information.

**Table 53.** *IPv6 Neighbor Discovery Cache Information Commands*

Command Syntax and Usage
<p><b>show ipv6 neighbors</b></p> <p>Shows all IPv6 Neighbor Discovery cache entries. For more information, see <a href="#">page 114</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show ipv6 neighbors find</b> &lt;IPv6 address&gt;</p> <p>Shows a single IPv6 Neighbor Discovery cache entry by IP address.</p> <p><b>Command mode:</b> All</p>
<p><b>show ipv6 neighbors interface port</b> &lt;port alias or number&gt;</p> <p>Shows IPv6 Neighbor Discovery cache entries on a single port.</p> <p><b>Command mode:</b> All</p>
<p><b>show ipv6 neighbors static</b></p> <p>Displays static IPv6 Neighbor Discovery cache entries.</p> <p><b>Command mode:</b> All</p>
<p><b>show ipv6 neighbors vlan</b> &lt;VLAN number&gt;</p> <p>Shows IPv6 Neighbor Discovery cache entries on a single VLAN.</p> <p><b>Command mode:</b> All</p>

### IPv6 Neighbor Discovery Cache Information

The following command displays a summary of IPv6 Neighbor Discovery cache information:

**show ipv6 neighbors**

**Command mode:** All

IPv6 Address	Age	Link-layer Addr	State	IF	VLAN	Port
-----						
2001:2:3:4::1	10	00:50:bf:b7:76:b0	Reachable	2	1	EXT1
fe80::250:bfff:feb7:76b0	0	00:50:bf:b7:76:b0	Stale	2	1	EXT2

## IPv6 Neighbor Discovery Prefix Information

The following command displays a summary of IPv6 Neighbor Discovery prefix information:

**show ipv6 prefix**

**Command mode:** All

```
Codes: A - Address , P - Prefix-Advertisement
       D - Default , N - Not Advertised
       [L] - On-link Flag is set
       [A] - Autonomous Flag is set

AD 10:: 64 [LA] Valid lifetime 2592000 , Preferred lifetime 604800
P 20:: 64 [LA] Valid lifetime 200 , Preferred lifetime 100
```

Neighbor Discovery prefix information includes information about all configured prefixes.

The following command displays IPv6 Neighbor Discovery prefix information for an interface:

**show ipv6 prefix interface** *<interface number>*

**Command mode:** All

## ECMP Static Route Information

The following command displays Equal Cost Multi-Path (ECMP) route information:

**show ip ecmp**

**Command mode:** All

Current ecmp static routes:				
Destination	Mask	Gateway	If	GW Status
10.10.1.1	255.255.255.255	100.10.1.1	1	up
		200.20.2.2	1	down
10.20.2.2	255.255.255.255	10.233.3.3	1	up
10.20.2.2	255.255.255.255	10.234.4.4	1	up
10.20.2.2	255.255.255.255	10.235.5.5	1	up

ECMP route information shows the status of each ECMP route configured on the switch.

## ECMP Hashing Result

The following command displays the status of ECMP hashing on each switch:

**show ip route ecmp hash**

**Command mode:** All

ECMP Hash Mechanism: dipsip
-----------------------------

## IGMP Information

The following commands display IGMP information:

**Table 54.** *IGMP Information Commands*

Command Syntax and Usage
<b>show ip igmp</b> Displays the current IGMP configuration parameters. <b>Command mode:</b> All
<b>show ip igmp filtering</b> Displays current IGMP Filtering parameters. <b>Command mode:</b> All
<b>show ip igmp groups</b> Displays information for all multicast groups. For a command sample output, see <a href="#">page 120</a> . <b>Command mode:</b> All
<b>show ip igmp groups address &lt;IP address&gt;</b> Displays a single IGMP multicast group by its IP address. <b>Command mode:</b> All
<b>show ip igmp groups detail &lt;IP address&gt;</b> Displays details about an IGMP multicast group, including source and timer information. <b>Command mode:</b> All
<b>show ip igmp groups interface port &lt;port alias or number&gt;</b> Displays all IGMP multicast groups on a single port. <b>Command mode:</b> All
<b>show ip igmp groups portchannel &lt;trunk number&gt;</b> Displays all IGMP multicast groups on a single Link Aggregation Group (LAG). <b>Command mode:</b> All
<b>show ip igmp groups vlan &lt;VLAN number&gt;</b> Displays all IGMP multicast groups on a single VLAN. <b>Command mode:</b> All
<b>show ip igmp ipmcgrp</b> Displays information for all IPMC groups. For details, see <a href="#">page 121</a> . <b>Command mode:</b> All
<b>show ip igmp mrouter [information]</b> Displays IGMP Multicast Router information. For details, see <a href="#">page 121</a> . <b>Command mode:</b> All

**Table 54.** IGMP Information Commands (continued)

Command Syntax and Usage
<b>show ip igmp mrouter dynamic</b> Displays IGMP Multicast Router dynamic information. <b>Command mode:</b> All
<b>show ip igmp mrouter interface port</b> <port alias or number> Displays IGMP Multicast Router information the specified interface. <b>Command mode:</b> All
<b>show ip igmp mrouter portchannel</b> <trunk number> Displays IGMP Multicast Router information the specified portchannel. <b>Command mode:</b> All
<b>show ip igmp mrouter static</b> Displays IGMP Multicast Router static information. <b>Command mode:</b> All
<b>show ip igmp mrouter vlan</b> <VLAN number> Displays IGMP Multicast Router information for the specified VLAN. <b>Command mode:</b> All
<b>show ip igmp profile</b> <1-16> Displays information about the current IGMP filter. <b>Command mode:</b> All
<b>show ip igmp querier vlan</b> <VLAN number> Displays IGMP Querier information. For details, see <a href="#">page 119</a> . <b>Command mode:</b> All
<b>show ip igmp snoop</b> Displays IGMP Snooping information. <b>Command mode:</b> All

## IGMP Querier Information

The following command displays IGMP Querier information:

```
show ip igmp querier vlan <VLAN number>
```

**Command mode:** All

```
Current IGMP Querier information:
IGMP Querier information for vlan 1:
Other IGMP querier - none
Switch-querier enabled, current state: Querier
Switch-querier type: Ipv4, address 1.1.1.1,
Switch-querier general query interval: 125 secs,
Switch-querier max-response interval: 100 'tenths of secs',
Switch-querier startup interval: 31 secs, count: 2
Switch-querier robustness: 2
IGMP configured version is v3
IGMP Operating version is v3
```

IGMP Querier information includes:

- VLAN number
- Querier status
  - Other IGMP querier—none
  - IGMP querier present, address: (IP or MAC address)
- Querier election type (IPv4 or MAC) and address
- Query interval
- Querier startup interval
- Maximum query response interval
- Querier robustness value
- Other IGMP querier present, interval (minutes:seconds)
- IGMP Querier current state: Querier/Non-Querier
- IGMP version number

## IGMP Group Information

The following command displays IGMP Group information:

**show ip igmp groups**

**Command mode:** All

```
Total entries: 5 Total IGMP groups: 2
Note: The <Total IGMP groups> number is computed as
the number of unique (Group, Vlan) entries!
Note: Local groups (224.0.0.x) are not snooped/relayed and will not
appear.
```

Source	Group	VLAN	Port	Version	Mode	Expires	Fwd
10.1.1.1	232.1.1.1	2	4	V3	INC	4:16	Yes
10.1.1.5	232.1.1.1	2	4	V3	INC	4:16	Yes
*	232.1.1.1	2	4	V3	INC	-	No
10.10.10.43	235.0.0.1	9	1	V3	EXC	2:26	No
*	235.0.0.1	9	1	V3	EXC	-	Yes

IGMP Group information includes:

- IGMP source address
- IGMP Group address
- VLAN and port
- IGMP version
- IGMPv3 filter mode
- Expiration timer value
- IGMP multicast forwarding state



## IGMP Multicast Router Information

The following command displays Mrouter information:

```
show ip igmp mrouter information
```

**Command mode:** All

Total entries: 3							
Total number of dynamic mroouters: 2							
Total number of installed static mroouters: 1							
SrcIP	VLAN	Port	Version	Expires	MRT	QRV	QQIC
10.1.1.1	3	EXT4	V3	4:09	128	2	125
10.1.1.5	2	EXT6	V2	4:09	125	-	-
*	9	EXT7	V2	static	-	-	-

IGMP Mrouter information includes:

- Source IP address
- VLAN and port where the Mrouter is connected
- IGMP version
- Mrouter expiration
- Maximum query response time
- Querier's Robustness Variable (QRV)
- Querier's Query Interval Code (QQIC)

## IPMC Group Information

The following command displays IGMP IPMC group information:

```
show ip igmp ipmcgrp
```

**Command mode:** All

Total number of displayed ipmc groups: 4						
Legend(possible values in Type column):						
SH - static host		DR - dynamic registered				
SP - static primary		DU - dynamic unregistered				
SB - static backup		M - mrouter				
0 - other						
Source	Group	Vlan	Port	Type	Timeleft	
*****	*****	====	*****	====	*****	
*	232.0.0.1	1	-	DU	6 sec	
*	232.0.0.2	1	-	DU	6 sec	
*	232.0.0.3	1	-	DU	6 sec	
*	232.0.0.4	1	-	DU	6 sec	

IGMP IPMC Group information includes:

- IGMPv3 source address
- Multicast group address
- VLAN and port
- Type of IPMC group
- Expiration timer value

## MLD information

[Table 55](#) describes the commands used to view Multicast Listener Discovery (MLD) information.

**Table 55.** *MLD Information Commands*

Command Syntax and Usage
<b>show ipv6 mld groups</b> Displays MLD multicast group information. <b>Command mode:</b> All
<b>show ipv6 mld groups address</b> <IPv6 address> Displays group information for the specified IPv6 address. <b>Command mode:</b> All
<b>show ipv6 mld groups interface port</b> <port alias or number> Displays MLD groups on a single interface port. <b>Command mode:</b> All
<b>show ipv6 mld groups portchannel</b> <LAG number> Displays groups on a single port channel. <b>Command mode:</b> All
<b>show ipv6 mld groups vlan</b> <VLAN number> Displays groups on a single VLAN. <b>Command mode:</b> All
<b>show ipv6 mld mrouter</b> Displays all MLD Mrouter ports. See <a href="#">page 123</a> for sample output. <b>Command mode:</b> All

## MLD Mrouter Information

The following command displays MLD Mrouter information:

```
show ipv6 mld mrouter
```

**Command mode:** All

```
Source: fe80:0:0:0:200:14ff:fea8:40c9
Port/Vlan: 26/4
Interface: 3
QRV: 2  QQIC:125
Maximum Response Delay: 1000
Version: MLDv2 Expires:1:02
```

The following table describes the MLD Mrouter information displayed in the output.

**Table 56.** *MLD Mrouter*

Statistic	Description
Source	Displays the link-local address of the reporter.
Port/Vlan	Displays the port/vlan on which the general query is received.
Interface	Displays the interface number on which the general query is received.
QRV	Displays the Querier's robustness variable value.
QQIC	Displays the Querier's query interval code.
Maximum Response Delay	Displays the configured maximum query response time.
Version	Displays the MLD version configured on the interface.
Expires	Displays the amount of time that must pass before the multicast router decides that there are no more listeners for a multicast address or a particular source on a link.

## VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on EN4093R 10Gb Ethernet Scalable Switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

The following command displays VRRP information:

**show ip vrrp information**

**Command mode:** All

```
VRRP information:
 1: vrid 2, 205.178.18.210, if 1, renter, prio 100, master
 2: vrid 1, 205.178.18.202, if 1, renter, prio 100, backup
 3: vrid 3, 205.178.18.204, if 1, renter, prio 100, master
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
  - owner identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
  - renter identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - master identifies the elected master virtual router.
  - backup identifies that the virtual router is in backup mode.
  - holdoff identifies that the virtual router is in holdoff state.
  - init identifies that the virtual router is waiting for a startup event. For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.

## Interface Information

The following command displays interface information:

**show interface ip**

**Command mode:** All

```
Interface information:
 126:   IP6 fd55:faaf:e1ab:1022:7699:75ff:fe91:a6ef/64   , vlan 4095, up
        fe80::7699:75ff:fe91:a6ef
 128:   IP4 9.37.78.51      255.255.252.0   9.37.79.255 , vlan 4095, up
```

For each interface, the following information is displayed:

- IPv4 interface address and subnet mask
- IPv6 address and prefix
- VLAN assignment
- Status (up, down, disabled)

## IPv6 Interface Information

The following command displays IPv6 interface information:

**show ipv6 interface** [*<interface number>*]

**Command mode:** All

```
Interface information:
 2: IP6 2001:0:0:0:225:3ff:febb:bb15/64          , vlan 1, up
    fe80::225:3ff:febb:bb15
Link local address:
  fe80::225:3ff:febb:bb15
Global unicast address(es):
 2001::225:3ff:febb:bb15/64
Anycast address(es):
  Not Configured.
Joined group address(es):
  ff02::1
  ff02::2
  ff02::1:ffbb:bb15
MTU is 1500
ICMP redirects are enabled
ND DAD is enabled, Number of DAD attempts: 1
ND router advertisement is disabled
```

For each interface, the following information is displayed:

- IPv6 interface address and prefix
- VLAN assignment
- Status (up, down, disabled)
- Path MTU size
- Status of ICMP redirects
- Status of Neighbor Discovery (ND) Duplicate Address Detection (DAD)
- Status of Neighbor Discovery router advertisements

## IPv6 Path MTU Information

The following command displays IPv6 Path MTU information:

**show ipv6 pmtu** [*<destination IPv6 address>*]

**Command mode:** All

```
Path MTU Discovery info:
Max Cache Entry Number : 10
Current Cache Entry Number: 2
Cache Timeout Interval : 10 minutes
Destination Address      Since      PMTU
5000:1::3                00:02:26  1400
FE80::203:A0FF:FED6:141D 00:06:55  1280
```

Path MTU Discovery information provides information about entries in the Path MTU cache. The PMTU field indicates the maximum packet size in octets that can successfully traverse the path from the switch to the destination node. It is equal to the minimum link MTU of all the links in the path to the destination node.

## IP Information

The following command displays Layer 3 information:

**show ip interface brief**

**Command mode:** All

```
IP information:
  AS number 0

Interface information:
126: IP6 0:0:0:0:0:0:0:0/0          , vlan 4095, up
      fe80::200:ff:fe00:ef
128: IP4 9.43.95.121      255.255.255.0   9.43.95.255,    vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
  4: 9.43.95.254,      FAILED

Default IP6 gateway information:

Current BOOTP relay settings: OFF
Global servers:
-----
Server 1 address 0.0.0.0
Server 2 address 0.0.0.0
Server 3 address 0.0.0.0
Server 4 address 0.0.0.0
Server 5 address 0.0.0.0

Current IP forwarding settings: ON, dirbr disabled, icmprd disabled

Current network filter settings:
  none

Current route map settings:
RIP is disabled.

OSPF is disabled.

OSPFv3 is disabled.

BGP is disabled.
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number, and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status.
- BootP relay settings.
- IP forwarding settings, including the forwarding status of directed broadcasts, and the status of ICMP re-directs.
- Network filter settings, if applicable.
- Route map settings, if applicable.



## IKEv2 Information

The following table lists commands that display information about IKEv2.

**Table 57.** *IKEv2 Information Commands*

<b>Command Syntax and Usage</b>
<b>show ikev2</b> Displays all IKEv2 information. See <a href="#">page 130</a> for sample output. <b>Command mode:</b> All
<b>show ikev2 ca-cert</b> Displays the CA certificate. <b>Command mode:</b> All
<b>show ikev2 host-cert</b> Displays the host certificate. <b>Command mode:</b> All
<b>show ikev2 identity</b> Displays IKEv2 identity information. <b>Command mode:</b> All
<b>show ikev2 preshare-key</b> Displays the IKEv2 preshare key. <b>Command mode:</b> All
<b>show ikev2 proposal</b> Displays the IKEv2 proposal. <b>Command mode:</b> All
<b>show ikev2 retransmit-interval</b> Displays the IKEv2 retransmit interval. <b>Command mode:</b> All
<b>show ikev2 sa</b> Displays the IKEv2 SA. <b>Command mode:</b> All

## IKEv2 Information Dump

The following command displays IKEv2 information:

**show ikev2**

**Command mode:** All

```
IKEv2 retransmit time:      20
IKEv2 cookie notification:  disable
IKEv2 authentication method: Pre-shared key
IKEv2 proposal:
Cipher:                     3des
Authentication:             sha1
DH Group:                   dh-2
Local preshare key:         lenovo123
IKEv2 choose IPv6 address as ID type
No SAD entries.
```

IKEv2 information includes:

- IKEv2 retransmit time, in seconds.
- Whether IKEv2 cookie notification is enabled.
- The IKEv2 proposal in force. This includes the encryption algorithm (cipher), the authentication algorithm type, and the Diffie-Hellman (DH) group, which determines the strength of the key used in the key exchange process. Higher DH group numbers are more secure but require additional time to compute the key.
- The local preshare key.
- Whether IKEv2 is using IPv4 or IPv6 addresses as the ID type.
- Security Association Database (SAD) entries, if applicable.

## IPsec Information

The following table describes the commands used to display information about IPsec.

**Table 58.** *IPsec Information Commands*

Command Syntax and Usage
<b>show ipsec dynamic-policy</b> <1-10> Displays dynamic policy information. <b>Command mode:</b> All
<b>show ipsec manual-policy</b> <1-10> Displays manual policy information. See <a href="#">page 132</a> for sample output. <b>Command mode:</b> All
<b>show ipsec sa</b> Displays all security association information. <b>Command mode:</b> All
<b>show ipsec spd</b> Displays all security policy information. <b>Command mode:</b> All
<b>show ipsec traffic-selector</b> <1-10> Displays IPsec traffic selector information. <b>Command mode:</b> All
<b>show ipsec transform-set</b> <1-10> Displays IPsec transform set information. <b>Command mode:</b> All

## IPsec Manual Policy Information

The following command displays IPsec manual key management policy information:

**show ipsec manual-policy**

**Command mode:** All

```
IPsec manual policy 1 -----
IP Address:                2002:0:0:0:0:0:151
Associated transform ID:    1
Associated traffic selector ID: 1
IN-ESP SPI:                9900
IN-ESP encryption KEY:     3456789abcdef012
IN-ESP authentication KEY: 23456789abcdef0123456789abcdef0123456789
OUT-ESP SPI:                7700
OUT-ESP encryption KEY:    6789abcdef012345
OUT-ESP authentication KEY: 56789abcdef0123456789abcdef0123456789abc
Applied on interface:
interface 1
```

IPsec manual policy information includes:

- The IP address of the remote peer
- The transform set ID associated with this policy
- Traffic selector ID associated with this policy
- ESP inbound SPI
- ESP inbound encryption key
- ESP inbound authentication key
- ESP outbound SPI
- ESP outbound encryption key
- ESP outbound authentication key
- The interface to which this manual policy has been applied

## DHCP Snooping Information

The following command displays DHCP Snooping information:

**show ip dhcp snooping**

**Command mode:** All

```
DHCP Snooping is configured on the following VLANs:
empty
Insertion of option 82 information is Disable
  Interface   Trusted   Rate limit (pps)
-----
           1         No         none
           5         No         none
           6         No         none
           7         No         none
           8         No         none
           9         No         none
          10         No         none
          11         No         none
          12         No         none
          13         No         none
          14         No         none
          15         No         none
...

```

The following command displays the DHCP binding table:

**show ip dhcp snooping binding**

**Command mode:** All

Mac Address	IP Address	Lease(seconds)	Type	VLAN	Interface
00:00:01:00:02:01	10.0.0.1	1600	dynamic	100	port 1
02:1c:5f:d1:18:9c	210.38.197.63	86337	Static	127	1
06:51:4d:e6:16:2d	194.116.155.190	86337	Static	105	1
08:69:0f:1d:ba:3d	40.90.17.26	86337	Static	150	1
08:a2:6d:00:36:56	40.194.18.213	86337	Static	108	1
0e:a7:f8:a2:74:2c	130.254.47.129	86337	Static	171	1
0e:b7:64:02:97:7c	35.92.27.110	86337	Static	249	1

Total number of bindings: 7

The DHCP Snooping binding table displays information for each entry in the table. Each entry has a MAC address, an IP address, the lease time, the interface to which the entry applies and the VLAN to which the interface belongs.

## PIM Information

The following commands display PIM information.

**Table 59.** PIM Information Options

Command Syntax and Usage
<p><b>show ip pim bsr</b> [<i>&lt;component ID&gt;</i>]</p> <p>Displays information about the PIM bootstrap router (BSR).</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim component</b> [<i>&lt;component ID (1-2)&gt;</i>]</p> <p>Displays PIM component information. For details, see <a href="#">page 135</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim elected-rp</b> [<b>group</b> <i>&lt;multicast group address&gt;</i>]</p> <p>Displays a list of the elected Rendezvous Points.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim interface</b> [<i>&lt;interface number&gt;</i>   <b>detail</b>   <b>port</b> <i>&lt;port number&gt;</i>]</p> <p>Displays PIM interface information. To view sample output, see <a href="#">page 135</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim mroute</b> [<i>&lt;component ID&gt;</i>   <b>count</b>   <b>flags</b>   <b>group</b> <i>&lt;multicast group address&gt;</i>   <b>interface</b> {<i>&lt;interface number&gt;</i>   <b>port</b> <i>&lt;port number&gt;</i>}   <b>source</b> <i>&lt;multicast source address&gt;</i>]</p> <p>Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see <a href="#">page 137</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim neighbor</b> [<i>&lt;interface number&gt;</i>   <b>port</b> <i>&lt;port number&gt;</i>]</p> <p>Displays PIM neighbor information. To view sample output, see <a href="#">page 136</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim neighbor-filters</b></p> <p>Displays information about PIM neighbor filters.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim rp-candidate</b> [<i>&lt;component ID&gt;</i>]</p> <p>Displays a list of the candidate Rendezvous Points configured.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim rp-set</b> [<i>&lt;RP IP address&gt;</i>]</p> <p>Displays a list of the Rendezvous Points learned.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim rp-static</b> [<i>&lt;component ID&gt;</i>]</p> <p>Displays a list of the static Rendezvous Points configured.</p> <p><b>Command mode:</b> All</p>

## PIM Component Information

The following command displays Protocol Independent Multicast (PIM) component information:

**show ip pim component** [*<component ID>*]

**Command mode:** All

```
PIM Component Information
-----
Component-Id: 1
  PIM Mode: sparse,   PIM Version: 2
  Elected BSR: 1.1.1.1
  Candidate RP Holdtime: 100
```

```
PIM Component Information
-----
Component-Id: 1
  PIM Mode: dense,   PIM Version: 2
  Graft Retry Count: 1
```

PIM component information includes the following:

- Component ID
- Mode (sparse, dense)
- PIM Version
- Elected Bootstrap Router (BSR) address
- Candidate Rendezvous Point (RP) hold time, in seconds

## PIM Interface Information

The following command displays information about PIM interfaces:

**show ip pim interface**

**Command mode:** All

Address	IfName/IfId	Ver/Mode	Nbr Count	Qry Interval	DR-Address	DR-Prio
40.0.0.3	net4/4	2/Sparse	1	30	40.0.0.3	1
50.0.0.3	net5/5	2/Sparse	0	30	50.0.0.3	1

PIM interface information includes the following for each PIM interface:

- IP address
- Name and ID
- Version and mode
- Neighbor count
- Query interval
- Designated Router address
- Designated Router priority value

## PIM Neighbor Information

The following command displays PIM neighbor information:

**show ip pim neighbor**

**Command mode:** All

Neighbour Address	IfName/Idx	Uptime/Expiry	Ver	DRPri/Mode	CompId	Override Interval	Lan Delay
40.0.0.2	net4/4	00:00:37/79	v2	1/S	1	0	0
40.0.0.4	net1/160	00:03:41/92	v2	32/S	2	0	0

PIM neighbor information includes the following:

- Neighbor IP address, interface name, and interface ID
- Name and ID of interface used to reach the PIM neighbor
- Up time (the time since this neighbor became the neighbor of the local router)
- Expiry Time (the minimum time remaining before this PIM neighbor expires)
- Version number
- Designated Router priority and mode
- Component ID
- Override interval
- LAN delay interval



## PIM Multicast Route Information Commands

The following commands display PIM Multicast Route information.

**Table 60.** PIM Multicast Route Information Options

Command Syntax and Usage
<b>show ip pim mroute</b> Displays information about all PIM multicast routes. <b>Command mode:</b> All
<b>show ip pim mroute [&lt;component ID&gt;]</b> Displays PIM multicast routes for the selected component. <b>Command mode:</b> All
<b>show ip pim mroute count</b> Displays a count of PIM multicast routes of each type. <b>Command mode:</b> All
<b>show ip pim mroute flags [s] [r] [w]</b> Displays PIM multicast routes based on the selected entry flags. Enter flags in any combination: <ul style="list-style-type: none"><li>o <b>S:</b> Shortest Path Tree (SPT) bit</li><li>o <b>R:</b> Rendezvous Point Tree (RPT) bit</li><li>o <b>W:</b> Wildcard bit</li></ul> <b>Command mode:</b> All
<b>show ip pim mroute group &lt;multicast group IP address&gt;</b> Displays PIM multicast routes for the selected multicast group. <b>Command mode:</b> All
<b>show ip pim mroute interface &lt;interface number&gt;</b> Displays PIM multicast routes for the selected incoming IP interface. <b>Command mode:</b> All
<b>show ip pim mroute source &lt;multicast source IP address&gt;</b> Displays PIM multicast routes for the selected source IP address. <b>Command mode:</b> All

## *PIM Multicast Route Information*

The following command displays PIM multicast route information:

**show ip pim mroute**

**Command mode:** All

```
IP Multicast Routing Table
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires

(8.8.8.111, 224.2.2.100) ,00:42:03/00:01:11
Incoming Interface : net44 ,RPF nbr : 44.44.44.1 ,Route Flags : S
Outgoing InterfaceList :
    net17, Forwarding/Sparse ,00:42:03/---

(*, 224.2.2.100) ,00:45:15/--- ,RP : 88.88.88.2
Incoming Interface : net5 ,RPF nbr : 5.5.5.2 ,Route Flags : WR
Outgoing InterfaceList :
    net17, Forwarding/Sparse ,00:45:15/---

Total number of (*,G) entries : 1
Total number of (S,G) entries : 1
```

---

## Quality of Service Information

The following commands display Quality of Service information.

**Table 61.** *QoS Information Options*

<b>Command Syntax and Usage</b>
<b>show qos dscp</b> Displays the current DSCP parameters. <b>Command mode:</b> All
<b>show qos protocol-packet-control information protocol</b> Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. <b>Command mode:</b> All
<b>show qos protocol-packet-control information queue [all]</b> Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. <b>Command mode:</b> All
<b>show qos transmit-queue</b> Displays mapping of 802.1p value to Class of Service queue number, and COS queue weight value. <b>Command mode:</b> All
<b>show qos transmit-queue information</b> Displays all 802.1p information. For details, see <a href="#">page 140</a> . <b>Command mode:</b> All
<b>show qos random-detect</b> Displays WRED ECN information. <b>Command mode:</b> All

## 802.1p Information

The following command displays 802.1p information:

**show qos transmit-queue information**

**Command mode:** All

```

Current priority to COS queue information:
Priority  COSq  Weight
-----  -
    0      0      1
    1      1      2
    2      2      3
    3      3      4
    4      4      5
    5      5      7
    6      6     15
    7      7      0

Current port priority information:
Port     Priority  COSq  Weight
-----  -
INT1     0         0      1
INT2     0         0      1
...
MGT1     0         0      1
MGT2     0         0      1
EXT1     0         0      1
EXT2     0         0      1
EXT3     0         0      1
EXT4     0         0      1
...

```

The following table describes the IEEE 802.1p priority-to-COS queue information.

**Table 62.** *802.1p Priority-to-COS Queue Parameter Descriptions*

Parameter	Description
Priority	Displays the 802.1p Priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight of the COS queue.

The following table describes the IEEE 802.1p port priority information.

**Table 63.** *802.1p Port Priority Parameter Descriptions*

Parameter	Description
Port	Displays the port alias.
Priority	Displays the 802.1p Priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight.

## WRED and ECN Information

The following command displays WRED and ECN information:

**show qos random-detect**

**Command mode:** All

```
Current wred and ecn configuration:
Global ECN: Disable
Global WRED: Disable

--WRED--TcpMinThr--TcpMaxThr--TcpDrate--NonTcpMinThr--NonTcpMaxThr--NonTcpDrate--
TQ0:  Dis      0      0      0      0      0      0
TQ1:  Dis      0      0      0      0      0      0
TQ2:  Dis      0      0      0      0      0      0
TQ3:  Dis      0      0      0      0      0      0
TQ4:  Dis      0      0      0      0      0      0
TQ5:  Dis      0      0      0      0      0      0
TQ6:  Dis      0      0      0      0      0      0
TQ7:  Dis      0      0      0      0      0      0
...
```

---

## Access Control List Information Commands

The following commands display Access Control List information.

**Table 64.** *ACL Information Options*

Command Syntax and Usage
<b>show access-control group</b> [ <i>&lt;1-640&gt;</i> ] Displays ACL group information. <b>Command mode:</b> All
<b>show access-control list</b> [ <i>&lt;1-640&gt;</i> ] Displays ACL list information. For details, see <a href="#">page 143</a> . <b>Command mode:</b> All
<b>show access-control list6</b> [ <i>&lt;1-128&gt;</i> ] Displays IPv6 ACL list information. <b>Command mode:</b> All
<b>show access-control list</b> <i>&lt;1-640&gt;</i> <b>log</b> Displays the current IPv4 ACL log state. <b>Command mode:</b> All
<b>show access-control vmap</b> [ <i>&lt;1-128&gt;</i> ] Displays VMAP information. <b>Command mode:</b> All

## Access Control List Information

The following command displays Access Control List (ACL) information:

```
show access-control list <1-640>
```

**Command mode:** All

```
Current ACL information:
-----
Filter 2 profile:
 Ethernet
  - VID          : 2/0xffff
 Meter
  - Set to disabled
  - Set committed rate : 64
  - Set max burst size : 32
 Re-Mark
  - Set use of TOS precedence to disabled
 Actions         : Permit
 Statistics      : enabled
```

Access Control List (ACL) information includes configuration settings for each ACL and ACL Group.

**Table 65.** *ACL Parameter Descriptions*

Parameter	Description
Filter <i>x</i> profile	Indicates the ACL number.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
Actions	Displays the configured action for the ACL.
Statistics	Displays the status of ACL statistics configuration (enabled or disabled).

---

## OpenFlow Information

The following commands display OpenFlow information.

**Table 66.** *OpenFlow Information Options*

Command Syntax and Usage
<p><b>show openflow [flow-allocation group information table]</b></p> <p>Displays the current OpenFlow configuration. For more information, see <a href="#">page 145</a>.</p> <ul style="list-style-type: none"><li>o <b>flow-allocation</b> displays the configured, current and maximum number of flows for each OpenFlow instance. For more information, see <a href="#">page 147</a>.</li><li>o <b>group</b> displays group information for all OpenFlow 1.3 instances. For more information, see <a href="#">page 149</a>.</li><li>o <b>information</b> displays the configuration for each OpenFlow instance. For more information, see <a href="#">page 150</a>.</li><li>o <b>table</b> displays the basic and emergency flow tables for each OpenFlow instance. For more information, see <a href="#">page 152</a></li></ul> <p><b>Command mode:</b> All</p>
<p><b>show openflow instance &lt;1-2&gt; [group information table]</b></p> <p>Displays OpenFlow information for the specified instance ID:</p> <ul style="list-style-type: none"><li>o <b>group</b> displays group information per instance</li><li>o <b>information</b> displays the instance configuration</li><li>o <b>table</b> displays the basic and emergency flow tables</li></ul> <p><b>Command mode:</b> All</p>



## OpenFlow Global Configuration Information

The following command displays the global OpenFlow configuration parameters for all instances in OpenFlow 1.0 and OpenFlow 1.3:

**show openflow**

**Command mode:** All

In OpenFlow 1.0:

```
Protocol Version: 1.0
Openflow State: Enabled
FDB Table Priority: 1000
FDB Table FDB-timeout: Disabled

Openflow Instance ID: 1
  state: enabled , buffering: enabled
  retry 3, emergency time-out 30
  echo req interval 120, echo reply time-out 60
  min-flow-timeout : use controller provided values.
  max flows acl      : Maximum Available
  max flows unicast fdb : Maximum Available
  max flows multicast fdb : Maximum Available
  emergency feature: disabled
  dpid: 0x00010817f40a0400
  ports : EXT1-EXT3
  Controller Id: 1
    Active Controller
    IP Address: 9.70.31.71, port: 6633, Extm-port

Openflow instance 2 is currently disabled

Openflow Edge ports : None
```

### In OpenFlow 1.3:

```
Protocol Version: 1.3.1
Openflow State: Enabled
FDB Table Priority: 1000
MPLS Table Priority: 65535
FDB Table FDB-timeout: Disabled

Openflow instance 1 is currently disabled

Openflow Instance ID: 2
  state: enabled , buffering: disabled , table-miss: drop
  echo req interval 30, echo reply time-out 15, retry 4
  min-flow-timeout : use controller provided values.
  max flows acl      : Maximum Available
  max flows unicast fdb : Maximum Available
  max flows multicast fdb : Maximum Available
  max flows mpls push : Maximum Available
  max flows mpls pop : Maximum Available
  dpid: 0x0002749975ab5c00
  table-miss cookie: 0xffffffffffffffff
  mirror-to-controller cookie: 0xffffffffffffffff
  send-to-controller cookie: 0xffffffffffffffff
  ports : EXT1-EXT3
  portchannel: 10
  Controller Id: 1
    Active Controller
    IP Address: 9.70.31.71, port: 6633, Mgt-Port

Openflow Edge ports : None
```

## OpenFlow Flow Allocation Information

The following command displays the OpenFlow flow allocation for all instances in OpenFlow 1.0 and OpenFlow 1.3:

**show openflow flow-allocation**

**Comand mode:** All

In OpenFlow 1.0:

```
Flow Allocation Information

Instance 1

Maximum ACL Count Configured      : Maximum Available
Maximum Unicast FDB Count Configured : Maximum Available
Maximum Multicast FDB Count Configured: Maximum Available

Basic Entries

Current ACL Count                  : 3
Current Unicast FDB Count          : 0
Current Multicast FDB Count        : 0

Emergency Entries

Current ACL Count                  : 0
Current Unicast FDB Count          : 0
Current Multicast FDB Count        : 0

Maximum Current Availability

Maximum Available ACL Count        : 750
Maximum Available Unicast FDB Count : 123904
Maximum Available Multicast FDB Count: 4096

Instance 2
...
```

## In OpenFlow 1.3:

```
Flow Allocation Information

Instance 1

Maximum ACL Count Configured           : Maximum Available
Maximum Unicast FDB Count Configured   : Maximum Available
Maximum Multicast FDB Count Configured : Maximum Available
Maximum MPLS PUSH Count Configured     : Maximum Available
Maximum MPLS POP Count Configured      : Maximum Available

Basic Entries

Current ACL Count                       : 3
Current Unicast FDB Count                : 0
Current Multicast FDB Count             : 0
Current MPLS PUSH Count                  : 0
Current MPLS POP Count                   : 0

Static Entries

Current static ACL Count                 : 0
Current static MPLS PUSH Count           : 0
Current static MPLS POP Count            : 0

Maximum Current Availability

Maximum Available ACL Count              : 750
Maximum Available Unicast FDB Count      : 123904
Maximum Available Multicast FDB Count    : 4096
Maximum Available MPLS PUSH Count        : 2000
Maximum Available MPLS POP Count         : 1000

...
```

## OpenFlow Group Information

The following command displays the OpenFlow 1.3 group information for all instances:

**show openflow group**

**Command mode:** All

```
Openflow Instance Id: 1
Group count: 3
Group 1, Type: ALL, Bucket count: 2
  Bucket #0: output:INGRESS
  Bucket #1: output:ext1
Group 2, Type: ALL, Bucket count: 2
  Bucket #0: output:INGRESS
  Bucket #1: output:PCH64
Group 3, Type: ALL, Bucket count: 2
  Bucket #0: output:PCH52
  Bucket #1: output:PCH64
Openflow instance 2 is currently disabled
```

## OpenFlow Configuration Information

The following command displays the OpenFlow configuration for all instances in OpenFlow 1.0 and OpenFlow 1.3:

### show openflow information

**Command mode:** All

In OpenFlow 1.0:

```
Openflow feature is Enabled
-----
Openflow Instance ID: 1
  State : Enabled
  DataPath ID: 0x00010817f40a0400
  Max Retries per controller: 3
  Echo Request Interval: 120
  Echo Reply Timeout: 60
  Emergency Timeout: 30
  Min-flow-timeout : 0, use controller provided values.
  Max ACL Flows: Maximum Available
  Max Unicast FDB Flows: Maximum Available
  Max Multicast FDB Flows: Maximum Available
  Buffering: Enabled
  Operational Mode: Normal
  Miss Send Len: 65535

Port  Alias  Status  State  Config  Current  Advertised  Supported  Peer
43    EXT1    d       0x201  0x2     0x140    0x0         0x0         0x0
44    EXT2    d       0x201  0x2     0x140    0x0         0x0         0x0
45    EXT3    e       0x200  0x2     0x2a0    0x0         0x0         0x0

Number of Ports: 3
Configured Controllers:
  Openflow Controller 1:
    IP Address: 9.70.31.71
    Port: 6633
    State: Active
    Retry Count: 0

-----

Openflow instance 2 is currently disabled
```

In OpenFlow 1.3:

```
Openflow feature is Enabled
-----
Openflow Instance ID: 1
  State : Enabled
  DataPath ID: 0x00010817f40a0400
  Table-miss cookie: 0xffffffffffffffff
  Mirror-to-controller cookie: 0xffffffffffffffff
  Send-to-controller cookie: 0xffffffffffffffff
  Max Retries per controller: 3
  Echo Request Interval: 120
  Echo Reply Timeout: 60
  Min-flow-timeout : 0, use controller provided values.
  Max ACL Flows: Maximum Available
  Max Unicast FDB Flows: Maximum Available
  Max Multicast FDB Flows: Maximum Available
  Max MPLS Push Flows: Maximum Available
  Max MPLS Pop Flows: Maximum Available
  Buffering: Enabled
  Table Miss: Drop
  Operational Mode: Normal
  Miss Send Len: 65535

Port  Alias  Status  State  Config  Current  Advertised  Supported  Peer
43    EXT1    d       0x1    0x0     0x1040   0x0         0x0        0x0
44    EXT2    d       0x1    0x0     0x1040   0x0         0x0        0x0
45    EXT3    e       0x0    0x0     0x2820   0x0         0x0        0x0

Number of Ports: 3
Number of Portchannels: 0

Configured Controllers:
  Openflow Controller 1:
    IP Address: 9.70.31.71
    Port: 6633
    State: Active
-----

Openflow instance 2 is currently disabled
```

## OpenFlow Table Information

The following command displays the basic and emergency flow tables for all instances in OpenFlow 1.0 and OpenFlow 1.3:

### **show openflow table**

**Command mode:** All

In OpenFlow 1.0:

```
Openflow Instance Id: 1
BASIC FLOW TABLE
CONTROLLER ADDED FLOWS
Flow:1
  Filter Based, priority:    0, hard-time-out:    0, idle-time-out:    0
  cookie: 0x0
  QUALIFIERS:
  ACTION: drop
  STATS:  packets=0, bytes=0
Flow:2
  Filter Based, priority:65535, hard-time-out:    0, idle-time-out:    0
  cookie: 0x0
  QUALIFIERS: ether-type:0x88cc
               protocol: 0, tos: 0
               src-ip:0.0.0.0/32, dst-ip:0.0.0.0/32
               src-port: 0, dst-port: 0
  ACTION: output:CONTROLLER [Max Len: 65535 / 65535 bytes (C/S)]
  STATS:  packets=0, bytes=0
Flow:3
  Filter Based, priority:    2, hard-time-out:    0, idle-time-out:    0
  cookie: 0x0
  QUALIFIERS:
  ACTION: output:CONTROLLER [Max Len: 65535 / 65535 bytes (C/S)]
  STATS:  packets=2, bytes=190
Openflow instance 2 is currently disabled
```



In OpenFlow 1.3:

```
Openflow Instance Id: 1
CONTROLLER added FLOWS

Flow 1, Filter Based, priority:2, hard-time-out:0, idle-time-out:0
  cookie:0x0
  QUALIFIERS:
  Instruction: apply_action
  ACTION: output:CONTROLLER [Max Len: 65535 / 65535 bytes (C/S)]
  STATS: packets=0, bytes=0

Flow 2, Filter Based, priority:65535, hard-time-out:0, idle-time-out:0
  cookie:0x0
  QUALIFIERS: eth-type:0x88cc
  Instruction: apply_action
  ACTION: output:CONTROLLER [Max Len: 65535 / 65535 bytes (C/S)]
  STATS: packets=0, bytes=0

Flow 3, Filter Based, priority:0, hard-time-out:0, idle-time-out:0
  cookie:0x0
  QUALIFIERS:
  Instruction: empty
  ACTION: drop
  STATS: packets=0, bytes=0

Openflow instance 2 is currently disabled
```

OpenFlow table information includes detailed configuration information for each entry in the flow table.

**Note:** Flow qualifiers used for matching packets are not listed in the display if the qualifier is set to `any`.

---

## RMON Information Commands

The following table describes the Remote Monitoring (RMON) Information commands.

**Table 67.** *RMON Information commands*

Command Syntax and Usage
<b>show rmon</b> Displays all RMON information. <b>Command mode:</b> All
<b>show rmon alarm [<i>&lt;alarm group number&gt;</i>]</b> Displays RMON Alarm information. For details, see <a href="#">page 156</a> . <b>Command mode:</b> All
<b>show rmon event [<i>&lt;event group number&gt;</i>]</b> Displays RMON Event information. For details, see <a href="#">page 157</a> . <b>Command mode:</b> All
<b>show rmon history [<i>&lt;history group number&gt;</i>]</b> Displays RMON History information. For details, see <a href="#">page 155</a> . <b>Command mode:</b> All

## RMON History Information

The following command displays RMON History information:

**show rmon history**

**Command mode:** All

RMON History group configuration:				
Index	IFOID	Interval	Rbnum	Gbnum
1	1.3.6.1.2.1.2.2.1.1.24	30	5	5
2	1.3.6.1.2.1.2.2.1.1.22	30	5	5
3	1.3.6.1.2.1.2.2.1.1.20	30	5	5
4	1.3.6.1.2.1.2.2.1.1.19	30	5	5
5	1.3.6.1.2.1.2.2.1.1.24	1800	5	5
Index	Owner			
1	dan			

The following table describes the RMON History Information parameters.

**Table 68.** RMON History Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each history instance.
IFOID	Displays the MIB Object Identifier.
Interval	Displays the time interval for each sampling bucket.
Rbnum	Displays the number of requested buckets, which is the number of data slots into which data is to be saved.
Gbnum	Displays the number of granted buckets that may hold sampled data.
Owner	Displays the owner of the history instance.

## RMON Alarm Information

The following command displays RMON Alarm information:

**show rmon alarm**

**Command mode:** All

```

RMON Alarm group configuration:
Index  Interval  Sample  Type      rLimit    fLimit    last value
-----  -----  -----  -----  -----  -----  -----
   1     1800     abs     either           0           0         7822

Index  rEvtIdx  fEvtIdx                OID
-----  -----  -----  -----
   1         0         0  1.3.6.1.2.1.2.2.1.10.1

Index                                Owner
-----
   1  dan
  
```

The following table describes the RMON Alarm Information parameters.

**Table 69.** RMON Alarm Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each alarm instance.
Interval	Displays the time interval over which data is sampled and compared with the rising and falling thresholds.
Sample	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: <ul style="list-style-type: none"> <li>o <code>abs</code>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li> <li>o <code>delta</code>—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</li> </ul>
Type	Displays the type of alarm, as follows: <ul style="list-style-type: none"> <li>o <code>falling</code>—alarm is triggered when a falling threshold is crossed.</li> <li>o <code>rising</code>—alarm is triggered when a rising threshold is crossed.</li> <li>o <code>either</code>—alarm is triggered when either a rising or falling threshold is crossed.</li> </ul>
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.
Last value	Displays the last sampled value.

**Table 69.** *RMON Alarm Parameter Descriptions (continued)*

Parameter	Description
rEvtIdx	Displays the rising alarm event index that is triggered when a rising threshold is crossed.
fEvtIdx	Displays the falling alarm event index that is triggered when a falling threshold is crossed.
OID	Displays the MIB Object Identifier for each alarm index.
Owner	Displays the owner of the alarm instance.

## RMON Event Information

The following command displays RMON Alarm information:

**show rmon event**

**Command mode:** All

```

RMON Event group configuration:
Index Type      Last Sent          Description
-----
  1  both  0D: 0H: 1M:20S  Event_1
  2  none  0D: 0H: 0M: 0S  Event_2
  3  log   0D: 0H: 0M: 0S  Event_3
  4  trap  0D: 0H: 0M: 0S  Event_4
  5  both  0D: 0H: 0M: 0S  Log and trap event for Link Down
 10  both  0D: 0H: 0M: 0S  Log and trap event for Link Up
 11  both  0D: 0H: 0M: 0S  Send log and trap for icmpInMsg
 15  both  0D: 0H: 0M: 0S  Send log and trap for icmpInEchos

Index          Owner
-----
  1  dan
    
```

The following table describes the RMON Event Information parameters.

**Table 70.** *RMON Event Parameter Descriptions*

Parameter	Description
Index	Displays the index number that identifies each event instance.
Type	Displays the type of notification provided for this event, as follows: none, log, trap, both.
Last sent	Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots.
Description	Displays a text description of the event.
Owner	Displays the owner of the alarm instance.

## Link Status Information

The following command displays link information:

**show interface status** [*<port alias or number>*]

**Command mode:** All

Alias	Port	Speed	Duplex	Flow Ctrl		Link	Name
				TX	RX		
INTA1	1	1G/10G	full	yes	yes	down	INTA1
INTA2	2	1G/10G	full	yes	yes	down	INTA2
INTA3	3	1G/10G	full	yes	yes	down	INTA3
INTA4	4	1G/10G	full	yes	yes	down	INTA4
...							
INTA14	14	1G/10G	full	yes	yes	down	INTA14
INTB1	15	1G/10G	full	yes	yes	down	INTB1
INTB2	16	1G/10G	full	yes	yes	down	INTB2
INTB3	17	1G/10G	full	yes	yes	down	INTB3
INTB4	18	1G/10G	full	yes	yes	down	INTB4
...							
INTC14	42	1G/10G	full	yes	yes	down	INTC14
EXT1	43	1G/10G	full	no	no	down	EXT1
EXT2	44	1G/10G	full	no	no	down	EXT2
EXT3	45	10000	full	no	no	up	EXT3
EXT4	46	1G/10G	full	no	no	down	EXT4
...							
EXT20	62	10000	full	no	no	disabled	EXT20
EXT21	63	10000	full	no	no	disabled	EXT21
EXT22	64	10000	full	no	no	disabled	EXT22
EXTM	65	1000	full	yes	yes	up	EXTM
MGT1	66	1000	full	no	no	up	MGT1

**Note:** The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Lenovo Switch that you are using and the firmware versions and options that are installed.

Use this command to display link status information about each port on the EN4093R, including:

- Port alias and port number
- Port speed and Duplex mode (half, full, any)
- Flow control for transmit and receive (no, yes, or both)
- Link status (up, down, or disabled)

## Port Information

The following command displays port information:

```
show interface trunk <port alias or number>
```

**Command mode:** All

Alias	Port	Tag Trk	Type	RMON	Lrn	Fld	PVID NVLAN	DESCRIPTION	VLAN(s)
INTA1	1	n	Internal	d	e	e	4081#	INTA1	4081
INTA2	2	n	Internal	d	e	e	4081#	INTA2	4081
INTA3	3	n	Internal	d	e	e	4081#	INTA3	4081
INTA4	4	n	Internal	d	e	e	4081#	INTA4	4081
INTA5	5	n	Internal	d	e	e	4081#	INTA5	4081
INTA6	6	n	Internal	d	e	e	4081#	INTA6	4081
INTA7	7	n	Internal	d	e	e	4081#	INTA7	4081
INTA8	8	n	Internal	d	e	e	4081#	INTA8	4081
INTA9	9	n	Internal	d	e	e	4081#	INTA9	4081
INTA10	10	n	Internal	d	e	e	4081#	INTA10	4081
INTA11	11	n	Internal	d	e	e	4081#	INTA11	4081
INTA12	12	n	Internal	d	e	e	4081#	INTA12	4081
INTA13	13	n	Internal	d	e	e	4081#	INTA13	4081
INTA14	14	n	Internal	d	e	e	4081#	INTA14	4081
INTB1	15	n	Internal	d	e	e	4082#	INTB1	4082
INTB2	16	n	Internal	d	e	e	4082#	INTB2	4082
INTB3	17	n	Internal	d	e	e	4082#	INTB3	4082
INTB4	18	n	Internal	d	e	e	4082#	INTB4	4082
INTB5	19	n	Internal	d	e	e	4082#	INTB5	4082
INTB6	20	n	Internal	d	e	e	4082#	INTB6	4082
INTB7	21	n	Internal	d	e	e	4082#	INTB7	4082
INTB8	22	n	Internal	d	e	e	4082#	INTB8	4082
INTB9	23	n	Internal	d	e	e	4082#	INTB9	4082
INTB10	24	n	Internal	d	e	e	4082#	INTB10	4082
INTB11	25	n	Internal	d	e	e	4082#	INTB11	4082
INTB12	26	n	Internal	d	e	e	4082#	INTB12	4082
INTB13	27	n	Internal	d	e	e	4082#	INTB13	4082
INTB14	28	n	Internal	d	e	e	4082#	INTB14	4082
INTC1	29	n	Internal	d	e	e	4083#	INTC1	4083
INTC2	30	n	Internal	d	e	e	4083#	INTC2	4083
INTC3	31	n	Internal	d	e	e	4083#	INTC3	4083
INTC4	32	n	Internal	d	e	e	4083#	INTC4	4083
INTC5	33	n	Internal	d	e	e	4083#	INTC5	4083
INTC6	34	n	Internal	d	e	e	4083#	INTC6	4083
...									
EXT21	63	n	External	d	e	e	1	EXT21	1
EXT22	64	n	External	d	e	e	1	EXT22	1
EXTM	65	n	Mgmt	d	e	e	4095	EXTM	4095
MGT1	66	y	Mgmt	d	e	e	4095	MGT1	4095

\* = PVID/Native-VLAN is tagged.  
# = PVID is ingress tagged.  
Trk = Trunk mode  
NVLAN = Native-VLAN

**Note:** The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Lenovo Switch that you are using and the firmware versions and options that are installed.

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (y or n)
- Whether the port uses PVID/Native-VLAN tagging or not (y or n)
- Whether the port uses PVID ingress tagging or not (y or n)
- Whether the port is internal, external or used for management
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB Learning enabled (**Lrn**)
- Whether the port has Port Flooding enabled (**Fld**)
- Port VLAN ID (PVID/Native-VLAN)
- Port description
- VLAN membership



---

## Port Transceiver Status

The following command displays the status of the transceiver module on each external port:

**show interface transceiver**

**Command mode:** All

Port	Link	Transceiver	Vendor	Part	Approve
43 SFP+ 1		< NO Device Installed >			
44 SFP+ 2	Down	CU SFP	IBM-Finisar	78P3177-N81713	Approved
53 FLEX 1		< NO Device Installed >			
54 FLEX 2		< NO Device Installed >			
55 FLEX 3	Down	3m ACTX	IBM-Amphenol	46K6183-L36836B	Accepted
56 FLEX 4		< NO Device Installed >			
57 FLEX 5		< NO Device Installed >			
58 FLEX 6		< NO Device Installed >			
59 FLEX 7		< NO Device Installed >			
60 FLEX 8	LINK	3m DAC	BLADE NETWORKS	BN-SP-CBL-3M	Accepted
61 FLEX 9		< NO Device Installed >			
62 FLEX 10	LINK	1m DAC	BLADE NETWORKS	BN-SP-CBL-1M	Accepted
63 FLEX 11		< NO Device Installed >			
64 FLEX 12		< NO Device Installed >			

This command displays information about the transceiver module on each port, as follows:

- Port number and media type
- Link status
- Transceiver detail
- Vendor information
- Part number
- Approval state

Use the following command to display extended transceiver information:

**show interface port** <port number> **transceiver details**

**Command mode:** All

Port	TX	Link	TXFlt	Volts	DegsC	TXuW	RXuW	Transceiver	Approve
55	FLEX	3 Ena	Down	-N/A-	-N/A-	-N/A-	-N/A-	3m ACTX	Accepted
IBM-Amphenol Part:46K6183-L36836B Date:111231 S/N:YL11FY1CY40G									

This command displays detailed information about the transceiver module, as follows:

- Port number and media type
- TX: Transmission status
- TXflt: Transmission fault indicator
- Volts: Power usage, in volts
- DegsC: Temperature, in degrees centigrade
- TXuW: Transmit power, in micro-watts
- RXuW: Receive power, in micro-watts
- Media type (LX, LR, SX, SR)
- Approval status: One of the following:
  - Accepted: You can use this transceiver at your own risk.
  - Approved: This transceiver is on the list of officially supported transceivers.

The optical power levels shown for transmit and receive functions for the transceiver must fall within the expected range defined in the IEEE 802-3-2008 specification for each transceiver type. For convenience, the expected range values are summarized in the following table.

**Table 71.** *Expected Transceiver Optical Power Levels*

Transceiver Type	Tx Minimum	Tx Maximum	Rx Minimum	Rx Maximum
SFP SX	112μW	1000μW	20μW	1000μW
SFP LX	70.8μW	501μW	12.6μW	501μW
SFP+ SR	186μW	794μW	102μW	794μW
SFP+ LR	151μW	891μW	27.5μW	891μW

**Note:** Power level values in the IEEE specification are shown in dBm, but have been converted to mW in this table to match the unit of measure shown in the display output.

---

## VM Ready Information

The following command display information about Virtual Machines (VMs).

**Table 72.** *Virtual Machines Information Options*

Command Syntax and Usage
<b>show virt</b> Displays the current virtualization parameters. For a sample output, see <a href="#">page 165</a> . <b>Command mode:</b> All
<b>show virt oui</b> Displays all the configured MAC OUIs. For a sample output, see <a href="#">page 165</a> . <b>Command mode:</b> All
<b>show virt port</b> <port alias or number> Displays VM Ready information for the selected port. For a sample output, see <a href="#">page 166</a> . <b>Command mode:</b> All
<b>show virt portchannel</b> <portchannel group member> Displays Virtual Machine information for the selected portchannel. For a sample output, see <a href="#">page 166</a> . <b>Command mode:</b> All
<b>show virt vm [-v -r]</b> Displays all VM Ready information. <ul style="list-style-type: none"><li>o -v displays verbose information</li><li>o -r rescans the data center</li></ul> For a sample output, see <a href="#">page 167</a> . <b>Command mode:</b> All
<b>show virt vmcheck</b> Displays the current VM Check settings. For a sample output, see <a href="#">page 167</a> . <b>Command mode:</b> All
<b>show virt vmgroup</b> [<1-4096>] Displays the current VM Group parameters. For a sample output, see <a href="#">page 168</a> . <b>Command mode:</b> All

**Table 72.** *Virtual Machines Information Options*

<b>Command Syntax and Usage</b>
<p><b>show virt</b></p> <p>Displays the current virtualization parameters. For a sample output, see <a href="#">page 165</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show virt oui</b></p> <p>Displays all the configured MAC OUIs. For a sample output, see <a href="#">page 165</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show virt vmpolicy vmbandwidth</b> [&lt;MAC address&gt;   &lt;UUID&gt;   &lt;name&gt;   &lt;IP address&gt;   &lt;index number&gt;]</p> <p>Displays the current VM bandwidth management parameters. For a sample output, see <a href="#">page 168</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show virt vmprofile</b> [&lt;profile name&gt;]</p> <p>Displays the current VM Profile parameters. For a sample output, see <a href="#">page 168</a>.</p> <p><b>Command mode:</b> All</p>

## VMReady Information

The following command displays the current virtualization options:

**show virt**

**Command mode:** All

```
VMready is currently enabled

Current Hello setting: disabled

Current VMware-specific settings
-----

ESX/ESXi-to-vCenter heartbeat UDP port number: 902

Current VM profiles:
-----
      None

VM group 1 current configuration:Current VM group's secure mode: Disabled
Current Group Ports: 13 17
Current Group vPorts: : empty
VLAN: 2
VLAN Tagging: Disabled
Current GROUP VMAP Config is empty

VM group 2 current configuration: empty
...
```

## VM OUI Information

The following command displays all the configured MAC OUIs:

**show virt oui**

**Command mode:** All

```
      VM MAC OUI      Vendor Name
      -----
      00:50:56        VMware
      00:0c:29        VMware
      00:05:69        VMware
      00:0f:4b        VirtualIron
      00:03:ff        Microsoft
      00:15:5d        Microsoft
      00:1c:42        Parallels
      00:16:3e        Xen
      00:80:27        Sun

      Number of MAC OUI entries: 9
```

## VM Port Information

The following command displays VM information for a specific port:

**show virt port** <port alias or number>

**Command mode:** All

IP Address	VMAC Address	Index	Port	VM Group	(Profile)	Check status
3.3.3.2	00:50:56:a5:32:f7	0	23			
40.40.31.1	00:50:56:a5:4e:9f	1	23	30	test30	

Number of entries: 2

## VM Portchannel Information

The following command displays VM information for a specific portchannel:

**show virt portchannel** <1-128>

**Command mode:** All

IP Address	VMAC Address	Index	Port	VM Group	(Profile)	Check status
5.5.5.2	00:50:56:a5:17:07	2	ST 5			
0.0.0.0	00:50:56:a5:4b:03	4	ST 5			
5.5.5.3	00:50:56:af:20:6f	3	ST 5			

Number of entries: 3  
0.0.0.0 indicates IP address not yet available  
ST: Server Trunk

## VM Information

The following command displays VM information:

```
show virt vm
```

**Command mode:** All

IP Address	VMAC Address	Index	Port	VM Group(Profile)	Check Status
*127.31.46.50	00:50:56:4e:62:f5	4	INTA3		
*127.31.46.10	00:50:56:4f:f2:85	2	INTA4		
+127.31.46.51	00:50:56:72:ec:86	1	INTA3		
+127.31.46.11	00:50:56:7c:1c:ca	3	INTA4		
127.31.46.25	00:50:56:9c:00:c8	5	INTA4		
127.31.46.15	00:50:56:9c:21:2f	0	INTA4		
127.31.46.35	00:50:56:9c:29:29	6	INTA3		
Number of entries: 7					
* indicates VMware ESX Service Console Interface					
+ indicates VMware ESX/ESXi VMKernel or Management Interface					

VM information includes the following for each Virtual Machine (VM):

- State of the Virtual Machine (~ indicates the VM is inactive/idle)
- IP address
- MAC address
- Index number assigned to the VM
- Server port on which the VM was detected
- VM group that contains the VM, if applicable
- VM Check status for the corresponding VM

## VM Check Information

The following command displays VM Check information:

```
show virt vmcheck
```

**Command mode:** All

```
Action to take for spoofed VMs:  
    Basic: Oper disable the link  
    Advanced: Install ACL to drop traffic  
  
Maximum number of acls that can be used for mac spoofing: 50  
Trusted ports by configuration: empty
```

## VM Group Information

The following command displays VM Group parameters:

```
show virt vmgroup [<1-4096>]
```

**Command mode:** All

```
VM group 1 current configuration:
Current VM group's secure mode: Disabled
Current Group Ports: 13 17
Current Group vPorts: : empty
VLAN: 2
Tagging/Trunk-mode: Disabled
Current GROUP VMAP Config is empty
```

## VM Bandwidth Information

The following command displays VM bandwidth management parameters:

```
show virt vmpolicy vmbwidth
```

**Command mode:** All

```
Bandwidth Profile for VM 00:50:56:a5:32:f7 is enabled.
-----
TX:
  Rate:           1024
  Burst:          2048
  ACL:            127
```

## VM Profile Information

The following command displays VM Profile parameters:

```
show virt vmprofile
```

**Command mode:** All

```
VM profile "test30":
  VLAN ID: 30
  Traffic shaping not enabled.
  VM Groups: 30
```



## VMware Information

Use these commands to display information about Virtual Machines (VMs) and VMware hosts in the data center. These commands require the presence of a configured Virtual Center.

**Table 73.** *VMware Information Options*

<b>Command Syntax and Usage</b>
<b>show virt vmware hosts</b> Displays a list of VMware hosts. For a sample output, see <a href="#">page 175</a> . <b>Command mode:</b> All
<b>show virt vmware hello</b> Displays VMware hello settings. For a sample output, see <a href="#">page 174</a> . <b>Command mode:</b> All
<b>show virt vmware showhost {&lt;host UUID&gt; &lt;host IP address&gt; &lt;host name&gt;}</b> Displays detailed information about a specific VMware host. For a sample output, see <a href="#">page 175</a> . <b>Command mode:</b> All
<b>show virt vmware showvm {&lt;VM UUID&gt; &lt;VM IP address&gt; &lt;VM name&gt;}</b> Displays detailed information about a specific Virtual Machine (VM). For a sample output, see <a href="#">page 172</a> . <b>Command mode:</b> All
<b>show virt vmware switchport-mapping</b> Displays ESX Server - switchport mapping. For a sample output, see <a href="#">page 172</a> . <b>Command mode:</b> All
<b>show virt vmware vms</b> Displays a list of VMs. For a sample output, see <a href="#">page 172</a> . <b>Command mode:</b> All

## VMware Hello Information

The following command displays VM hello parameters:

```
show virt vmware hello
```

**Command mode:** All

```
Current Settings:  
Hello Disabled  
Hello timer: 23 seconds  
Hello ports: 13  
Hello address: 10.36.30.1
```

## VMware Host Information

The following command displays VM host information:

```
show virt vmware hosts
```

**Command mode:** All

UUID	Name(s), IP Address
80a42681-d0e5-5910-a0bf-bd23bd3f7803	127.12.41.30
3c2e063c-153c-dd11-8b32-a78dd1909a69	127.12.46.10
64f1fe30-143c-dd11-84f2-a8ba2cd7ae40	127.12.44.50
c818938e-143c-dd11-9f7a-d8defa4b83bf	127.12.46.20
fc719af0-093c-dd11-95be-b0adac1bcf86	127.12.46.30
009a581a-143c-dd11-be4c-c9fb65ff04ec	127.12.46.40

VM host information includes the following:

- UUID associated with the VMware host.
- Name or IP address of the VMware host.

The following command displays information for a specific VM host:

```
show virt vmware showhost {<host UUID>|<host IP address>|<host name>}
```

**Command mode:** All

```
Vswitches available on the host:

    vSwitch0
    vSwitch1

Host physical nics:

Device      vSwitch          MAC Address
-----
vmnic0      None             5c:f3:fc:49:f0:e4
vmnic1      vSwitch0        5c:f3:fc:49:f0:e6
vmnic2      None             00:00:c9:da:f5:d8
vmnic3      vSwitch1        00:00:c9:da:f5:dc
vusb0       None             5e:f3:fc:4f:f0:e7

Port Groups and their vSwitches on the host:

    Lenovo_test          vSwitch0
    VM Network           vSwitch0
    Management Network   vSwitch0
    Lenovo_Default       vSwitch1
    Lenovo_test30        vSwitch1
    Lenovo_test40        vSwitch1
    VM Network 2         vSwitch1
    Lenovo_test50        vSwitch1
    Lenovo_unu           vSwitch1

Detailed information about host and VM interfaces on this hypervisor:
-----
MAC Address      5c:f3:fc:49:f0:e6
Port             N/A
Type            VM Kernel
IP Address       10.241.32.131
Host Name        10.241.32.131
Host UUID        cab9df06-8fd7-3ecf-a4ba-f373ed60ad9d
vSwitch         vSwitch0
Port Group       Management Network
VLAN ID          0
...
```

## VMware VM Information

The following command displays information for a specific Virtual Machine (VM):

```
show virt vmware showvm {<VM UUID>|<VM IP address>|<VM name>}
```

**Command mode:** All

MAC Address	00:50:56:a5:32:f7
Port	23
Type	Virtual Machine
VM vCenter Name	arch131_nfs_3
VM OS hostname	Not Available
VM IP Address	3.3.3.2
VM UUID	422547ad-0ef7-5992-1184-63aa9030377e
Current VM Host	10.241.32.131
vSwitch	vSwitch1
Port Group	Lenovo_Default
VLAN ID	0

The following command displays the UUIDs and the names of all the VMware VMs:

```
show virt vmware vms
```

**Command mode:** All

Rescanning data center. Please wait.	
UUID	Name(s), IP Address
-----	
42312c26-2a75-c05b-eed2-6d837ac46fdd	SNSC
4225801c-dfdb-061d-65e4-4e4860d6fbcf	arch2_06
42253440-6de7-7416-8a29-fb462114ead0	arch2_05
422f49df-bf88-e4d5-6cee-047a626029aa	arch2_4_clone
4225a4f2-3422-038f-77b5-6134f5fd00b6	arch_clone
422fddf6-b9c3-fb52-9eed-fb7ccab48ab8	WIN_iperf
422573e7-f2a1-373a-87ec-7f78d8313cca	linux
422f08f6-c3b1-a641-a44a-f2698a850f3c	IxVM008, localhost, 10.241.30.208
422f15d2-5e6e-88ef-689e-9af8e4c69c34	IxVM007, localhost, 10.241.30.207
422f54d3-55b5-3731-e8f1-62abac8a0911	IxVM006, localhost, 10.241.30.206
422f42d0-329e-aec2-99c8-2724aa26db7a	IxVM005, localhost, 10.241.30.205
...	

VMware VM information includes the following:

- UUID associated with the VMware VM.
- Name or IP address of the VMware VM.

## ESX Server - Switchport Mapping

The following command displays ESX Server - switchport mapping:

```
show virt vmware switchport-mapping
```

**Command mode:** All

ST 5 ==> 10.241.32.133 vmnic4
ST 5 ==> 10.241.32.133 vmnic5
23 ==> 10.241.32.131 vmnic3

---

## EVB Information

The following commands display Edge Virtual Bridge (EVB) Virtual Station Interface (VDP) discovery and configuration information.

**Table 74.** *EVB Information Options*

Command Syntax and Usage
<b>show virt evb profile [ports]</b> Displays all EVB profile parameters. The <code>ports</code> option also display port parameters. <b>Command mode:</b> All
<b>show virt evb profile &lt;1-16&gt; [ports]</b> Displays the selected EVB profile parameters. The <code>ports</code> option also display port parameters. <b>Command mode:</b> All
<b>show virt evb vdp vm</b> Displays all active Virtual Machines (VMs). For a sample output, see <a href="#">page 175</a> . <b>Command mode:</b> All
<b>show virt evb vdp tlv</b> Displays all active Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) type-length-values (TLVs). <b>Command mode:</b> All
<b>show virt evb vsidb &lt;VSI_database_number&gt;</b> Displays Virtual Station Interface database information. <b>Command mode:</b> All
<b>show virt evb vsitypes [mgrid &lt;0-255&gt; typeid &lt;1-16777215&gt;   version &lt;0-255&gt;]</b> Displays the current Virtual Station Interface Type database parameters. For a sample output, see <a href="#">page 174</a> . <b>Command mode:</b> All

## EVB VSIType Information

The following command displays VSITypes database parameters:

```
show virt evb vsitypes
```

**Command mode:** All

```
Time Since Last Poll: 0 days 0 hours 0 minutes 14 seconds
Time Since Last Update: 14 days 16 hours 29 minutes 18 seconds

Total number of VSIType entries : 69

INDEX : 1
-----
Name :
Type ID : 9
Version : 1
Manager ID : 1
VLAN : 9, 50
TxRate : 10000000
TxBurst : 64
RxRate : 10000000
RxBurst : 64
ACL Index: 1
    SRC MAC : 00:00:00:00:00:00
    SRC MAC MASK : 00:00:00:00:00:00
    DST MAC : ff:ff:ff:ff:ff:ff
    DST MAC MASK : ff:ff:ff:ff:ff:ff
    VLAN : 0 (0x000)
    Ether Type : 0x0800 (IPv4)
    SRC IP : 0.0.0.0
    SRC IP MASK : 0.0.0.0
    DST IP : 0.0.0.0
    DST IP MASK : 0.0.0.0
    TOS : 0 (0x00)
    ACL Action : deny
ACL Index: 2
    SRC MAC : 00:00:00:00:00:00
    SRC MAC MASK : 00:00:00:00:00:00
    DST MAC : ff:ff:ff:ff:ff:ff
    DST MAC MASK : ff:ff:ff:ff:ff:ff
    VLAN : 0 (0x000)
    Ether Type : 0x0000
    ACL Action : permit
...

INDEX : 2
-----
Name :
Type ID : 20
Version : 1
Manager ID : 1
VLAN : 10, 11, 12, 13, 14, 15, 16, 20
TxRate : 10000000
TxBurst : 64
RxRate : 10000000
RxBurst : 64
```

```

ACL Index: 1
    SRC MAC : 00:00:00:00:00:00
    SRC MAC MASK : 00:00:00:00:00:00
    DST MAC : ff:ff:ff:ff:ff:ff
    DST MAC MASK : ff:ff:ff:ff:ff:ff
    VLAN : 0 (0x000)
    Ether Type : 0x0800 (IPv4)
    SRC IP : 0.0.0.0
    SRC IP MASK : 0.0.0.0
    DST IP : 0.0.0.0
    DST IP MASK : 0.0.0.0
    TOS : 0 (0x00)
    ACL Action : deny
ACL Index: 2
    SRC MAC : 00:00:00:00:00:00
    SRC MAC MASK : 00:00:00:00:00:00
    DST MAC : ff:ff:ff:ff:ff:ff
    DST MAC MASK : ff:ff:ff:ff:ff:ff
    VLAN : 0 (0x000)
    Ether Type : 0x0000
    ACL Action : permit

```

***EVB VMs Information***

The following command displays all active VMs:

```
show virt evb vdp vm
```

**Command mode:** All

```

Total number of VM Association entries : 2
TypeId      MAC          Vlan Port TxACL RxEntry ACLs
-----
9           00:50:56:95:30:ec 50  13.1 250    251 252 253 254 255 256
70          00:50:56:a5:6e:e7 70  13.1 232    226 227 228 229 230 231

```

---

## vNIC Information

The following commands display information about Virtual NICs (vNICs).

**Table 75.** *vNIC Information Options*

<b>Command Syntax and Usage</b>
<b>show vnic information-dump</b> Displays all vNIC information. <b>Command mode:</b> All
<b>show vnic vnic</b> Displays information about each vNIC. <b>Command mode:</b> All
<b>show vnic vnicgroup &lt;1-32&gt;</b> Displays information about each vNIC Group, including: <ul style="list-style-type: none"><li>o Status (enabled or disabled)</li><li>o VLAN assigned to the vNIC Group</li><li>o Uplink Failover status (enabled or disabled)</li><li>o Link status for each vNIC (up, down, or disabled)</li><li>o Port link status for each port associated with the vNIC Group (up, down, or disabled)</li></ul> <b>Command mode:</b> All



## Virtual NIC (vNIC) Information

The following command displays Virtual NIC (vNIC) information:

**show vnic vnic**

**Command mode:** All

vNIC	vNICGroup	Vlan	MaxBandwidth	Type	MACAddress	Link
INTA1.1	1	100	25	Default	00:00:c9:c6:d0:2a	up
INTA1.2	#	*	0	FCoE	00:00:c9:c6:d0:2b	up
INTA1.3	3	300	25	Default	00:00:c9:c6:d0:2c	up
INTA1.4	4	400	25	Default	00:00:c9:c6:d0:2d	up
INTA2.1	1	100	25	Default	00:00:c9:c6:cf:72	up
INTA2.2	#	*	0	FCoE	00:00:c9:c6:cf:73	up
INTA2.3	3	300	25	Default	00:00:c9:c6:cf:74	up
INTA2.4	4	400	25	Default	00:00:c9:c6:cf:75	up
INTA3.1	1	100	25	Default	00:00:c9:e3:09:5c	up
INTA3.3	3	300	25	Default	00:00:c9:e3:09:5e	up
INTA3.4	4	400	25	Default	00:00:c9:e3:09:5f	up
INTA4.2	#	*	0	FCoE	00:00:c9:b2:55:6f	up
INTA9.2	#	*	0	FCoE	00:00:c9:c6:cf:33	up

# = Not added to any vNIC group  
\* = Not added to any vNIC group or no vlan set for its vNIC group

vNIC information includes the following for each vNIC:

- vNIC ID
- vNIC Group that contains the vNIC
- VLAN assigned to the vNIC Group
- Maximum bandwidth allocated to the vNIC
- MAC address of the vNIC, if applicable
- Link status (up, down, or disabled)

## vNIC Group Information

The following command displays vNIC Group information:

**show vnic vnicgroup** <1-32>

**Command mode:** All

```
vNIC Group 1: enabled
-----
VLAN          : 100
Failover      : disabled

vNIC          Link
-----
INTA1.1      up
INTA2.1      up
INTA3.1      up

Port          Link
-----

UplinkPort    Link
-----
EXT6          up
```

vNIC Group information includes the following for each vNIC Group:

- Status (enabled or disabled)
- VLAN assigned to the vNIC Group
- Uplink Failover status (enabled or disabled)
- Link status for each vNIC (up, down, or disabled)
- Port link status for each port associated with the vNIC Group (up, down, or disabled)

---

## SLP Information

The following commands display information about Service Location Protocol settings:

**Table 76.** *SLP Information Options*

<b>Command Syntax and Usage</b>
<b>show ip slp directory-agents</b> Lists all detected Directory Agents (DAs). <b>Command mode:</b> All
<b>show ip slp information</b> Displays the SLP version, whether SLP is enabled or disabled and whether DA auto-discovery is enabled or disabled. <b>Command mode:</b> All
<b>show ip slp user-agents</b> Lists all detected User Agents (UAs). <b>Command mode:</b> All

## UFP Information

The following commands display information about Unified Fabric Port (UFP) settings.

**Table 77.** *UFP Information Options*

Command Syntax and Usage
<p><b>show ufp [port &lt;port_no.&gt;] [vport &lt;1-8&gt;] [network qos evb]</b></p> <p>Displays the UFP network and QoS settings applied on all ports or on specified physical and virtual ports.</p> <ul style="list-style-type: none"><li>o network filters only UFP network settings</li><li>o qos filters only QoS network settings</li><li>o evb filters only EVB profile settings</li></ul> <p><b>Command mode:</b> All</p>
<p><b>show ufp information {cdcp qos tlvstat} [port &lt;port_no.&gt;]</b></p> <p>Displays global or port-specific UFP information on:</p> <ul style="list-style-type: none"><li>o cdcp displays S-Channel Discovery and Configuration Protocol (CDCP) information. CDCP allows hypervisor hosts to create on-demand S-channels with the switch. For details, see <a href="#">page 182</a>.</li><li>o qos displays bandwidth allocation between virtual ports. For details, see <a href="#">page 182</a>.</li><li>o tlvstat displays status for Type-Length-Values transmitted on UFP-enabled physical ports. For details, see <a href="#">page 183</a>.</li></ul> <p><b>Command mode:</b> All</p>
<p><b>show ufp information getvlan &lt;2-4094&gt;</b></p> <p>Displays state, operating mode and VLAN related information for physical and virtual ports associated to a specified VLAN ID.</p> <p><b>Command mode:</b> All</p>
<p><b>show ufp information port [&lt;port_no.&gt;]</b></p> <p>Displays UFP status for all physical ports or only for a specified physical port. Information includes whether the UFP is enabled on the physical port, how many virtual ports are enabled and the link stats for each virtual port. For details, see <a href="#">page 181</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show ufp information qos [port &lt;port_no.&gt;] [vport &lt;1-8&gt;]</b></p> <p>Displays bandwidth allocation between virtual ports for all physical ports or specified physical and virtual ports. For details, see <a href="#">page 182</a>.</p> <p><b>Command mode:</b> All</p>

**Table 77.** UFP Information Options

Command Syntax and Usage
<b>show ufp information vport [port &lt;port_no.&gt;] [vport &lt;1-8&gt;]</b> Displays state, operating mode and VLAN related information for all virtual ports, for virtual ports belonging to a specified physical port or for a single virtual port. For details, see <a href="#">page 184</a> . <b>Command mode:</b> All
<b>show ufp information vlan [&lt;1-4094&gt;]</b> Displays ports and vports associated to all configured VLANs or to a specified VLAN ID. For details, see <a href="#">page 185</a> . <b>Command mode:</b> All

## Port Information

The following command displays UFP port information:

**show ufp information port**

**Command mode:** All

Alias	Port	state	vPorts	link up	link down	mismatch	disabled
INTA4	4	ena	4	1 3 4		2	

Port information includes the following for each physical port:

- Port alias
- Port number
- UFP state
- Number of virtual ports enabled
- Link status on each channel (up, down or disabled)

## CDCP Information

The following command displays S-Channel Discovery and Configuration Protocol information:

**show ufp information cdc**

**Command mode:** All

```
INT1  : Channel Request
INT2  : Channel Request
INT3  : TxSVIDs
INT4  : TxSVIDs
INT5  : Disable
INT6  : Disable
INT7  : Disable
INT8  : Disable
INT9  : Disable
INT10 : Disable
INT11 : Disable
INT12 : Disable
INT13 : Disable
INT14 : Disable
```

CDCP information includes the following for each physical port:

- Whether there is a channel set up
- CDCP communication status for active channels

## QoS Information

The following command displays Quality of Service information:

**show ufp information qos**

**Command mode:** All

```
Global UFP QoS mode: UFP QoS BW

Port | Vport | Mode | Minbw% | Maxbw% | Prio | HstCtrl
-----|-----|-----|-----|-----|-----|-----
INTA6 | 3     | ETS  |         |         | 3    | Dis
      | 4     | ETS  |         |         | 0    | Dis
-----|-----|-----|-----|-----|-----|-----
INTA8 | 1     | BW   | 30      | 100    |      | 
      | 2     | BW   | 30      | 100    |      | 
      | 3     | BW   | 10      | 100    |      | 
      | 4     | BW   | 10      | 100    |      | 
-----|-----|-----|-----|-----|-----|-----
INTA10| 1     | ETS  |         |         | 0    | Dis
      | 2     | ETS  |         |         | 3    | Dis
      | 3     | ETS  |         |         | 2    | Dis
      | 4     | ETS  |         |         | 0    | Dis
      | 5     | ETS  |         |         | 4    | Dis
      | 6     | ETS  |         |         | 5    | Dis
      | 7     | ETS  |         |         | 6    | Dis
      | 8     | ETS  |         |         | 7    | Dis
...  
```

QoS information includes the following:

- Physical port number
- Virtual port number
- Minimum guaranteed bandwidth allocated
- Maximum bandwidth achievable
- ETS or Bandwidth mode
- 802.1p priority associated to the vport
- Host control

## TLV Status Information

The following command displays Type-Length-Values information:

**show ufp information tlvstat**

**Command mode:** All

INT1	:	Success
INT2	:	Success
INT3	:	Disabled
INT4	:	Disabled
INT5	:	Disabled
INT6	:	Disabled
INT7	:	Disabled
INT8	:	Disabled
INT9	:	Disabled
INT10	:	Disabled
INT11	:	Disabled
INT12	:	Disabled
INT13	:	Disabled
INT14	:	Disabled

TLV status information includes the following:

- Physical port alias
- Type-Length-Values status

## Virtual Port Information

The following command displays virtual port information:

```
show ufp information vport
```

**Command mode:** All

vPort	state	mode	svid	defvlan	deftag	evb	VLANs
INTA1.1	dis	tunnel	0	0	dis	dis	
INTA1.2	dis	tunnel	0	0	dis	dis	
INTA1.3	dis	tunnel	0	0	dis	dis	
INTA1.4	dis	tunnel	0	0	dis	dis	
...							
INTA14.4	dis	tunnel	0	0	dis	dis	
INTB1.1	dis*	access	4002	100	dis	dis	100
INTB1.2	up	fcoe	2500	2500	dis	dis	2500
INTB1.3	dis*	trunk	4004	300	dis	dis	300 500
INTB1.4	dis	tunnel	0	0	dis	dis	
INTB2.1	dis*	access	4002	100	dis	dis	100
INTB2.2	up	fcoe	2500	2500	dis	dis	2500
INTB2.3	dis*	trunk	4004	300	dis	dis	300 500
INTB2.4	dis	tunnel	0	0	dis	dis	
INTB3.1	dis*	access	4002	100	dis	dis	100
INTB3.2	up	fcoe	2500	2500	dis	dis	2500
INTB3.3	dis*	trunk	4004	300	dis	dis	300 500
INTB3.4	dis	tunnel	0	0	dis	dis	

Virtual port information includes the following for each virtual port:

- Virtual port number
- Channel status
- Operating mode (trunk, access, tunnel, auto or FCoE)
- S-channel VLAN ID
- Default VLAN ID
- Default VLAN ID tagging enforcement
- EVB profile
- VLANs the virtual port is associated with



## VLAN Information

The following command displays VLAN information:

**show ufp information vlan**

**Command mode:** All

```
VLAN
----
 100

vPort list:
  INTB1.1  INTB2.1  INTB3.1  INTB4.1  INTB5.1  INTB6.1
  INTB7.1  INTB8.1  INTB9.1  INTB10.1 INTB11.1 INTB12.1

EXT Port list:
  EXT3     EXT4     EXT8     EXT9

INT Port list:
  INTB13

UFP Port list:
  INTB1  INTB2  INTB3  INTB4  INTB5  INTB6  INTB7  INTB8
  INTB9  INTB10 INTB11 INTB12

VMR Port list:
```

VLAN information includes the following for each VLAN:

- VLAN ID
- Associated virtual ports
- Associated external ports
- Associated internal ports
- Associated UFP ports

## TLV Information

The following commands display TLV information:

```
show ufp {receive|transmit} cap port <port_no.>
```

**Command mode:** All

```
UFP Capability Discovery TLV Received on port INT2:
  tlv      : Type 127 Length 7 OUI 00-18-b1 Subtype 1
  version  : Max 1 Oper 1
  cna      : Req 1 Oper 1 Res 0x00
  switch   : Cap 1 Oper 1 Res 0x00
```

UFP Capability Discovery TLV information includes the following:

- TLV type and length
- Lenovo Organizationally Unique Identifier
- TLV Subtype
- Max Version and Operation Version
- UFP CNA Status which include UFP Request and UFP Operation
- UFP Switch Status which includes UFP Capable and UFP Operation

```
show ufp {receive|transmit} cdcv port <port_no.>
```

**Command mode:** All

```
CDCV TLV Transmitted on port INT2:
  tlv      : Type 127 Length 23 OUI 00-80-c2 Subtype 14
  local    : Role 0 SComp 1 Channel Cap 5
  SCID 1   : SVID 1
  SCID 2   : SVID 4002
  SCID 3   : SVID 4003
  SCID 4   : SVID 0
  SCID 5   : SVID 0
```

UFP Channel Discovery and Configuration Protocol TLV includes the following:

- TLV type and length
- Lenovo Organizationally Unique Identifier
- TLV Subtype
- Role bit
- S-Component bit
- Channel Cap
- Corresponding index/SVID pairs

**show ufp transmit linkdown port** <port alias or number>

**Command mode:** All

```
UFP LINK-DOWN TLV transmitted on port INTA8:
Header  : Type 2 Length 3 Flags 0x0 Status 0x0
SCID   : 5
```

**show ufp receive linkup port** <port alias or number>

**Command mode:** All

```
UFP LINK-UP TLV received on port INTA9:
Header  : Type 3 Length 4 Flags 0x1 Status 0x0
SCID   : 6 9
```

**show ufp receive prop port** <port alias or number>

**Command mode:** All

```
UFP NIC-PROPS TLV transmitted on port INTA9:
Header  : Type 1 Length 17 Flags 0x0 Status 0x0
Props   : Channel Type 1 SCHED Type 0 Res 0x0 Num VLAN 0
SCID 6 SVID 4006 iSCSI 0 Host Pri 0 FCoE 0 TC 7 Min BW 0 Max BW
0
SCID 9 SVID 4009 iSCSI 0 Host Pri 0 FCoE 0 TC 2 Min BW 0 Max BW
0
```

---

## DCBX Information Commands

The following commands display DCBX information.

**Table 78.** *DCBX Information Commands*

Command Syntax and Usage
<b>show dcbx receive</b> <port alias or number> Displays the Type-Length-Value (TLV) list received in the DCBX TLV. <b>Command mode:</b> All
<b>show dcbx transmit</b> <port alias or number> Displays the Type-Length-Value (TLV) list transmitted in the DCBX TLV. <b>Command mode:</b> All

---

## Converged Enhanced Ethernet Information

Table 79 describes the Converged Enhanced Ethernet (CEE) information options.

**Table 79.** *CEE Information Options*

Command Syntax and Usage
<b>show cee global {ets pfc} [information]</b> Displays global ETS or PFC information. <b>Command mode:</b> All
<b>show cee [information]</b> Displays all CEE information. <b>Command mode:</b> All
<b>show cee iscsi</b> Displays the current ISCSI TLV parameters. <b>Command mode:</b> All
<b>show cee port &lt;port alias or number&gt;</b> Displays CEE information for the specified port. <b>Command mode:</b> All

## DCBX Information

[Table 80](#) describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

**Table 80.** *DCBX Information Options*

Command Syntax and Usage
<b>show cee information dcbx port</b> <i>&lt;port alias or number&gt;</i> Displays all DCBX information. <b>Command mode:</b> All
<b>show cee information dcbx port</b> <i>&lt;port alias or number&gt;</i> <b>app_proto</b> Displays information about the DCBX Application Protocol state machine on the selected port. For details, see <a href="#">page 195</a> . <b>Command mode:</b> All
<b>show cee information dcbx port</b> <i>&lt;port alias or number&gt;</i> <b>control</b> Displays information about the DCBX Control state machine for the selected port. For details, see <a href="#">page 191</a> . <b>Command mode:</b> All
<b>show cee information dcbx port</b> <i>&lt;port alias or number&gt;</i> <b>ets</b> Displays information about the DCBX ETS state machine. For details, see <a href="#">page 193</a> . <b>Command mode:</b> All
<b>show cee information dcbx port</b> <i>&lt;port alias or number&gt;</i> <b>feature</b> Displays information about the DCBX Feature state machine for the selected port. For details, see <a href="#">page 192</a> . <b>Command mode:</b> All
<b>show cee information dcbx port</b> <i>&lt;port alias or number&gt;</i> <b>pfc</b> Displays information about the DCBX PFC state machine. For details, see <a href="#">page 194</a> . <b>Command mode:</b> All

## DCBX Control Information

The following command displays DCBX control information:

```
show cee information dcbx port <port alias or number> control
```

**Command mode:** All

DCBX Port Control State-machine Info						
=====						
Alias	Port	OperStatus	OperVer	MaxVer	SeqNo	AckNo
-----						
INTA1	1	enabled	0	0	0	0
INTA2	2	enabled	0	0	4	2
INTA3	3	enabled	0	0	0	0
INTA4	4	enabled	0	0	1	1
...						

DCBX control information includes the following:

- Port alias and number
- DCBX status (enabled or disabled)
- Operating version negotiated with the peer device
- Maximum operating version supported by the system
- Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes
- Sequence number of the most recent DCB feature TLV that has been acknowledged

## DCBX Feature Information

The following command displays DCBX feature information:

**show cee information dcbx port** <port alias or number> **feature**

**Command mode:** All

```

DCBX Port Feature State-machine Info
=====
Alias  Port  Type   AdmState Will  Advrt OpVer  MxVer PrWill SeqNo Err OperMode Syncd
-----
INTA2  2     ETS    enabled No   Yes   0     0     Yes   1    No  enabled  Yes
INTA2  2     PFC    enabled No   Yes   0     0     Yes   1    No  enabled  Yes
INTA2  2     AppProt disabled No   Yes   0     0     Yes   1    No  disabled Yes
...

```

The following table describes the DCBX feature information.

**Table 81.** DCBX Feature Information Fields

Parameter	Description
Alias	Displays each port's alias.
Port	Displays each port's number.
Type	Feature type.
AdmState	Feature status (Enabled or Disabled).
Will	Willing flag status (Yes/True or No/Untrue).
Advrt	Advertisement flag status (Yes/True or No/Untrue).
OpVer	Operating version negotiated with the peer device.
MxVer	Maximum operating version supported by the system.
PrWill	Peer's Willing flag status (Yes/True or No/Untrue).
SeqNo	Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes.
Err	Error condition flag (Yes or No). Yes indicates that an error occurred during the exchange of configuration data with the peer.
OperMode	Operating status negotiated with the peer device (enabled or disabled).
Syncd	Synchronization status between this port and the peer (Yes or No).



## DCBX ETS Information

The following command displays DCBX ETS information:

```
show cee information dcbx port <port alias or number> ets
```

**Command mode:** All

```

DCBX Port Priority Group - Priority Allocation Table
=====
Alias  Port  Priority  PgIdDes  PgIdOper  PgIdPeer
-----
INTA2  2    0         PGID0    PGID0     PGID0
INTA2  2    1         PGID0    PGID0     PGID0
INTA2  2    2         PGID0    PGID0     PGID0
INTA2  2    3         PGID1    PGID1     PGID1
INTA2  2    4         PGID2    PGID2     PGID0
INTA2  2    5         PGID2    PGID2     PGID0
INTA2  2    6         PGID2    PGID2     PGID0
INTA2  2    7         PGID2    PGID2     PGID0

DCBX Port Priority Group - Bandwidth Allocation Table
=====
Alias  Port  PrioGrp  BwDes  BwOper  BwPeer
-----
INTA2  2    0         10    10     50
INTA2  2    1         50    50     50
INTA2  2    2         40    40     0

```

The following table describes the DCBX ETS information.

**Table 82.** DCBX Feature Information Fields

Parameter	Description
<b>DCBX Port Priority Group - Priority Allocation Table</b>	
Alias	Displays each port's alias.
Port	Displays each port's number.
PgIdDes	Priority Group ID configured on this switch.
PgIdOper	Priority Group negotiated with the peer (operating Priority Group).
PgIdPeer	Priority Group ID configured on the peer.
<b>DCBX Port Priority Group - Bandwidth Allocation Table</b>	
BwDes	Bandwidth allocation configured on this switch.
BwOper	Bandwidth allocation negotiated with the peer (operating bandwidth).
BwPeer	Bandwidth allocation configured on the peer.

## DCBX PFC Information

The following command displays DCBX Priority Flow Control (PFC) information:

```
show cee information dcbx port <port alias or number> pfc
```

**Command mode:** All

DCBX Port Priority Flow Control Table					
Alias	Port	Priority	EnableDesr	EnableOper	EnablePeer
INTA2	2	0	disabled	disabled	disabled
INTA2	2	1	disabled	disabled	disabled
INTA2	2	2	disabled	disabled	disabled
INTA2	2	3	enabled	enabled	enabled
INTA2	2	4	disabled	disabled	disabled
INTA2	2	5	disabled	disabled	disabled
INTA2	2	6	disabled	disabled	disabled
INTA2	2	7	disabled	disabled	disabled

DCBX PFC information includes the following:

- Port alias and number
- 802.1p value
- **EnableDesr**: Status configured on this switch
- **EnableOper**: Status negotiated with the peer (operating status)
- **EnablePeer**: Status configured on the peer

## DCBX Application Protocol Information

The following command displays DCBX Application Protocol information:

**show cee information dcbx port** <port alias or number> **app-proto**

**Command mode:** All

```

DCBX Application Protocol Table
=====

FCoE Priority Information
=====
Protocol ID           : 0x8906
Selector Field       : 0
Organizationally Unique ID: 0x1b21

Alias  Port Priority EnableDesr EnableOper EnablePeer
-----
INTA2  2   0      disabled   disabled   disabled
INTA2  2   1      disabled   disabled   disabled
INTA2  2   2      disabled   disabled   disabled
INTA2  2   3      enabled    disabled   enabled
INTA2  2   4      disabled   disabled   disabled
INTA2  2   5      disabled   disabled   disabled
INTA2  2   6      disabled   disabled   disabled
INTA2  2   7      disabled   disabled   disabled

FIP Snooping Priority Information
=====
Protocol ID           : 0x8914
Selector Field       : 0
Organizationally Unique ID: 0x1b21

Alias  Port Priority EnableDesr EnableOper EnablePeer
-----
INTA2  2   0      disabled   disabled   disabled
INTA2  2   1      disabled   disabled   disabled
INTA2  2   2      disabled   disabled   disabled
INTA2  2   3      enabled    disabled   disabled
INTA2  2   4      disabled   disabled   disabled
INTA2  2   5      disabled   disabled   disabled
INTA2  2   6      disabled   disabled   disabled
INTA2  2   7      disabled   disabled   disabled

```

The following table describes the DCBX Application Protocol information.

**Table 83.** DCBX Application Protocol Information Fields

Parameter	Description
Protocol ID	Identifies the supported Application Protocol.
Selector Field	Specifies the Application Protocol type, as follows: <ul style="list-style-type: none"> <li>o 0 = Ethernet Type</li> <li>o 1 = TCP socket ID</li> </ul>
Organizationally Unique ID	DCBX TLV identifier

**Table 83.** *DCBX Application Protocol Information Fields (continued)*

<b>Parameter</b>	<b>Description</b>
Alias	Port alias
Port	Port number
Priority	802.1p value
EnableDesr	Status configured on this switch
EnableOper	Status negotiated with the peer (operating status)
EnablePeer	Status configured on the peer

## ETS Information

Table 84 describes the Enhanced Transmission Selection (ETS) information options.

**Table 84.** *ETS Information Options*

Command Syntax and Usage
<p><b>show cee global ets [information]</b>            Displays global ETS information.  <b>Command mode:</b> All</p>
<p><b>show cee global ets priority-group &lt;0-7, 15&gt;</b>            Displays the current global ETS Priority Group parameters.  <b>Command mode:</b> All</p>

The following command displays ETS information:

**show cee global ets information**

**Command mode:** All

Global ETS information:		
Number of COSq: 8		
Mapping of 802.1p Priority to Priority Groups:		
Priority	PGID	COSq
-----	----	----
0	0	0
1	0	0
2	0	0
3	1	1
4	2	2
5	2	2
6	2	2
7	2	2
Bandwidth Allocation to Priority Groups:		
PGID	PG%	Description
----	----	-----
0	10	
1	50	
2	40	

Enhanced Transmission Selection (ETS) information includes the following:

- Number of Class of Service queues (COSq) configured
- 802.1p mapping to Priority Groups and Class of Service queues
- Bandwidth allocated to each Priority Group

## PFC Information

[Table 85](#) describes the Priority Flow Control (PFC) information options.

**Table 85.** *PFC Information Options*

Command Syntax and Usage
<p><b>show cee global pfc [information]</b>            Displays global PFC information.  <b>Command mode:</b> All</p>
<p><b>show cee global pfc priority &lt;priority value&gt;</b>            Displays the current global PFC 802.1p priority parameters.  <b>Command mode:</b> All</p>
<p><b>show cee port &lt;port alias or number&gt; pfc [information]</b>            Displays PFC information on the specified port.  <b>Command mode:</b> All</p>
<p><b>show cee port &lt;port alias or number&gt; pfc priority &lt;priority value&gt;</b>            Displays the current PFC 802.1p priority parameters for the specified port.  <b>Command mode:</b> All</p>

The following command displays PFC information for a port:

**show cee port <port alias or number> pfc information**

**Command mode:** All

Global PFC Information:		
PFC - ON		
Priority	State	Description
-----	-----	-----
0	Dis	
1	Dis	
2	Dis	
3	Ena	
4	Dis	
5	Dis	
6	Dis	
7	Dis	
-----		
State - indicates whether PFC is Enabled/Disabled on a particular priority		

---

## FCoE Information

Table 86 describes the Fibre Channel over Ethernet (FCoE) information options.

**Table 86.** *FCoE Information Options*

Command Syntax and Usage
<b>show fcoe information</b> Displays all current FCoE information. <b>Command mode:</b> All

## FIP Snooping Information

Table 87 describes the Fibre Channel Initialization Protocol (FIP) Snooping information options.

**Table 87.** *FIP Snooping Information Options*

Command Syntax and Usage
<b>show fcoe fips [information]</b> Displays FIP Snooping information for all ports. <b>Command mode:</b> All
<b>show fcoe fips fcf</b> Displays FCF information for all FCFs learned. <b>Command mode:</b> All
<b>show fcoe fips fcoe</b> Displays FCoE connections established on the switch. <b>Command mode:</b> All
<b>show fcoe fips port &lt;port alias or number&gt; [information]</b> Displays FIP Snooping (FIPS) information for the selected port, including a list of current FIPS ACLs. <b>Command mode:</b> All
<b>show fcoe fips vlans</b> Displays VLAN information. <b>Command mode:</b> All

The following command displays FIP Snooping information for the selected port:

**show fcoe fips port** *<port alias or number>* **information**

**Command mode:** All

```
FIP Snooping on port INTA2:
This port has been configured to automatically detect FCF.
It has currently detected to have 0 FCF connecting to it.
FIPS ACLs configured on this port:
SMAC 00:c0:dd:13:9b:6f, action deny.
SMAC 00:c0:dd:13:9b:70, action deny.
SMAC 00:c0:dd:13:9b:6d, action deny.
SMAC 00:c0:dd:13:9b:6e, action deny.
DMAC 00:c0:dd:13:9b:6f, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:70, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6d, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6e, ethertype 0x8914, action permit.
SMAC 0e:fc:00:01:0a:00, DMAC 00:c0:dd:13:9b:6d, ethertype 0x8906, vlan
1002, action permit.
DMAC 01:10:18:01:00:01, Ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:02, Ethertype 0x8914, action permit.
Ethertype 0x8914, action deny.
Ethertype 0x8906, action deny.
SMAC 0e:fc:00:00:00:00, SMAC mask ff:ff:ff:00:00:00, action deny.
```

FIP Snooping port information includes the following:

- Fibre Channel Forwarding (FCF) mode
- Number of FCF links connected to the port
- List of FIP Snooping ACLs assigned to the port



---

## Information Dump

The following command dumps switch information:

**show information-dump**

**Command mode:** All

Use the dump command to dump all switch information available (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.



---

## Chapter 3. Statistics Commands

You can use the Statistics Commands to view switch performance statistics in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch statistics.

**Table 88.** *Statistics Commands*

<b>Command Syntax and Usage</b>
<p><b>show counters</b></p> <p>Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. For details, see <a href="#">page 318</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show layer3 counters</b></p> <p>Displays Layer 3 statistics.</p> <p><b>Command mode:</b> All</p>
<p><b>show ntp counters</b></p> <p>Displays Network Time Protocol (NTP) Statistics. See <a href="#">page 314</a> for a sample output and a description of NTP Statistics.</p> <p><b>Command mode:</b> All</p>
<p><b>show ptp counters</b></p> <p>Displays Precision Time Protocol (PTP) Statistics. See <a href="#">page 316</a> for a sample output and a description of PTP Statistics.</p> <p><b>Command mode:</b> All</p>
<p><b>show snmp-server counters</b></p> <p>Displays SNMP statistics. See <a href="#">page 310</a> for sample output.</p> <p><b>Command mode:</b> All</p>

---

## Forwarding Database Statistics

The following commands display Forwarding Database statistics.

**Table 89.** *Forwarding Database statistics commands*

Command Syntax and Usage
<p><b>show mac-address-table counters [all]</b></p> <p>Displays Forwarding Database (FDB) statistics. The <b>all</b> options displays all FDB statistics (unicast and multicast).</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table counters interface port</b> <i>&lt;port alias or number&gt;</i></p> <p>Displays Forwarding Database (FDB) statistics for the specified port.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table counters portchannel</b> <i>&lt;trunk group number&gt;</i></p> <p>Displays Forwarding Database (FDB) statistics for the specified trunk group.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table counters state {forward trunk unknown}</b></p> <p>Displays Forwarding Database (FDB) statistics by state:</p> <ul style="list-style-type: none"><li>o forward displays FDB statistics for forwarding state MAC address entries</li><li>o trunk displays FDB statistics for trunk state MAC address entries</li><li>o unknown displays FDB statistics for unknown state MAC address entries</li></ul> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table counters static</b></p> <p>Displays Forwarding Database (FDB) statistics for static MAC address entries.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table counters unicast</b></p> <p>Displays Forwarding Database (FDB) statistics for unicast MAC address entries.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table counters vlan</b> <i>&lt;VLAN number&gt;</i></p> <p>Displays Forwarding Database (FDB) statistics for the specified VLAN.</p> <p><b>Command mode:</b> All</p>
<p><b>clear mac-address-table counters</b></p> <p>Clears Forwarding Database (FDB) statistics.</p> <p><b>Command mode:</b> All except User EXEC</p>

---

## Port Statistics

These commands display traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

**Table 90.** *Port Statistics Commands*

Command Syntax and Usage
<b>show interface counters</b> Displays interface statistics. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; all-counters</b> Displays all statistics for the specified port. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; bridging-counters</b> Displays bridging (“dot1”) statistics for the specified port. See <a href="#">page 211</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; dot1x counters</b> Displays IEEE 802.1X statistics for the specified port. See <a href="#">page 207</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; ethernet-counters</b> Displays Ethernet (“dot3”) statistics for the specified port. See <a href="#">page 212</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; interface-counters</b> Displays interface statistics for the specified port. See <a href="#">page 215</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; ip-counters</b> Displays IP statistics for the specified port. See <a href="#">page 218</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; link-counters</b> Displays link statistics for the specified port. See <a href="#">page 218</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; link-counters oam counters</b> Displays OAM link statistics for the specified port. <b>Command mode:</b> All

**Table 90.** *Port Statistics Commands*

<b>Command Syntax and Usage</b>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>maintenance-counters</b></p> <p>Displays maintenance statistics for the specified port.</p> <p><b>Command mode:</b> All</p>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>oam counters</b></p> <p>Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port.</p> <p><b>Command mode:</b> All</p>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>ptp-counters</b></p> <p>Displays Precision Time Protocol statistics for the port. See <a href="#">page 316</a> for a sample output and a description of PTP Statistics.</p> <p><b>Command mode:</b> All</p>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>rmon-counters</b></p> <p>Displays Remote Monitoring (RMON) statistics for the port. See <a href="#">page 219</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<p><b>clear counters</b></p> <p>Clears statistics for all ports.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>clear interface port</b> <i>&lt;port alias or number&gt;</i> <b>counters</b></p> <p>Clears all statistics for the port.</p> <p><b>Command mode:</b> All except User EXEC</p>

## 802.1X Authenticator Statistics

Use the following command to display the 802.1X authenticator statistics of the selected port:

**show interface port** <port alias or number> **dot1x counters**

**Command mode:** All

Authenticator Statistics:	
eapolFramesRx	= 925
eapolFramesTx	= 3201
eapolStartFramesRx	= 2
eapolLogoffFramesRx	= 0
eapolRespIdFramesRx	= 463
eapolRespFramesRx	= 460
eapolReqIdFramesTx	= 1820
eapolReqFramesTx	= 1381
invalidEapolFramesRx	= 0
eapLengthErrorFramesRx	= 0
lastEapolFrameVersion	= 1
lastEapolFrameSource	= 00:01:02:45:ac:51

**Table 91.** 802.1X Authenticator Statistics of a Port

Statistics	Description
eapolFramesRx	Total number of EAPOL frames received.
eapolFramesTx	Total number of EAPOL frames transmitted.
eapolStartFramesRx	Total number of EAPOL Start frames received.
eapolLogoffFramesRx	Total number of EAPOL Logoff frames received.
eapolRespIdFramesRx	Total number of EAPOL Response Identity frames received.
eapolRespFramesRx	Total number of Response frames received.
eapolReqIdFramesTx	Total number of Request Identity frames transmitted.
eapolReqFramesTx	Total number of Request frames transmitted.
invalidEapolFramesRx	Total number of invalid EAPOL frames received.
eapLengthErrorFramesRx	Total number of EAP length error frames received.
lastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
lastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

## 802.1X Authenticator Diagnostics

Use the following command to display the 802.1X authenticator diagnostics of the selected port:

**show interface port** *<port alias or number>* **dot1x counters**

**Command mode:** All

Authenticator Diagnostics:	
authEntersConnecting	= 1820
authEapLogoffsWhileConnecting	= 0
authEntersAuthenticating	= 463
authSuccessesWhileAuthenticating	= 5
authTimeoutsWhileAuthenticating	= 0
authFailWhileAuthenticating	= 458
authReauthsWhileAuthenticating	= 0
authEapStartsWhileAuthenticating	= 0
authEapLogoffWhileAuthenticating	= 0
authReauthsWhileAuthenticated	= 3
authEapStartsWhileAuthenticated	= 0
authEapLogoffWhileAuthenticated	= 0
backendResponses	= 923
backendAccessChallenges	= 460
backendOtherRequestsToSupplicant	= 460
backendNonNakResponsesFromSupplicant	= 460
backendAuthSuccesses	= 5
backendAuthFails	= 458

**Table 92.** 802.1X Authenticator Diagnostics of a Port

Statistics	Description
authEntersConnecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhile Connecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
authEntersAuthenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
authSuccessesWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.



**Table 92.** 802.1X Authenticator Diagnostics of a Port (continued)

Statistics	Description
authTimeoutsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request.
authEapStartsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccessChallenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.

**Table 92.** 802.1X Authenticator Diagnostics of a Port (continued)

<b>Statistics</b>	<b>Description</b>
backendOtherRequestsToSupplicant	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.
backendNonNakResponsesFromSupplicant	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
backendAuthSuccesses	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
backendAuthFails	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

## Bridging Statistics

Use the following command to display the bridging statistics of the selected port:

**show interface port** <port alias or number> **bridging-counters**

**Command mode:** All

Bridging statistics for port INT1:	
dot1PortInFrames:	63242584
dot1PortOutFrames:	63277826
dot1PortInDiscards:	0
dot1TpLearnedEntryDiscards:	0
dot1StpPortForwardTransitions:	0

**Table 93.** *Bridging Statistics of a Port*

Statistics	Description
dot1PortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortOutFrames	The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortInDiscards	Count of valid frames received which were discarded (that is, filtered) by the Forwarding Process.
dot1TpLearnedEntry Discards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
dot1StpPortForward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

## Ethernet Statistics

Use the following command to display the ethernet statistics of the selected port:

**show interface port** <port alias or number> **ethernet-counters**

**Command mode:** All

Ethernet statistics for port INT1:	
dot3StatsAlignmentErrors:	0
dot3StatsFCSErrors:	0
dot3StatsSingleCollisionFrames:	0
dot3StatsMultipleCollisionFrames:	0
dot3StatsLateCollisions:	0
dot3StatsExcessiveCollisions:	0
dot3StatsInternalMacTransmitErrors:	NA
dot3StatsFrameTooLongs:	0
dot3StatsInternalMacReceiveErrors:	0

**Table 94.** *Ethernet Statistics for Port*

Statistics	Description
dot3StatsAlignmentErrors	<p>A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>alignmentError</code> status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsFCSErrors	<p>A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>frameCheckError</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>

**Table 94.** Ethernet Statistics for Port (continued)

Statistics	Description
dot3StatsSingleCollision Frames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsMultipleCollisionFrame</code> object.</p>
dot3StatsMultipleCollision Frames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsSingleCollisionFrames</code> object.</p>
dot3StatsLateCollisions	<p>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.</p> <p>Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.</p>
dot3StatsExcessive Collisions	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
dot3StatsInternalMac TransmitErrors	<p>A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsLateCollisions</code> object, the <code>dot3StatsExcessiveCollisions</code> object, or the <code>dot3StatsCarrierSenseErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.</p>

**Table 94.** *Ethernet Statistics for Port (continued)*

Statistics	Description
dot3StatsFrameTooLongs	<p>A count of frames received on a particular interface that exceed the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsInternalMacReceiveErrors	<p>A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsFrameTooLongs</code> object, the <code>dot3StatsAlignmentErrors</code> object, or the <code>dot3StatsFCSErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.</p>

## Interface Statistics

Use the following command to display the interface statistics of the selected port:

**show interface port** <port alias or number> **interface-counters**

**Command mode:** All

Interface statistics for port EXT1:			
	ifHCIn Counters		ifHCOut Counters
Octets:	0		648329
UcastPkts:	0		0
BroadcastPkts:	0		271
MulticastPkts:	0		7654
FlowCtrlPkts:	0		0
PriFlowCtrlPkts:	0		0
Discards:	0		11
Errors:	0		0
Ingress Discard reasons:		Egress Discard reasons:	
VLAN Discards:	0	HOL-blocking Discards:	0
Filter Discards:	0	MMU Discards:	0
Policy Discards:	0	Cell Error Discards:	0
Non-Forwarding State:	0	MMU Aging Discards:	0
IBP/CBP Discards:	0	Other Discards:	11

**Table 95.** *Interface Statistics for Port*

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
ifInMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
ifInFlowControlPkts	The total number of flow control pause packets received on the interface.
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

**Table 95.** *Interface Statistics for Port (continued)*

<b>Statistics</b>	<b>Description</b>
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of <code>ifOutBroadcastPkts</code> .
ifOutMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of <code>ifOutMulticastPkts</code> .
ifOutFlowControlPkts	The total number of flow control pause packets transmitted out of the interface.
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
VLAN Discards	Discarded because the packet was tagged with a VLAN to which this port is not a member.
Filter Discards	Dropped by the Content Aware Engine (user-configured filter).



**Table 95.** *Interface Statistics for Port (continued)*

<b>Statistics</b>	<b>Description</b>
Policy Discards	Dropped due to policy setting. For example, due to a user-configured static entry.
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).
HOL-blocking Discards	Discarded because of the Head Of Line (HOL) blocking mechanism. Low-priority packets are placed in a separate queue and can be discarded while applications or the TCP protocol determine whether a retransmission is necessary. HOL blocking forces transmission to stop until the overloaded egress port buffer can receive data again.
MMU Discards	Discarded because of the Memory Management Unit.
Cell Error Discards	
MMU Aging Discards	
Other Discards	Discarded packets not included in any category.
Empty Egress Portmap	Dropped due to an egress port bitmap of zero condition (no ports in the egress mask). This counter increments whenever the switching decision found that there was no port to send out.

## Interface Protocol Statistics

Use the following command to display the interface protocol statistics of the selected port:

**show interface port** *<port alias or number>* **ip-counters**

**Command mode:** All

```
GEA IP statistics for port INT1:
ipInReceives   :      0
ipInHeaderError:      0
ipInDiscards   :      0
```

**Table 96.** *Interface Protocol Statistics*

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHeaderErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

## Link Statistics

Use the following command to display the link statistics of the selected port:

**show interface port** *<port alias or number>* **link-counters**

**Command mode:** All

```
Link statistics for port INT1:
linkStateChange:      1
```

**Table 97.** *Link Statistics*

Statistics	Description
linkStateChange	The total number of link state changes.

## RMON Statistics

Use the following command to display the Remote Monitoring (RMON) statistics of the selected port:

**show interface port** <port alias or number> **rmon-counters**

**Command mode:** All

RMON statistics for port EXT2:	
etherStatsDropEvents:	NA
etherStatsOctets:	0
etherStatsPkts:	0
etherStatsBroadcastPkts:	0
etherStatsMulticastPkts:	0
etherStatsCRCAlignErrors:	0
etherStatsUndersizePkts:	0
etherStatsOversizePkts:	0
etherStatsFragments:	NA
etherStatsJabbers:	0
etherStatsCollisions:	0
etherStatsPkts64to127octets:	0
etherStatsPkts128to255octets:	0
etherStatsPkts256to511octets:	0
etherStatsPkts512to1023octets:	0
etherStatsPkts1024to1518octets:	0

**Table 98.** RMON Statistics of a Port

Statistics	Description
etherStatsDropEvents	The total number of packets received that were dropped because of system resource constraints.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
etherStatsCRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

**Table 98.** *RMON Statistics of a Port (continued)*

<b>Statistics</b>	<b>Description</b>
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).

**Table 98.** *RMON Statistics of a Port (continued)*

<b>Statistics</b>	<b>Description</b>
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

## QoS Queue Statistics

The following commands display Quality of Service (QoS) Queue statistics.

**Table 99.** *QoS Queue Statistics*

Command Syntax and Usage
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>egress-queue-counters</b> [<i>&lt;0-7&gt;</i>   <b>drop</b>]</p> <p>Displays the total number of successfully transmitted or dropped packets and bytes for each QoS queue for the selected port.</p> <ul style="list-style-type: none"><li>o <i>&lt;0-7&gt;</i> displays statistics only for the specified queue</li><li>o <b>drop</b> displays statistics only for the dropped packets and bytes</li></ul> <p><b>Command mode:</b> All</p>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>egress-mcast-queue-counters</b> [<i>&lt;8-11&gt;</i>   <b>drop</b>]</p> <p>Displays the total number of successfully transmitted or dropped packets and bytes for each multicast QoS queue for the selected port.</p> <ul style="list-style-type: none"><li>o <i>&lt;8-11&gt;</i> displays statistics only for the specified queue</li><li>o <b>drop</b> displays statistics only for the dropped packets and bytes</li></ul> <p><b>Command mode:</b> All</p>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>egress-queue-rate</b> [<i>&lt;0-7&gt;</i>   <b>drop</b>]</p> <p>Displays the number of successfully transmitted or dropped packets and bytes per second for each QoS queue for the selected port.</p> <ul style="list-style-type: none"><li>o <i>&lt;0-7&gt;</i> displays statistics only for the specified queue</li><li>o <b>drop</b> displays statistics only for the dropped packets and bytes</li></ul> <p><b>Command mode:</b> All</p>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>egress-mcast-queue-rate</b> [<i>&lt;8-11&gt;</i>   <b>drop</b>]</p> <p>Displays the number of successfully transmitted or dropped packets and bytes per second for each multicast QoS queue for the selected port.</p> <ul style="list-style-type: none"><li>o <i>&lt;8-11&gt;</i> displays statistics only for the specified queue</li><li>o <b>drop</b> displays statistics only for the dropped packets and bytes</li></ul> <p><b>Command mode:</b> All</p>

Use the following command to display the rate-based QoS queue statistics of the selected port:

**show interface port** <port alias or number> **egress-queue-rate**

**Command mode:** All

```

QoS Rate for port INTA14:
QoS Queue 0:
  Tx Packets:                5
  Dropped Packets:          0
  Tx Bytes:                  363
  Dropped Bytes:            0
QoS Queue 1:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 2:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 3:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 4:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 5:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 6:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 7:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
  
```

**Table 100.** QoS Queue Rate-Based Statistics of a Port

Statistics	Description
Tx Packets	Number of successfully transmitted packets per second for the QoS queue.
Dropped Packets	Number of dropped packets per second for the QoS queue.

**Table 100.** QoS Queue Rate-Based Statistics of a Port (continued)

Statistics	Description
Tx Bytes	Number of successfully transmitted bytes per second for the QoS queue.
Dropped Bytes	Number of dropped bytes per second for the QoS queue.

Use the following command to display the -based QoS queue statistics of the selected port:

**show interface port** *<port alias or number>* **egress-queue-counters**

**Command mode:** All

```
QoS Rate for port 1:1:
QoS Queue 0:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
QoS Queue 1:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
QoS Queue 2:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
QoS Queue 3:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
QoS Queue 4:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
QoS Queue 5:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
QoS Queue 6:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
QoS Queue 7:
  Tx Packets:                                0
  Dropped Packets:                          0
  Tx Bytes:                                  0
  Dropped Bytes:                             0
```



**Table 101.** *QoS Queue Rate-Based Statistics of a Port*

<b>Statistics</b>	<b>Description</b>
Tx Packets	Total number of successfully transmitted packets for the QoS queue.
Dropped Packets	Total number of dropped packets for the QoS queue.
Tx Bytes	Total number of successfully transmitted bytes for the QoS queue.
Dropped Bytes	Total number of dropped bytes for the QoS queue.

---

## Link Aggregation Group (LAG) Statistics

The following commands display Link Aggregation Group (LAG) statistics.

**Table 102.** LAG Statistics Commands

Command Syntax and Usage
<b>show interface portchannel</b> <i>&lt;trunk group number&gt;</i> <b>interface-counters</b> Displays interface statistics for the LAG. For a sample output see <a href="#">page 226</a> . <b>Command mode:</b> All
<b>clear interface portchannel</b> <i>&lt;trunk group number&gt;</i> <b>counters</b> Clears all the statistics on the specified LAG. <b>Command mode:</b> All except User EXEC

## Trunk Group Interface Statistics

The following command displays interface statistics for the specified trunk group.

**show interface portchannel** *<trunk group number>* **interface-counters**

Command mode: All

Interface statistics for trunk group 12:		
	ifHCIn Counters	ifHCOut Counters
Octets:	6003620	27746863
UcastPkts:	0	0
BroadcastPkts:	0	33358
MulticastPkts:	42883	135420
FlowCtrlPkts:	0	0
PriFlowCtrlPkts:	0	0
Discards:	0	0
Errors:	0	0
Ingress Discard reasons for trunk group 12:		
VLAN Discards:	0	
Empty Egress Portmap:	0	
Filter Discards:	0	
Policy Discards:	0	
Non-Forwarding State:	0	
IBP/CBP Discards:	0	

---

## Layer 2 Statistics

The following commands display Layer 2 statistics.

**Table 103.** *Layer 2 Statistics Commands*

Command Syntax and Usage
<b>show fcoe counters</b> Displays Fibre Channel over Ethernet (FCoE) statistics. See <a href="#">page 309</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; lacp counters</b> Displays Link Aggregation Control Protocol (LACP) statistics for the specified port. See <a href="#">page 229</a> for sample output. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; lldp counters</b> Displays LLDP statistics for the specified port. See <a href="#">page 231</a> for sample output. <b>Command mode:</b> All except User EXEC
<b>show hotlinks counters</b> Displays Hot Links statistics. See <a href="#">page 230</a> for sample output. <b>Command mode:</b> All except User EXEC
<b>show oam counters</b> Displays OAM statistics. See <a href="#">page 233</a> for sample output. <b>Command mode:</b> All except User EXEC
<b>show spanning-tree statistics</b> Displays all Spanning Tree Protocol (STP) statistics. See <a href="#">page 232</a> for sample output. <b>Command mode:</b> All
<b>clear fcoe counters</b> Clears all Fibre Channel over Ethernet (FCoE) statistics. <b>Command mode:</b> All
<b>clear interface port &lt;port alias or number&gt; lacp counters</b> Clears all Link Aggregation Control Protocol (LACP) statistics for the specified port. <b>Command mode:</b> All except User EXEC

**Table 103.** *Layer 2 Statistics Commands (continued)*

<b>Command Syntax and Usage</b>
<b>clear interface port</b> <i>&lt;port alias or number&gt;</i> <b>lldp counters</b> Clears all LLDP statistics for the port. <b>Command mode:</b> All except User EXEC
<b>clear hotlinks</b> Clears all Hot Links statistics. <b>Command mode:</b> All except User EXEC

## LACP Statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics:

```
show interface port <port alias or number> lACP counters
```

**Command mode:** All

```
Port EXT1:
-----
Valid LACPDUs received:      - 870
Valid Marker PDUs received:  - 0
Valid Marker Rsp PDUs received: - 0
Unknown version/TLV type:    - 0
Illegal subtype received:    - 0
LACPDUs transmitted:        - 6031
Marker PDUs transmitted:     - 0
Marker Rsp PDUs transmitted: - 0
```

Link Aggregation Control Protocol (LACP) statistics are described in the following table:

**Table 104.** *LACP Statistics*

Statistic	Description
Valid LACPDUs received	Total number of valid LACP data units received.
Valid Marker PDUs received	Total number of valid LACP marker data units received.
Valid Marker Rsp PDUs received	Total number of valid LACP marker response data units received.
Unknown version/TLV type	Total number of LACP data units with an unknown version or type, length, and value (TLV) received.
Illegal subtype received	Total number of LACP data units with an illegal subtype received.
LACPDUs transmitted	Total number of LACP data units transmitted.
Marker PDUs transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs transmitted	Total number of LACP marker response data units transmitted.

## Hotlinks Statistics

Use the following command to display Hot Links statistics:

**show hotlinks counters**

**Command mode:** All

```
Hot Links Trigger Stats:
-----
Trigger 1 statistics:
  Trigger Name: Trigger 1
  Master active:           0
  Backup active:          0
  FDB update:             0   failed: 0
```

The following table describes the Hotlinks statistics:

**Table 105.** *Hotlinks Statistics*

Statistic	Description
Master active	Total number of times the Master interface transitioned to the Active state.
Backup active	Total number of times the Backup interface transitioned to the Active state.
FDB update	Total number of FDB update requests sent.
failed	Total number of FDB update requests that failed.

## LLDP Port Statistics

Use the following command to display LLDP statistics:

```
show interface port <port alias or number> lldp counters
```

**Command mode:** All

```
LLDP Port INT1 Statistics
-----
Frames Transmitted      : 0
Frames Received         : 0
Frames Received in Errors : 0
Frames Discarded        : 0
TLVs Unrecognized       : 0
Neighbors Aged Out     : 0
...
```

The following table describes the LLDP port statistics:

**Table 106.** *LLDP Port Statistics*

Statistic	Description
Frames Transmitted	Total number of LLDP frames transmitted.
Frames Received	Total number of LLDP frames received.
Frames Received in Errors	Total number of LLDP frames that had errors.
Frames Discarded	Total number of LLDP frames discarded.
TLVs Unrecognized	Total number of unrecognized TLV (Type, Length, and Value) fields received.
Neighbors Aged Out	Total number of neighbor devices that have had their LLDP information aged out.

## Spanning Tree Statistics

Use the following command to display Spanning Tree Protocol (STP) statistics:

**show spanning-tree statistics**

**Command mode:** All

Spanning-tree group: 1									
Port	RxBpdu	TxBpdu	RxTCN	LastTCNRx		TxTCN	LastTCNTx		
17	28	212246	22	13:53:41	7-15-2016	210286	11:35:54	7-20-2016	
18	13	212244	7	13:53:18	7-15-2016	210289	11:35:54	7-20-2016	
20	212328	210259	181570	11:35:55	7-20-2016	210257	11:35:54	7-20-2016	
21	212326	2	210366	11:35:54	7-20-2016	1	13:33:07	7-15-2016	
22	238753	423006	204170	11:35:54	7-20-2016	420536	11:35:54	7-20-2016	
23	232365	423004	204612	11:35:54	7-20-2016	420530	11:35:54	7-20-2016	
24	240073	423000	199662	11:35:53	7-20-2016	420528	11:35:54	7-20-2016	
Spanning-tree group: 23									
Port	RxBpdu	TxBpdu	RxTCN	LastTCNRx		TxTCN	LastTCNTx		
11	39	211499	5	14:01:02	7-15-2016	101	2:11:41	7-20-2016	
12	36	211499	2	13:53:06	7-15-2016	104	2:11:41	7-20-2016	
13	36	211497	2	13:53:06	7-15-2016	104	2:11:41	7-20-2016	
14	36	211481	2	13:53:06	7-15-2016	104	2:11:41	7-20-2016	
15	36	211497	2	13:53:06	7-15-2016	104	2:11:41	7-20-2016	

Use the following command to display STP statistics for a specific port:

**show spanning-tree statistics port** *<port alias or number>*

**Command mode:** All

Port: 17									
stg	RxBpdu	TxBpdu	RxTCN	LastTCNRx		TxTCN	LastTCNTx		
1	28	212329	22	13:53:41	7-15-2016	210369	11:38:41	7-20-2016	
Dropped Bpdu counter: 28									

Use the following command to display STP statistics for a specific Spanning Tree Group (STG):

**show spanning-tree statistics stp** *<1-256>*

**Command mode:** All

Spanning-tree group: 1									
Port	RxBpdu	TxBpdu	RxTCN	LastTCNRx		TxTCN	LastTCNTx		
17	28	212246	22	13:53:41	7-15-2016	210286	11:35:54	7-20-2016	
18	13	212244	7	13:53:18	7-15-2016	210289	11:35:54	7-20-2016	
20	212328	210259	181570	11:35:55	7-20-2016	210257	11:35:54	7-20-2016	
21	212326	2	210366	11:35:54	7-20-2016	1	13:33:07	7-15-2016	
22	238753	423006	204170	11:35:54	7-20-2016	420536	11:35:54	7-20-2016	
23	232365	423004	204612	11:35:54	7-20-2016	420530	11:35:54	7-20-2016	
24	240073	423000	199662	11:35:53	7-20-2016	420528	11:35:54	7-20-2016	



## OAM Statistics

Use the following command to display OAM statistics:

**show oam counters**

**Command mode:** All

```
OAM statistics on port INT1
-----
Information OAMPDU Tx :      0
Information OAMPDU Rx :      0
Unsupported OAMPDU Tx :      0
Unsupported OAMPDU Rx :      0

Local faults
-----
  0 Link fault records
  0 Critical events
  0 Dying gasps

Remote faults
-----
  0 Link fault records
  0 Critical events
  0 Dying gasps
```

OAM statistics include the following:

- Total number of OAM Protocol Data Units (OAMPDU) transmitted and received.
- Total number of unsupported OAM Protocol Data Units (OAMPDU) transmitted and received.
- Local faults detected.
- Remote faults detected.

## vLAG Statistics

The following table describes the vLAG statistics commands:

**Table 107.** *vLAG Statistics Options*

Command Syntax and Usage
<b>show vlag isl-statistics</b> Displays vLAG ISL statistics for the selected port. See <a href="#">page 234</a> for sample output.
<b>show vlag statistics</b> Displays all vLAG statistics. See <a href="#">page 234</a> for sample output.
<b>clear vlag statistics</b> Clears all vLAG statistics.

### vLAG ISL Statistics

Use the following command to display vLAG statistics:

**show vlag isl-statistics**

**Command mode:** All

	In Counter	Out Counter
Octets:	2755820	2288
Packets:	21044	26

ISL statistics include the total number of octets received/transmitted, and the total number of packets received/transmitted over the Inter-Switch Link (ISL).

### vLAG Statistics

Use the following command to display vLAG statistics:

**show vlag statistics**

**Command mode:** All

vLAG PDU sent:			
Role Election:	0	System Info:	0
Peer Instance Enable:	0	Peer Instance Disable:	0
FDB Dynamic Add:	0	FDB Dynamic Del:	0
FDB Inactive Add:	0	FDB Inactive Del:	0
Health Check:	0	ISL Hello:	0
Other:	0	Unknown:	0
vLAG PDU received:			
Role Election:	0	System Info:	0
Peer Instance Enable:	0	Peer Instance Disable:	0
FDB Dynamic Add:	0	FDB Dynamic Del:	0
FDB Inactive Add:	0	FDB Inactive Del:	0
Health Check:	0	ISL Hello:	0
Other:	0	Unknown:	0
vLAG IGMP packets forwarded:			
IGMP Reports:	0		
IGMP Leaves:	0		

The following table describes the vLAG statistics:

**Table 108.** *vLAG Statistics*

<b>Statistic</b>	<b>Description</b>
Role Election	Total number of vLAG PDUs sent for role elections.
System Info	Total number of vLAG PDUs sent for getting system information.
Peer Instance Enable	Total number of vLAG PDUs sent for enabling peer instance.
Peer Instance Disable	Total number of vLAG PDUs sent for disabling peer instance.
FDB Dynamic Add	Total number of vLAG PDUs sent for addition of FDB dynamic entry.
FDB Dynamic Del	Total number of vLAG PDUs sent for deletion of FDB dynamic entry.
FDB Inactive Add	Total number of vLAG PDUs sent for addition of FDB inactive entry.
FDB Inactive Del	Total number of vLAG PDUs sent for deletion of FDB inactive entry.
Health Check	Total number of vLAG PDUs sent for health checks.
ISL Hello	Total number of vLAG PDUs sent for ISL hello.
Other	Total number of vLAG PDUs sent for other reasons.
Unknown	Total number of vLAG PDUs sent for unknown operations.
IGMP Reports	Total number of IGMP Reports forwarded over vLAG.
IGMP Leaves	Total number of IGMP Leave messages forwarded over vLAG.

---

## Layer 3 Statistics

The following commands display Layer 3 statistics.

**Table 109.** *Layer 3 Statistics Commands*

Command Syntax and Usage
<b>show ip arp counters</b> Displays Address Resolution Protocol (ARP) statistics. See <a href="#">page 250</a> for sample output. <b>Command mode:</b> All
<b>show ip arp inspection statistics [vlan &lt;VLAN ID (1-4094)&gt;]</b> Displays Dynamic ARP Inspection statistics. See <a href="#">page 250</a> for sample output. <b>Command mode:</b> All
<b>show ip counters</b> Displays IP statistics. See <a href="#">page 240</a> for sample output. <b>Command mode:</b> All
<b>show ip dhcp snooping counters</b> Displays Dynamic Host Control Protocol (DHCP) Snooping statistics. <b>Command mode:</b> All
<b>show ip dns counters</b> Displays Domain Name System (DNS) statistics. See <a href="#">page 252</a> for sample output. <b>Command mode:</b> All
<b>show ip icmp counters</b> Displays ICMP statistics. See <a href="#">page 253</a> for sample output. <b>Command mode:</b> All
<b>show ip igmp counters</b> Displays IGMP statistics. See <a href="#">page 258</a> for sample output. <b>Command mode:</b> All
<b>show ip igmp vlan &lt;VLAN number&gt; counter</b> Displays IGMP statistics for a specific VLAN. See <a href="#">page 258</a> for sample output. <b>Command mode:</b> All
<b>show ip pim counters</b> Displays PIM statistics for all configured PIM interfaces. See <a href="#">page 273</a> for sample output. <b>Command mode:</b> All

**Table 109.** Layer 3 Statistics Commands (continued)

<b>Command Syntax and Usage</b>
<b>show ip pim interface</b> <interface number> <b>counters</b> Displays PIM statistics for the selected interface. <b>Command mode:</b> All
<b>show ip pim mroute count</b> Displays statistics of various multicast entry types. <b>Command mode:</b> All
<b>show ip ospf counters</b> Displays OSPF statistics. See <a href="#">page 264</a> for sample output. <b>Command mode:</b> All
<b>show ip rip counters</b> Displays Routing Information Protocol (RIP) statistics. See <a href="#">page 274</a> for sample output. <b>Command mode:</b> All
<b>show ip route counters</b> Displays route statistics. See <a href="#">page 248</a> for sample output. <b>Command mode:</b> All
<b>show ip slp counter</b> Displays Service Location Protocol (SLP) packet statistics. See <a href="#">page 317</a> for a sample output. <b>Command mode:</b> All
<b>show ip tcp counters</b> Displays TCP statistics. See <a href="#">page 255</a> for sample output. <b>Command mode:</b> All
<b>show ip udp counters</b> Displays UDP statistics. See <a href="#">page 257</a> for sample output. <b>Command mode:</b> All
<b>show ip vrrp counters</b> When virtual routers are configured, you can display the protocol statistics for VRRP. See <a href="#">page 272</a> for sample output. <b>Command mode:</b> All
<b>show ipv6 counters</b> Displays IPv6 statistics. See <a href="#">page 243</a> for sample output. <b>Command mode:</b> All
<b>show ipv6 mld counters</b> Displays Multicast Listener Discovery (MLD) statistics. <b>Command mode:</b> All

**Table 109.** *Layer 3 Statistics Commands (continued)*

<b>Command Syntax and Usage</b>
<b>show ipv6 ospf counters</b> Displays OSPFv3 statistics. See <a href="#">page 269</a> for sample output. <b>Command mode:</b> All
<b>clear ip counters</b> Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip arp counters</b> Clears Address Resolution Protocol (ARP) statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip arp inspection statistics [vlan &lt;VLAN ID (1-4094)&gt;]</b> Clears Dynamic ARP Inspection statistics. <b>Command mode:</b> Privileged EXEC
<b>clear ip dhcp snooping counters</b> Clears DHCP Snooping statistics. <b>Command mode:</b> Privileged EXEC
<b>clear ip dns counters</b> Clears Domain Name System (DNS) statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip icmp counters</b> Clears Internet Control Message Protocol (ICMP) statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip igmp [&lt;VLAN number&gt;] counters</b> Clears IGMP statistics for all VLANs or for a specific VLAN. <b>Command mode:</b> All
<b>clear ip ospf counters</b> Clears Open Shortest Path First (OSPF) statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip rip counters</b> Clears Routing Information Protocol (RIP) statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip slp counters</b> Clears Service Location Protocol (SLP) packet statistics. <b>Command mode:</b> All except user EXEC

**Table 109.** *Layer 3 Statistics Commands (continued)*

<b>Command Syntax and Usage</b>
<b>clear ip tcp counters</b> Clears Transmission Control Protocol (TCP) statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip udp counters</b> Clears User Datagram Protocol (UDP) statistics. <b>Command mode:</b> All except User EXEC
<b>clear ip vrrp counters</b> Clears VRRP statistics. <b>Command mode:</b> All
<b>clear ipv6 counters</b> Clears IPv6 statistics. Use this command with caution as it deletes all the IPv6 statistics. <b>Command mode:</b> All except User EXEC
<b>show layer3 counters</b> Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. <b>Command mode:</b> All

## IPv4 Statistics

The following command displays IPv4 statistics:

**show ip counters**

**Command mode:** All

IP statistics:			
ipInReceives:	3115873	ipInHdrErrors:	1
ipInAddrErrors:	35447	ipForwDatagrams:	0
ipInUnknownProtos:	500504	ipInDiscards:	0
ipInDelivers:	2334166	ipOutRequests:	1010542
ipOutDiscards:	4	ipOutNoRoutes:	4
ipReasmReqds:	0	ipReasmOKs:	0
ipReasmFails:	0	ipFragOKs:	0
ipFragFails:	0	ipFragCreates:	0
ipRoutingDiscards:	0	ipDefaultTTL:	255
ipReasmTimeout:	5		

**Table 110.** *IP Statistics*

Statistic	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.



**Table 110.** *IP Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this <i>no-route</i> criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.
ipReasmFails	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their DON ' t Fragment flag was set.

**Table 110.** *IP Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the <b>Time-To-Live (TTL)</b> field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

Use the following command to clear IPv4 statistics:

**clear ip counters**

**Command mode:** All except User EXEC

## IPv6 Statistics

The following command displays IPv6 statistics:

**show ipv6 counters**

**Command mode:** All

```
IPv6 Statistics
*****
48016 Rcvd                0 HdrErrors                0 TooBigErrors
  0 AddrErrors            0 FwdDgrams                0 UnknownProtos
  0 Discards              48016 Delivers            48155 OutRequests
  0 OutDiscards           0 OutNoRoutes             0 ReasmReqds
  0 ReasmOKs              0 ReasmFails
  0 FragOKs               0 FragFails               0 FragCreates
  0 RcvdMcastPkt         146 SentMcastPkts        0 TruncatedPkts
  0 RcvdRedirects        0 SentRedirects

ICMP Statistics
*****
Received :
43353 ICMPPkts          1 ICMPErrPkt              91 DestUnreach          0 TimeExcds
  0 ParmProbs            0 PktTooBigMsg           39512 ICMEchoReq        0 ICMEchoReps
  0 RouterSols           0 RouterAdv              1828 NeighSols         1922 NeighAdv
  0 Redirects            91 AdminProhib           0 ICMPBadCode

Sent :
43269 ICMPMsgs          0 ICMPErrMsgs            0 DstUnReach            0 TimeExcds
  0 ParmProbs            0 PktTooBigMsg           0 EchoReq               39512 EchoReply
  6 RouterSols           0 RouterAdv              1924 NeighSols         1827 NeighborAdv
  0 RedirectMsgs         0 AdminProhibMsgs

UDP statistics
*****
Received :
4679 UDPDgrams          0 UDPNoPorts              0 UDPErrPkts
Sent :
91 UDPDgrams
```

Table 111 describes the IPv6 statistics.

**Table 111.** *IPv6 Statistics*

<b>Statistic</b>	<b>Description</b>
Rcvd	Number of datagrams received from interfaces, including those received in error.
HdrErrors	Number of datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
TooBigErrors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
AddrErrors	Number of datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses. For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
FwdDgrams	Number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.
UnknownProtos	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Discards	Number of IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Delivers	Number of datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
OutDiscards	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).

**Table 111.** *IPv6 Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
OutNoRoutes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ReasmReqds	Number of IP fragments received which needed to be reassembled at this entity (the switch).
ReasmOKs	Number of IP datagrams successfully re- assembled.
ReasmFails	Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don ' t Fragment flag was set.
FragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
RcvdMcastPkt	The number of multicast packets received by the interface.
SentMcastPkts	The number of multicast packets transmitted by the interface.
TruncatedPkts	The number of input datagrams discarded because datagram frame didn't carry enough data.
RcvdRedirects	The number of Redirect messages received by the interface.
SentRedirects	The number of Redirect messages sent.

The following table describes the IPv6 ICMP statistics.

**Table 112.** *ICMP Statistics*

<b>Statistic</b>	<b>Description</b>
<b>Received</b>	
ICMPPkts	Number of ICMP messages which the entity (the switch) received.
ICMPErrPkt	Number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth).
DestUnreach	Number of ICMP Destination Unreachable messages received.
TimeExcds	Number of ICMP Time Exceeded messages received.
ParmProbs	Number of ICMP Parameter Problem messages received.
PktTooBigMsg	The number of ICMP Packet Too Big messages received by the interface.
ICMPEchoReq	Number of ICMP Echo (request) messages received.
ICMPEchoReps	Number of ICMP Echo Reply messages received.
RouterSols	Number of Router Solicitation messages received by the switch.
RouterAdv	Number of Router Advertisements received by the switch.
NeighSols	Number of Neighbor Solicitations received by the switch.
NeighAdv	Number of Neighbor Advertisements received by the switch.
Redirects	Number of ICMP Redirect messages received.
AdminProhib	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPBadCode	The number of ICMP Parameter Problem messages received by the interface.
<b>Sent</b>	
ICMPMsgs	Number of ICMP messages which this entity (the switch) attempted to send.
ICMPErrMsgs	Number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
DstUnReach	Number of ICMP Destination Unreachable messages sent.

**Table 112.** ICMP Statistics (continued)

Statistic	Description
TimeExcds	Number of ICMP Time Exceeded messages sent.
ParmProbs	Number of ICMP Parameter Problem messages sent.
PktTooBigs	The number of ICMP Packet Too Big messages sent by the interface.
EchoReq	Number of ICMP Echo (request) messages sent.
EchoReply	Number of ICMP Echo Reply messages sent.
RouterSols	Number of Router Solicitation messages sent by the switch.
RouterAdv	Number of Router Advertisements sent by the switch.
NeighSols	Number of Neighbor Solicitations sent by the switch.
NeighAdv	Number of Neighbor Advertisements sent by the switch.
RedirectMsgs	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
AdminProhibMsgs	Number of ICMP destination unreachable/communication administratively prohibited messages sent.

Table 113 describes the UDP statistics.

**Table 113.** UDP Statistics

Statistic	Description
<b>Received</b>	
UDPDgrams	Number of UDP datagrams received by the switch.
UDPNoPorts	Number of received UDP datagrams for which there was no application at the destination port.
UDPErrPkts	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
<b>Sent</b>	
UDPDgrams	Number of UDP datagrams sent from this entity (the switch).

Use the following command to clear IPv6 statistics:

**clear ipv6 counters**

**Command mode:** All except User EXEC

## IPv4 Route Statistics

The following command displays IPv4 route statistics:

**show ip route counters**

**Command mode:** All

```

Route statistics:
-----
Current total outstanding routes      :           1
Highest number ever recorded         :           1
Current static routes                 :           0
Current RIP routes                   :           0
Current OSPF routes                  :           0
Current BGP routes                   :           0
Maximum supported routes              :          2048

ECMP statistics (active in ASIC):
-----
Maximum number of ECMP routes        :          2048
Maximum number of static ECMP routes :           128
Number of routes with ECMP paths     :           0
  
```

**Table 114.** *Route Statistics*

Statistics	Description
Current total outstanding routes	Total number of outstanding routes in the route table.
Highest number ever recorded	Highest number of routes ever recorded in the route table.
Current static routes	Total number of static routes in the route table.
Current RIP routes	Total number of Routing Information Protocol (RIP) routes in the route table.
Current OSPF routes	Total number of OSPF routes in the route table.
Current BGP routes	Total number of Border Gateway Protocol routes in the route table.
Maximum supported routes	Maximum number of routes that are supported.
Maximum number of ECMP routes	Maximum number of ECMP routes that are supported.
Maximum number of static ECMP routes	Maximum number of static ECMP routes that are supported.
Number of routes with ECMP paths	Current number of routes that contain ECMP paths.



## IPv6 Route Statistics

The following command displays IPv6 route statistics:

**show ipv6 route counters**

**Command mode:** All

IPv6 Route statistics:			
ipv6RoutesCur:	4	ipv6RoutesHighWater:	6
ipv6RoutesMax:	1156		
ECMP statistics:			
-----			
Maximum number of ECMP routes	:	600	
Max ECMP paths allowed for one route	:	5	

**Table 115.** *IPv6 Route Statistics*

Statistics	Description
ipv6RoutesCur	Total number of outstanding routes in the route table.
ipv6RoutesHighWater	Highest number of routes ever recorded in the route table.
ipv6RoutesMax	Maximum number of routes that are supported.
Maximum number of ECMP routes	Maximum number of ECMP routes supported.
Max ECMP paths allowed for one route	Maximum number of ECMP paths supported for each route.

Use the `clear` option to delete all IPv6 route statistics.

## ARP statistics

The following command displays Address Resolution Protocol statistics.

**show [ip] arp counters**

**Command mode:** All

ARP statistics:			
arpEntriesCur:	3	arpEntriesHighWater:	4
arpEntriesMax:	4095		

**Table 116.** *ARP Statistics*

Statistic	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.
arpEntriesMax	The maximum number of ARP entries that are supported.

The following command displays Dynamic ARP Inspection statistics.

**show ip arp inspection statistics [vlan <VLAN ID (1-4094)>]**

**Command mode:** All

Vlan	Forwarded	Dropped
2	100	200

## DHCP Statistics

The following commands display DHCP statistics:

**Table 117.** *DHCP Statistics Options*

Command Syntax and Usage
<b>show ip dhcp snooping counters</b> Displays DHCP Snooping statistics. <b>Command mode:</b> All
<b>clear ip dhcp snooping counters</b> Clears DHCP Snooping statistics. <b>Command mode:</b> Privileged EXEC

### *DHCP Snooping Statistics*

The following command displays DHCP Snooping statistics:

**show ip dhcp snooping counters**

**Command mode:** All

DHCP Snooping statistics:	
Received Request packets	2
Received Reply packets	2
Received Invalid packets	0
Dropped packets out of rate	0
Dropped packets other reason	0

DHCP Snooping Statistics count all DHCP packets processed by DHCP snooping.

## DNS Statistics

The following command displays Domain Name System statistics.

**show ip dns counters**

**Command mode:** All

DNS statistics:	
dnsInRequests:	0
dnsOutRequests:	0
dnsBadRequests:	0

**Table 118.** *DNS Statistics*

<b>Statistics</b>	<b>Description</b>
dnsInRequests	The total number of DNS response packets that have been received.
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

## ICMP Statistics

The following command displays ICMP statistics:

**show ip icmp counters**

**Command mode:** All

ICMP statistics:			
icmpInMsgs:	245802	icmpInErrors:	1393
icmpInDestUnreachs:	41	icmpInTimeExcds:	0
icmpInParmProbs:	0	icmpInSrcQuenchs:	0
icmpInRedirects:	0	icmpInEchos:	18
icmpInEchoReps:	244350	icmpInTimestamps:	0
icmpInTimestampReps:	0	icmpInAddrMasks:	0
icmpInAddrMaskReps:	0	icmpOutMsgs:	253810
icmpOutErrors:	0	icmpOutDestUnreachs:	15
icmpOutTimeExcds:	0	icmpOutParmProbs:	0
icmpOutSrcQuenchs:	0	icmpOutRedirects:	0
icmpOutEchos:	253777	icmpOutEchoReps:	18
icmpOutTimestamps:	0	icmpOutTimestampReps:	0
icmpOutAddrMasks:	0	icmpOutAddrMaskReps:	0

**Table 119.** ICMP Statistics

Statistic	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by icmpInErrors.
icmpInErrors	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received.

**Table 119.** *ICMP Statistics*

<b>Statistic</b>	<b>Description</b>
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by <code>icmpOutErrors</code> .
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

## TCP Statistics

The following command displays TCP statistics:

**show ip tcp counters**

**Command mode:** All

TCP statistics:			
tcpRtoAlgorithm:	4	tcpRtoMin:	0
tcpRtoMax:	240000	tcpMaxConn:	2048
tcpActiveOpens:	0	tcpPassiveOpens:	16
tcpAttemptFails:	0	tcpEstabResets:	0
tcpInSegs:	2035	tcpOutSegs:	1748
tcpRetransSegs:	21	tcpInErrs:	0
tcpCurrEstab:	1	tcpCurrConn:	5
tcpOutRsts:	0		

**Table 120.** TCP Statistics

Statistic	Description
tcpRtoAlgorithm	The algorithm used to determine the <code>timeout</code> value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>LBOUND</code> quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>UBOUND</code> quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the <code>SYN-SENT</code> state from the <code>CLOSED</code> state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the <code>SYN-RCVD</code> state from the <code>LISTEN</code> state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the <code>CLOSED</code> state from either the <code>SYN-SENT</code> state or the <code>SYN-RCVD</code> state, plus the number of times TCP connections have made a direct transition to the <code>LISTEN</code> state from the <code>SYN-RCVD</code> state.

**Table 120.** *TCP Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurEstab	The total number of outstanding TCP sessions in the ESTABLISHED state.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.



## UDP Statistics

The following command displays UDP statistics:

**show ip udp counters**

**Command mode:** All

UDP statistics:			
udpInDatagrams:	54	udpOutDatagrams:	43
udpInErrors:	0	udpNoPorts:	1578077

**Table 121.** *UDP Statistics*

Statistic	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

## IGMP Statistics

The following command displays statistics about IGMP protocol packets for all VLANs:

### show ip igmp counters

**Command mode:** All

```

IGMP vlan 2 statistics:
-----
rxIgmpValidPkts:          0  rxIgmpInvalidPkts:          0
rxIgmpGenQueries:         0  rxIgmpGrpSpecificQueries:   0
rxIgmpGroupSrcSpecificQueries: 0  rxIgmpDiscardPkts:         0
rxIgmpLeaves:            0  rxIgmpReports:             0
txIgmpReports:           0  txIgmpGrpSpecificQueries:   0
txIgmpLeaves:            0  rxIgmpV3CurrentStateRecords: 0
rxIgmpV3SourceListChangeRecords:0  rxIgmpV3FilterChangeRecords: 0
txIgmpGenQueries:       18  rxPimHellos:                0
  
```

The following command displays statistics about IGMP protocol packets for a specific VLAN:

### show ip igmp vlan <VLAN number> counter

**Command mode:** All

```

IGMP vlan 147 statistics:
-----
rxIgmpValidPkts:          0  rxIgmpInvalidPkts:          0
rxIgmpGenQueries:         0  rxIgmpGrpSpecificQueries:   0
rxIgmpGroupSrcSpecificQueries: 0  rxIgmpDiscardPkts:         0
rxIgmpLeaves:            0  rxIgmpReports:             0
txIgmpReports:           0  txIgmpGrpSpecificQueries:   0
txIgmpLeaves:            0  rxIgmpV3CurrentStateRecords: 0
rxIgmpV3SourceListChangeRecords:0  rxIgmpV3FilterChangeRecords: 0
txIgmpGenQueries:       0  rxPimHellos:                0
  
```

**Table 122.** IGMP Statistics

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received.
rxIgmpInvalidPkts	Total number of invalid packets received.
rxIgmpGenQueries	Total number of General Membership Query packets received.
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received for specific groups.
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received.
rxIgmpDiscardPkts	Total number of IGMP packets discarded.

**Table 122.** *IGMP Statistics*

<b>Statistic</b>	<b>Description</b>
rxIgmpLeaves	Total number of Leave requests received.
rxIgmpReports	Total number of Membership Reports received.
txIgmpReports	Total number of Membership reports transmitted.
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups.
txIgmpLeaves	Total number of Leave messages transmitted.
rxIgmpV3CurrentStateRecords	Total number of Current State records received.
rxIgmpV3SourceListChangeRecords	Total number of Source List Change records received.
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received.
txIgmpGenQueries	Total number of transmitted General Queries.
rxPimHellos	Total number of PIM hello packets received.

## MLD Statistics

The following commands display MLD statistics.

**Table 123.** *MLD Statistics Commands*

Command Syntax and Usage
<b>show ipv6 mld</b> Displays MLD global statistics. See <a href="#">page 261</a> for sample output. <b>Command mode:</b> All
<b>show ipv6 mld counters</b> Displays MLD area statistics. <b>Command mode:</b> All
<b>show ipv6 mld interface</b> Displays information for all MLD interfaces. <b>Command mode:</b> All
<b>show ipv6 mld interface counters</b> Displays total number of MLD entries. <b>Command mode:</b> All
<b>show ipv6 mld interface</b> <i>&lt;interface number&gt;</i> Displays MLD interface statistics for the specified interface. <b>Command mode:</b> All
<b>show ipv6 mld interface</b> [ <i>&lt;interface number&gt;</i> ] <b>counters</b> Displays MLD interface statistics. <b>Command mode:</b> All
<b>clear ipv6 mld counters</b> Clears MLD counters. <b>Command mode:</b> Privileged EXEC
<b>clear ipv6 mld dynamic</b> Clears all dynamic MLD tables. <b>Command mode:</b> Privileged EXEC
<b>clear ipv6 mld groups</b> Clears dynamic MLD registered group tables. <b>Command mode:</b> Privileged EXEC
<b>clear ipv6 mld mrouter</b> Clears dynamic MLD mrouter group tables. <b>Command mode:</b> Privileged EXEC

## MLD Global Statistics

The MLD global statistics displays information for all MLD packets received on all interfaces

### show ipv6 mld counters

Command mode: All

```
MLD global statistics:
-----
Total L3 IPv6 (S, G, V) entries: 2
Total MLD groups: 2
Bad Length: 0
Bad Checksum: 0
Bad Receive If: 0
Receive non-local: 0
Invalid Packets: 4

MLD packet statistics for interfaces:

MLD interface packet statistics for interface 1:
MLD msg type      Received      Sent      RxErrors
-----
General Query          0          1067          0
MAS Query              0           0           0
MASSQ Query           0           0           0
MLDv1 Report          0           0           0
MLDv1 Done            0           0           0
MLDv2 Report         1069         1084          0
INC CSRs(v2)          1            0           0
EXC CSRs(v2)         2134         1093          0
TO_INC FMCRs(v2)      1            0           0
TO_EXC FMCRs(v2)      0            15          0
ALLOW SLCRs(v2)       0            0           0
BLOCK SLCRs(v2)       0            0           0

MLD interface packet statistics for interface 2:
MLD msg type      Received      Sent      RxErrors
-----

MLD interface packet statistics for interface 3:
MLD msg type      Received      Sent      RxErrors
-----
General Query          0          2467          0
MAS Query              0           0           0
MASSQ Query           0           0           0
MLDv1 Report          0           0           0
MLDv1 Done            0           0           0
MLDv2 Report          2          2472          0
INC CSRs(v2)          1            0           0
EXC CSRs(v2)          0          2476          0
TO_INC FMCRs(v2)      0            0           0
TO_EXC FMCRs(v2)      0            8           0
ALLOW SLCRs(v2)       0            0           0
BLOCK SLCRs(v2)       1            0           0
```

The following table describes the fields in the MLD global statistics output.

**Table 124.** *MLD Global Statistics*

<b>Statistic</b>	<b>Description</b>
Bad Length	Number of messages received with length errors.
Bad Checksum	Number of messages received with an invalid IP checksum.
Bad Receive If	Number of messages received on an interface not enabled for MLD.
Receive non-local	Number of messages received from non-local senders.
Invalid packets	Number of rejected packets.
General Query (v1/v2)	Number of general query packets.
MAS Query(v1/v2)	Number of multicast address specific query packets.
MASSQ Query (v2)	Number of multicast address and source specific query packets.
Listener Report(v1)	Number of packets sent by a multicast listener in response to MLDv1 query.
Listener Done(v1/v2)	Number of packets sent by a host when it wants to stop receiving multicast traffic.
Listener Report(v2)	Number of packets sent by a multicast listener in response to MLDv2 query.
MLDv2 INC mode CSRs	Number of current state records with include filter mode.
MLDv2 EXC mode CSRs	Number of current state records with exclude filter mode.
MLDv2 TO_INC FMCRs	Number of filter mode change records for which the filter mode has changed to include mode.
MLDv2 TO_EXC FMCRs	Number of filter mode change records for which the filter mode has changed to exclude mode.
MLDv2 ALLOW SLCRs	Number of source list change records for which the specified sources from where the data is to be received has changed.
MLDv2 BLOCK SLCRs	Number of source list change records for which the specified sources from where the data is to be received is to be blocked.

## OSPF Statistics

The following commands display OSPF statistics.

**Table 125.** *OSPF Statistics Commands*

<b>Command Syntax and Usage</b>
<b>show ip ospf counters</b> Displays OSPF statistics. See <a href="#">page 264</a> for sample output. <b>Command mode:</b> All
<b>show ip ospf area counters</b> Displays OSPF area statistics. <b>Command mode:</b> All
<b>show ip ospf interface [<i>&lt;interface number&gt;</i>] counters</b> Displays OSPF interface statistics. <b>Command mode:</b> All

## OSPF Global Statistics

The following command displays statistics about OSPF packets received on all OSPF areas and interfaces:

**show ip ospf counters**

**Command mode:** All

```

OSPF stats
-----
Rx/Tx Stats:           Rx           Tx
-----
Pkts                   0           0
hello                  23          518
database               4           12
ls requests            3           1
ls acks                7           7
ls updates             9           7

Nbr change stats:           Intf change Stats:
hello                       up                       4
start                       down                      2
n2way                       loop                      0
adjoint ok                  unloop                   0
negotiation done            wait timer               2
exchange done               backup                   0
bad requests                nbr change               5
bad sequence                0
loading done                2
n1way                       0
rst_ad                      0
down                        1

Timers kickoff
hello                       514
retransmit                  1028
lsa lock                    0
lsa ack                     0
dbage                      0
summary                    0
ase export                  0
  
```

**Table 126.** *OSPF General Statistics*

Statistic	Description
<b>Rx/Tx Stats:</b>	
Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.



**Table 126.** *OSPF General Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
<b>Nbr Change Stats:</b>	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets must now be sent to the neighbor at intervals of <code>HelloInterval</code> seconds.) across all OSPF areas and interfaces.
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.

**Table 126.** *OSPF General Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
bad sequence	The sum total number of Database Description packets which have been received that either: <ul style="list-style-type: none"> <li>a. Has an unexpected DD sequence number.</li> <li>b. Unexpectedly has the init bit set.</li> <li>c. Has an options field differing from the last Options field received in a Database Description packet.</li> </ul> Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
<b>Intf Change Stats:</b>	
up	The sum total number of interfaces up in all OSPF areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

**Table 126.** *OSPF General Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
<b>Timers Kickoff:</b>	
hello	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA Ack timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (Dbage) has been fired.
summary	The total number of times the Summary timer has been fired.
ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

## OSPFv3 Statistics

The following commands display OSPFv3 statistics.

**Table 127.** *OSPFv3 Statistics Commands*

<b>Command Syntax and Usage</b>
<b>show ipv6 ospf counters</b> Displays OSPFv3 statistics. See <a href="#">page 264</a> for sample output. <b>Command mode:</b> All
<b>show ipv6 ospf area counters</b> Displays OSPFv3 area statistics. <b>Command mode:</b> All
<b>show ipv6 ospf interface [<i>&lt;interface number&gt;</i>] counters</b> Displays OSPFv3 interface statistics. <b>Command mode:</b> All

## OSPFv3 Global Statistics

The following command displays statistics about OSPFv3 packets received on all OSPFv3 areas and interfaces:

**show ipv6 ospf counters**

**Command mode:** All

```

OSPFv3 stats
-----
Rx/Tx/Discd Stats:      Rx          Tx          Discarded
                        -----
                        Pkts
      Pkts              9695          95933          0
      hello             9097          8994           0
      database           39            51             6
      ls requests       16             8             0
      ls acks           172           360            0
      ls updates        371           180            0

Nbr change stats:      Intf change Stats:
  down                  0              down          5
  attempt               0              loop          0
  init                  1              waiting       6
  n2way                 1              ptop          0
  exstart               1              dr            4
  exchange done        1              backup        6
  loading done          1              dr other      0
  full                  1              all events    33
  all events            6

Timers kickoff
  hello                 8988
  wait                  6
  poll                  0
  nbr probe             0

Number of LSAs
  originated             180
  rcvd newer originations 355
  
```

The OSPFv3 General Statistics contain the sum total of all OSPF packets received on all OSPFv3 areas and interfaces.

**Table 128.** *OSPFv3 General Statistics*

Statistics	Description
<b>Rx/Tx Stats:</b>	
Rx Pkts	The sum total of all OSPFv3 packets received on all OSPFv3 interfaces.
Tx Pkts	The sum total of all OSPFv3 packets transmitted on all OSPFv3 interfaces.
Discarded Pkts	The sum total of all OSPFv3 packets discarded.
Rx hello	The sum total of all Hello packets received on all OSPFv3 interfaces.
Tx hello	The sum total of all Hello packets transmitted on all OSPFv3 interfaces.

**Table 128.** *OSPFv3 General Statistics (continued)*

<b>Statistics</b>	<b>Description</b>
Discarded hello	The sum total of all Hello packets discarded, including packets for which no associated interface has been found.
Rx database	The sum total of all Database Description packets received on all OSPFv3 interfaces.
Tx database	The sum total of all Database Description packets transmitted on all OSPFv3 interfaces.
Discarded database	The sum total of all Database Description packets discarded.
Rx ls requests	The sum total of all Link State Request packets received on all OSPFv3 interfaces.
Tx ls requests	The sum total of all Link State Request packets transmitted on all OSPFv3 interfaces.
Discarded ls requests	The sum total of all Link State Request packets discarded.
Rx ls acks	The sum total of all Link State Acknowledgement packets received on all OSPFv3 interfaces.
Tx ls acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPFv3 interfaces.
Discarded ls acks	The sum total of all Link State Acknowledgement packets discarded.
Rx ls updates	The sum total of all Link State Update packets received on all OSPFv3 interfaces.
Tx ls updates	The sum total of all Link State Update packets transmitted on all OSPFv3 interfaces.
Discarded ls updates	The sum total of all Link State Update packets discarded.
<b>Nbr Change Stats:</b>	
down	The total number of Neighboring routers down (in the initial state of a neighbor conversation) across all OSPFv3 interfaces.
attempt	The total number of transitions into attempt state of neighboring routers across all OSPFv3 interfaces.
init	The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces.
n2way	The total number of bidirectional communication establishment between this router and other neighboring routers.
exstart	The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces.

**Table 128.** *OSPFv3 General Statistics (continued)*

<b>Statistics</b>	<b>Description</b>
exchange done	The total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPFv3 interfaces.
loading done	The total number of link state updates received for all out-of-date portions of the database across all OSPFv3 interfaces.
full	The total number of transitions into full state of neighboring routers across all OSPFv3 interfaces.
all events	The total number of state transitions of neighboring routers across all OSPFv3 interfaces.
<b>Intf Change Stats:</b>	
down	The total number of transitions into down state of all OSPFv3 interfaces.
loop	The total number of transitions into loopback state of all OSPFv3 interfaces.
waiting	The total number of transitions into waiting state of all OSPFv3 interfaces.
ptop	The total number of transitions into point-to-point state of all OSPFv3 interfaces.
dr	The total number of transitions into Designated Router other state of all OSPFv3 interfaces.
backup	The total number of transitions into backup state of all OSPFv3 interfaces.
all events	The total number of changes associated with any OSPFv3 interface, including changes into internal states.
<b>Timers Kickoff:</b>	
hello	The total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OSPFv3 interfaces.
wait	The total number of times the wait timer has been fired (which causes an interface to exit waiting state), across all OPSFv3 interfaces.
poll	The total number of times the timer whose firing causes hellos to be sent to inactive NBMA and Demand Circuit neighbors has been fired, across all OPSFv3 interfaces.
nbr probe	The total number of times the neighbor probe timer has been fired, across all OPSFv3 interfaces.
<b>Number of LSAs:</b>	
originated	The number of LSAs originated by this router.
rcvd newer originations	The number of LSAs received that have been determined to be newer originations.

## VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the EN4093R provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the protocol statistics for VRRP. The following command displays VRRP statistics:

**show ip vrrp counters**

**Command mode:** All

VRRP statistics:			
vrrpInAdvers:	0	vrrpBadAdvers:	0
vrrpOutAdvers:	0		
vrrpBadVersion:	0	vrrpBadVrid:	0
vrrpBadAddress:	0	vrrpBadData:	0
vrrpBadPassword:	0	vrrpBadInterval:	0

**Table 129.** VRRP Statistics

Statistics	Description
vrrpInAdvers	The total number of valid VRRP advertisements that have been received.
vrrpBadAdvers	The total number of VRRP advertisements received that were dropped.
vrrpOutAdvers	The total number of VRRP advertisements that have been sent.
vrrpBadVersion	The total number of VRRP advertisements received that had a bad version number.
vrrpBadVrid	The total number of VRRP advertisements received that had a bad virtual router ID.
vrrpBadAddress	The total number of VRRP advertisements received that had a bad address.
vrrpBadData	The total number of VRRP advertisements received that had bad data.
vrrpBadPassword	The total number of VRRP advertisements received that had a bad password.
vrrpBadInterval	The total number of VRRP advertisements received that had a bad interval.



## PIM Statistics

The following command displays Protocol Independent Multicast (PIM) statistics:

**show ip pim counters**

**Command mode:** All

Hello Tx/Rx	: 2595/2596
Join/Prune Tx/Rx	: 0/0
Assert Tx/Rx	: 0/0
Register Tx/Rx	: 0/0
Null-Reg Tx/Rx	: 0/0
RegStop Tx/Rx	: 0/0
CandRPAdv Tx/Rx	: 973/0
BSR Tx/Rx	: 0/1298
Graft Tx/Rx	: 0/0
Graft Ack Tx/Rx	: 0/0
Mcast data Tx/Rx	: 0/0
MDP drop Tx/Rx	: 0/0
CTL drop Tx/Rx	: 0/0
Bad pkts	: 0

**Table 130.** PIM Statistics

Statistics	Description
Hello Tx/Rx	Number of Hello messages transmitted or received.
Join/Prune Tx/Rx	Number of Join/Prune messages transmitted or received.
Assert Tx/Rx	Number of Assert messages transmitted or received.
Register Tx/Rx	Number of Register messages transmitted or received.
Null-Reg Tx/Rx	Number of NULL-register messages transmitted or received.
RegStop Tx/Rx	Number of Register Stop messages transmitted or received.
CandRPAdv Tx/Rx	Number of Candidate RP Advertisements transmitted or received.
BSR Tx/Rx	Number of Bootstrap Router (BSR) messages transmitted or received.
Graft Tx/Rx	Number of Graft messages transmitted or received.
Graft Ack Tx/Rx	Number of Graft Acknowledgements transmitted or received.
Mcast data Tx/Rx	Number of multicast datagrams transmitted or received.
MDP drop Tx/Rx	Number of Multicast data packet Tx/Rx dropped.
CTL drop Tx/Rx	Number of PIM control packet Tx/Rx dropped.
Bad pkts	Number of bad PIM packets received.

## Routing Information Protocol Statistics

The following command displays RIP statistics:

**show ip rip counters**

**Command mode:** All

```
RIP ALL STATS INFORMATION:
  RIP packets received           = 12
  RIP packets sent               = 75
  RIP request received           = 0
  RIP response received          = 12
  RIP request sent               = 3
  RIP reponse sent               = 72
  RIP route timeout              = 0
  RIP bad size packet received   = 0
  RIP bad version received       = 0
  RIP bad zeros received         = 0
  RIP bad src port received      = 0
  RIP bad src IP received        = 0
  RIP packets from self received = 0
```

---

## OpenFlow Statistics

The following commands display OpenFlow statistics.

**Table 131.** *OpenFlow Statistics Commands*

<b>Command Syntax and Usage</b>
<b>show openflow statistics</b> Displays OpenFlow traffic statistics for each OpenFlow instance. <b>Command mode:</b> All
<b>show openflow instance &lt;1-2&gt; statistics</b> Displays OpenFlow traffic statistics for the specified instance ID. <b>Command mode:</b> All
<b>clear openflow statistics</b> Clears OpenFlow data for all instances. <b>Command mode:</b> Privileged EXEC
<b>clear openflow instance &lt;1-2&gt; statistics</b> Clears OpenFlow data for the specified instance ID. <b>Command mode:</b> Privileged EXEC

Use the following command to display OpenFlow traffic statistics for each OpenFlow instance:

**show openflow statistics**

Command mode: All

In Openflow 1.0:

```
Openflow statistics for instance 1
Flow Count
  Basic Flows:      3
    (ACL Based: 3, Unicast FDB Based: 0, Multicast FDB Based: 0)
  Emergency Flows: 0
    (ACL Based: 0, Unicast FDB Based: 0, Multicast FDB Based: 0)

Buffering Count:
  Openflow Packets Buffered   : 2
  Openflow Packets Timed out  : 0
  Openflow Packets Retrieved  : 0
  Openflow Packets Retrieve attempts : 0

Message Count
Hello-Sent: 1                Hello-Received: 1
Echo-Request-Sent: 8         Echo-Request-Received: 78
Echo-Reply-Sent: 78          Echo-Reply-Received: 8
Vendor: 0

Vendor Flow-Mod:
  Add: 0
  Modify: 0
  Modify-Strict: 0
  Delete: 0
  Delete-Strict: 0

Feature-Request: 1           Feature-Reply: 1
Get-Config-Request: 0       Get-Config-Reply: 0
Set-Config: 1

Packet-In
  No-Match: 0
  Action: 2
  Action Mirror: 0

Flow-Removed:
  Idle-Timeout: 0
  Hard-Timeout: 0
  Delete: 0

Vendor-Flow-Removed:
  Idle-Timeout: 0
  Hard-Timeout: 0
  Delete: 0

Port-Status:
  Add: 0
  Delete: 0
  Modify: 0

Packet-Out: 572
Flow-Mod:
  Add: 3
  Modify: 0
  Modify-Strict: 0
  Delete: 0
  Delete-Strict: 1

Port-Mod: 0
```

```
Statistics-Request:
  Desc: 1
  Flow: 16
  Aggregate: 0
  Table: 0
  Port: 16
  Vendor: 0
    stats: 0
    stats-strict: 0
Statistics-Reply:
  Desc: 1
  Flow: 16
  Aggregate: 0
  Table: 0
  Port: 16
  Vendor: 0
    stats: 0
    stats-strict: 0
Barrier-Request: 2
Barrier-Reply: 2
Error Messages
Hello Failed Sent:
  Incompatible: 0
Hello Failed Recv:
  Incompatible: 0
Bad Request:
  Bad-Version: 0
  Bad-Type: 0
  Bad-Stat: 0
  Bad-Vendor: 0
  Bad-Subtype: 0
  Bad-Len: 0
  Buffer-Empty: 0
  Buffer-Unknown: 0
Bad Action:
  Bad-Type: 0
  Bad-Len: 0
  Bad-Out-Port: 0
  Bad-Argument: 0
  Too-many: 0
Flow-Mod-Failed:
  All-Table-Full: 0
  Overlap: 0
  Permission-Error: 0
  Emergency-Timeout: 0
  Bad-Command: 0
  Unsupported: 0
Port-Mod-Failed:
  Bad-Port: 0
  Bad-hw-addr: 0
-----
Openflow instance 2 is currently disabled
```

## In Openflow 1.3:

```
Openflow statistics for instance 1
Flow Count
  Static Flows: 0
    ACL Based: 0
    Mpls PUSH based: 0
    Mpls POP based: 0
  Dynamic Flows: 3
    ACL Based: 3
    Unicast FDB Based: 0
    Multicast FDB Based: 0
    Mpls PUSH based: 0
    Mpls POP based: 0
Group Count: 0
Buffering Count:
  Openflow Packets Buffered : 0
  Openflow Packets Timed out : 0
  Openflow Packets Retrieved : 0
  Openflow Packets Retrieve attempts : 0

Message Count
Hello-Sent: 1           Hello-Received: 1
Echo-Request-Sent: 5   Echo-Request-Received: 0
Echo-Reply-Sent: 0     Echo-Reply-Received: 5
Feature-Request: 1     Feature-Reply: 1
Get-Config-Request: 0  Get-Config-Reply: 0
Set-Config: 1
Packet-In
  No-Match: 17
  Action: 499
Flow-Removed:
  Idle-Timeout: 0
  Hard-Timeout: 0
  Delete: 0
  Group-Delete: 0
Port-Status:
  Add: 0
  Delete: 0
  Modify: 2
Packet-Out: 589
Flow-Mod:
  Add: 3
  Modify: 0
  Modify-Strict: 0
  Delete: 1
  Delete-Strict: 1
Group-Mod:
  Add: 0
  Modify: 0
  Delete: 0
Port-Mod: 0
Multipart-Request:
  Switch description: 2
  Individual flow statistics: 3
  Aggregate flow statistics: 0
  Flow table statistics: 0
  Port statistics: 3
  Group counter statistics: 0
  Group description: 0
  Group features: 0
  Port description: 1
```

```
Multipart-Reply:
  Switch description: 2
  Individual flow statistics: 3
  Aggregate flow statistics: 0
  Flow table statistics: 0
  Port statistics: 3
  Group counter statistics: 0
  Group description: 0
  Group features: 0
  Port description: 1
Barrier-Request: 3
Barrier-Reply: 3
Error Messages
Hello Failed Sent:
  Incompatible: 0
Hello Failed Recv:
  Incompatible: 0
Bad Request:
  Bad-Version: 0
  Bad-Type: 0
  Bad-Multipart: 0
  Permission-error: 0
  Bad-Len: 0
  Buffer-Empty: 0
  Buffer-Unknown: 0
  Bad-Table-ID: 0
  Bad-Port: 0
  Bad-Packet: 0
  Multipart-Buffer-Overflow: 0
Bad Action:
  Bad-Type: 0
  Bad-Len: 0
  Bad-Out-Port: 0
  Bad-Argument: 0
  Permission-Error: 0
  Too-many: 0
  Bad-Out-Group: 0
  Match-Inconsistent: 0
  Unsupported-Order: 0
  Bad-Set-Type: 0
  Bad-Set-Len: 0
  Bad-Set-Argument: 0
Bad Instruction:
  Unknown-Instruction: 0
  Unsupport-Instruction: 0
  Bad-Len: 0
  Permission-Error: 0
Bad Match:
  Bad-Type: 0
  Bad-Len: 0
  Bad-MAC-Addr-Mask: 0
  Bad-IP-Addr-Mask: 0
  Bad-Wildcards: 0
  Bad-Field: 0
  Bad-Value: 0
  Bad-Mask: 0
  Bad-Prerequisites: 0
  Duplicated-Field: 0
```

```

Flow-Mod-Failed:
  Unknown: 0
  Table-Full: 0
  Bad-Table-ID: 0
  Overlap: 0
  Permission-Error: 0
  Bad-Timeout: 0
  Bad-Command: 0
  Bad-Flags: 0
Group-Mod-Failed:
  Group-Exists: 0
  Invalid-Group: 0
  Weight-Unsupported: 0
  Out-of-Groups: 0
  Out-of-Buckets: 0
  Chaining-Unsupported: 0
  Watch-Unsupported: 0
  Loop: 0
  Unknown-Group: 0
  Chained-Group: 0
  Bad-Type: 0
  Bad-Command: 0
  Bad-Bucket: 0
  Bad-Watch: 0
  Permission-Error: 0
Port-Mod-Failed:
  Bad-Port: 0
  Bad-hw-addr: 0
  Bad-Config: 0
  Bad-Advertise: 0
  Permission-Error: 0
Switch-Config-Failed:
  Bad-Flags: 0
  Permission-Error: 0
-----
Openflow instance 2 is currently disabled

```

**Table 132.** *OpenFlow Table Statistics*

Parameter	Description
<b>Flow Count</b>	
Basic Flows	Count of flows stored in the basic flow table, sorted by type: ACL, unicast FDB and multicast FDB.
Emergency Flows	Count of flows stored in the emergency flow table, sorted by type: ACL, unicast FDB and multicast FDB.
Static Flows	Count of flows stored in the static flow table, sorted by type: ACL, MPLS push and MPLS pop. Available only in OpenFlow 1.3.
Dynamic Flows	Count of flows stored in the dynamic flow table, sorted by type: ACL, unicast FDB, multicast FDB, MPLS push and MPLS pop. Available only in OpenFlow 1.3.
<b>Buffering Count</b>	
Openflow Packets Buffered	Count of packets buffered.



Parameter	Description
Openflow Packets Timed out	Count of buffered packets dropped due to time out.
Openflow Packets Retrieved	Count of packets retrieved.
Openflow Packets Retrieve attempts	Count of attempts made to retrieve the buffer.
Message Count	Count of messages exchanged between Controller and switch.
Hello-Sent	Count of Hello messages sent from the switch to Controller.
Hello-Received	Count of Hello messages received by the Controller from the switch.
Echo-Request-Sent	Count of Echo Request messages sent from the switch to Controller.
Echo-Request-Received	Count of Echo Request messages received by the switch from the Controller.
Echo-Reply-Sent	Count of Echo Reply messages received by the switch from the Controller.
Echo-Reply-Received	Count of Echo Reply messages received by the switch from the Controller.
Vendor	Count of Vendor messages received by the switch from the Controller. Available only in OpenFlow 1.0.
<b>Vendor Flow-Mod</b>	Available only in OpenFlow 1.0
Add	Count of vendor-defined add flow_mod messages received by the switch. Available only in OpenFlow 1.0.
Modify	Count of vendor-defined modify flow_mod messages received by the switch. Available only in OpenFlow 1.0.
Modify-Strict	Count of vendor-defined modify_strict flow_mod messages received by the switch. Available only in OpenFlow 1.0.
Delete	Count of vendor-defined delete flow_mod messages received by the switch. Available only in OpenFlow 1.0.
Delete-Strict	Count of vendor-defined delete_strict flow_mod messages received by the switch. Available only in OpenFlow 1.0.
Feature-Request	Count of Feature Request messages received by the switch from the Controller.
Feature-Reply	Count of Feature Reply messages sent from the switch to the Controller.

<b>Parameter</b>	<b>Description</b>
Get-Config-Request	Count of <b>Get Config Request</b> messages received by the switch from the Controller.
Get-Config-Reply	Count of <b>Get Config Reply</b> messages sent from the switch to the Controller.
Set-Config	Count of <b>Set Config</b> messages received from the Controller.
<b>Packet-In</b>	
No-Match	Count of <b>Packet - In</b> messages sent to Controller due to no matching flows.
Action	Count of <b>Packet - In</b> messages sent to Controller due to action explicitly asking to forward to Controller.
Action Mirror	Count of NEC specific <b>Packet - In</b> messages sent to Controller due to action explicitly asking to forward to Controller. Available only in OpenFlow 1.0.
<b>Flow-Removed</b>	
Idle-Timeout	Count of flow entries removed due to idle-timeout expiration.
Hard-Timeout	Count of flow entries removed due to hard-timeout expiration.
Delete	Count of flow entries removed due to explicit deletion.
Group-Delete	Count of flow entries removed due to deletion of associated group. Available only in OpenFlow 1.3.
<b>Vendor-Flow-Removed</b>	Available only in OpenFlow 1.0
Idle-Timeout	Count of vendor-defined flow entries removed due to idle-timeout expiration. Available only in OpenFlow 1.0.
Hard-Timeout	Count of vendor-defined flow entries removed due to hard-timeout expiration. Available only in OpenFlow 1.0.
Delete	Count of vendor-defined flow entries removed due to explicit deletion. Available only in OpenFlow 1.0.
<b>Port-Status</b>	
Add	Count of <b>port - status</b> messages sent triggered by adding a port to OpenFlow.
Delete	Count of <b>port - status</b> messages sent triggered by removing a port from OpenFlow.
Modify	Count of <b>port - status</b> messages sent triggered by a modification of a port belonging to OpenFlow (for example, up/down status).

Parameter	Description
Packet-Out	Count of packet - out messages received from the Controller.
<b>Flow-Mod</b>	
Add	Count of add flow_mod messages received by the switch.
Modify	Count of modify flow_mod messages received by the switch.
Modify-Strict	Count of modify_strict flow_mod messages received by the switch.
Delete	Count of delete flow_mod messages received by the switch.
Delete-Strict	Count of delete-strict flow_mod messages received by the switch.
<b>Group-Mod</b>	Available only in OpenFlow 1.3
Add	Count of Group Add messages received from Controller. Available only in OpenFlow 1.3.
Modify	Count of Group Modify messages received from Controller. Available only in OpenFlow 1.3.
Delete	Count of Group Delete messages received from Controller. Available only in OpenFlow 1.3.
<b>Port-Mod</b>	Count of port_mod messages received by the switch from the Controller.
<b>Statistics-Request</b>	Available only in OpenFlow 1.0
Desc	Count of Description statistics requests received from the Controller. Available only in OpenFlow 1.0.
Flow	Count of Flow statistics requests received from the Controller. Available only in OpenFlow 1.0.
Aggregate	Count of Aggregate statistics requests received from the Controller. Available only in OpenFlow 1.0.
Table	Count of Table statistics requests received from the Controller. Available only in OpenFlow 1.0.
Port	Count of Port statistics requests received from the Controller. Available only in OpenFlow 1.0.
<b>Vendor</b>	Available only in OpenFlow 1.0
stats	Count of Vendor statistics requests received from the Controller. Available only in OpenFlow 1.0.
stats-strict	Count of Vendor strict statistics requests received from the Controller. Available only in OpenFlow 1.0.

<b>Parameter</b>	<b>Description</b>
<b>Statistics-Reply</b>	Available only in OpenFlow 1.0.
Desc	Count of Description statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Flow	Count of Flow statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Aggregate	Count of Aggregate statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Table	Count of Table statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Port	Count of Port statistics requests sent to the Controller. Available only in OpenFlow 1.0.
<b>Vendor</b>	Available only in OpenFlow 1.0.
stats	Count of Vendor statistics requests sent to the Controller. Available only in OpenFlow 1.0.
stats-strict	Count of Vendor strict statistics requests sent to the Controller. Available only in OpenFlow 1.0.
<b>Multipart-Request</b>	Available only in OpenFlow 1.3
Switch description	Count of Switch Description requests received from the Controller. Available only in OpenFlow 1.3.
Individual flow statistics	Count of Individual Flow statistics requests received from the Controller. Available only in OpenFlow 1.3.
Aggregate flow statistics	Count of Aggregate statistics requests received from the Controller. Available only in OpenFlow 1.3.
Flow table statistics	Count of Table statistics requests received from the Controller. Available only in OpenFlow 1.3.
Port statistics	Count of Port statistics requests received from the Controller. Available only in OpenFlow 1.3.
Group counter statistics	Count of Group statistics requests received from the Controller. Available only in OpenFlow 1.3.
Group description	Count of Group description requests received from the Controller. Available only in OpenFlow 1.3.
Group features	Count of Group features requests received from the Controller. Available only in OpenFlow 1.3.
Port description	Count of Port description requests received from the Controller. Available only in OpenFlow 1.3.
<b>Multipart-Reply</b>	Available only in OpenFlow 1.3
Switch description	Count of Switch Description replies sent to the Controller. Available only in OpenFlow 1.3.

<b>Parameter</b>	<b>Description</b>
Individual flow statistics	Count of Individual Flow statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Aggregate flow statistics	Count of Aggregate statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Flow table statistics	Count of Table statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Port statistics	Count of Port statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Group counter statistics	Count of Group statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Group description	Count of Group description replies sent to the Controller. Available only in OpenFlow 1.3.
Group features	Count of Group features replies sent to the Controller. Available only in OpenFlow 1.3.
Port description	Count of Port description replies sent to the Controller. Available only in OpenFlow 1.3.
<b>Barrier-Request</b>	Count of <code>barrier-request</code> messages received from the Controller.
<b>Barrier-Reply</b>	Count of <code>barrier-reply</code> messages sent to the Controller.
<b>Error Messages</b>	Count of error messages handled - sending/receiving error messages.
<b>Hello Failed Sent</b>	
Incompatible	Count of error messages sent by the switch if the version in the <code>HELLO</code> message is incompatible with the version in the Controller.
<b>Hello Failed Recv</b>	
Incompatible	Count of error messages received in the switch if the version in the <code>HELLO</code> message is incompatible with the version in the Controller.
<b>Bad Request</b>	
Bad-Version	Count of error messages sent due to <code>bad-version</code> in the request header.
Bad-Type	Count of error messages sent due to <code>bad-type</code> in the request header.
Bad-Stat	Count of error messages sent due to a specific statistics request that is not supported. Available only in OpenFlow 1.0.

Parameter	Description
Bad-Vendor	Count of error messages sent due to vendor-specific message that is not supported. Available only in OpenFlow 1.0.
Bad-Subtype	Count of error messages sent due to message subtype that is not supported. Available only in OpenFlow 1.0.
Bad-Multipart	Count of error messages sent due to unknown multipart request type specified in the <code>multipart-request</code> message. Available only in OpenFlow 1.3.
Permission-error	Count of error messages sent because the action received in the <code>flow-mod</code> message <code>Port-Mod-Failed</code> is not permitted. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong request length for type of message received in the request header.
Buffer-Empty	Count of error messages sent when the specified buffer in the request does not exist.
Buffer-Unknown	Count of error messages sent when the specified buffer in the request does not exist.
Bad-Table-ID	Count of error messages sent when the specified <code>table-id</code> in the request is invalid or the <code>table-id</code> doesn't exist. Available only in OpenFlow 1.3.
Bad-Port	Count of error messages sent due to invalid port in the <code>port-mod</code> message. Available only in OpenFlow 1.3.
Bad-Packet	Count of error messages sent when the specified packet is invalid in <code>packet-out</code> . Available only in OpenFlow 1.3.
Multipart-Buffer-Overflow	Count of error messages sent when the specified buffer in the <code>multi-part</code> request is overflowed. Available only in OpenFlow 1.3.
<b>Bad Action</b>	
Bad-Type	Count of error messages sent due to unknown action type specified in <code>flow_mod</code> message.
Bad-Len	Count of error messages sent due to wrong action length for type of message received in the <code>flow_mod</code> message.
Bad-Out-Port	Count of error message sent due to invalid port in the action field specified <code>flow_mod</code> message.
Bad-Argument	Count of error message sent due to bad action argument in <code>flow_mod</code> message that is not supported.
Permission-Error	Count of error message sent due to permission error while processing the <code>flow_mod</code> message received. Available only in OpenFlow 1.3.

Parameter	Description
Too-Many	Count of error message sent due to too many actions received in the <code>flow_mod</code> message that cannot be handled.
Bad-Out-Group	Count of error message sent due to inexistent group in the <code>flow_mod</code> message received. Available only in OpenFlow 1.3.
Match-Inconsistent	Count of error messages sent because the action cannot apply for this match or because there is a <code>set-field</code> missing prerequisite. Available only in OpenFlow 1.3.
Unsupported-Order	Count of error messages sent because the action order in an <code>apply-actions</code> instruction is unsupported for the action list. Available only in OpenFlow 1.3.
Bad-Set-Type	Count of error messages sent due to unsupported type in the <code>set-field</code> action. Available only in OpenFlow 1.3.
Bad-Set-Len	Count of error messages sent due to length problem in the <code>set-field</code> action. Available only in OpenFlow 1.3.
Bad-Set-Argument	Count of error messages sent due to bad argument in the <code>set-field</code> action. Available only in OpenFlow 1.3.
<b>Bad Instruction</b>	Available only in OpenFlow 1.3
Unknown-Instruction	Count of error messages sent due to unknown instruction in the received <code>flow-mod</code> message. Available only in OpenFlow 1.3.
Unsupport-Instruction	Count of error messages sent due to unsupported instruction in the received <code>flow-mod</code> message. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong instruction length. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the instruction. Available only in OpenFlow 1.3.
<b>Bad Match</b>	Available only in OpenFlow 1.3
Bad-Type	Count of error messages sent due to unsupported match type in the match. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong match length. Available only in OpenFlow 1.3.
Bad-MAC-Addr-Mask	Count of error messages sent due to unsupported MAC address mask in the match. Available only in OpenFlow 1.3.

Parameter	Description
Bad-IP-Addr-Mask	Count of error messages sent due to unsupported IP address mask in the match. Available only in OpenFlow 1.3.
Bad-Wildcards	Count of error messages sent due to unsupported combination of fields masked or omitted in the match. Available only in OpenFlow 1.3.
Bad-Field	Count of error messages sent due to unsupported field type in the match. Available only in OpenFlow 1.3.
Bad-Value	Count of error messages sent due to unsupported value in a match field. Available only in OpenFlow 1.3.
Bad-Mask	Count of error messages sent due to unsupported mask (neither a MAC address nor an IP address mask) in the match. Available only in OpenFlow 1.3.
Bad-Prerequisites	Count of error messages sent due to unfulfilled prerequisite in the match. Available only in OpenFlow 1.3.
Duplicated-Field	Count of error messages sent due to duplicated fields in the match. Available only in OpenFlow 1.3.
<b>Flow-Mod-Failed</b>	
All-Table-Full	Count of error messages due to table full when adding or updating <code>flow_mod</code> message. Available only in OpenFlow 1.0.
Unknown	Count of error messages sent when the error is unspecified. Available only in OpenFlow 1.3.
Table-Full	Count of error messages sent because of full table when adding or updating the <code>flow-mod</code> message. Available only in OpenFlow 1.3.
Bad-Table-ID	Count of error messages sent because the specified <code>table-id</code> in the <code>flow-mod</code> message is invalid or because the <code>table-id</code> doesn't exist. Available only in OpenFlow 1.3.
Overlap	Count of error messages sent due to an attempt to add overlapping <code>flow_mod</code> messages.
Permission-Error	Count of error messages due to permissions not available to perform action received in the <code>flow_mod</code> message <code>Port_Mod_Failed</code> .
Emergency-Timeout	Count of error messages sent due to invalid emergency-timeout in the <code>flow-mod</code> message. Available only in OpenFlow 1.0.
Bad-Timeout	Count of error messages sent when the specified idle/hard timeout in the <code>flow_mod</code> message is unsupported. Available only in OpenFlow 1.3.



Parameter	Description
Bad-Command	Count of error messages sent due to unknown command.
Unsupported	Count of error messages sent due to unsupported action list. Available only in OpenFlow 1.0.
Bad-Flags	Count of error messages sent when the specified flags in the <code>flow_mod</code> message are unsupported. Available only in OpenFlow 1.3.
<b>Group-Mod-Failed</b>	Available only in OpenFlow 1.3
Group-Exists	Count of error message sent to Controller due to already existing group. Available only in OpenFlow 1.3.
Invalid-Group	Count of error message sent to Controller due to invalid group. Available only in OpenFlow 1.3.
Weight-Unsupported	Count of error message sent to Controller due to unsupported "weight" parameter. Available only in OpenFlow 1.3.
Out-of-Groups	Count of error message sent to Controller due to full group table. Available only in OpenFlow 1.3.
Out-of-Buckets	Count of error message sent to Controller due to full bucket count per group. Available only in OpenFlow 1.3.
Chaining-Unsupported	Count of error message sent to Controller due to unsupported groups that forward to groups. Available only in OpenFlow 1.3.
Watch-Unsupported	Count of error message sent to Controller due to unsupported "watch" parameter. Available only in OpenFlow 1.3.
Loop	Count of error message sent to Controller due to unsupported checking that no loop is created while chaining groups. Available only in OpenFlow 1.3.
Unknown-Group	Count of error message sent to Controller due to unsupported group type. Available only in OpenFlow 1.3.
Chained-Group	Count of error message sent to Controller due to unsupported groups that forward to groups. Available only in OpenFlow 1.3.
Bad-Type	Count of error message sent to Controller due to wrong group type. Available only in OpenFlow 1.3.
Bad-Command	Count of error message sent to Controller due to unsupported command. Available only in OpenFlow 1.3.
Bad-Bucket	Count of error message sent to Controller due to error in bucket. Available only in OpenFlow 1.3.
Bad-Watch	Count of error message sent to Controller due to error in watch group. Available only in OpenFlow 1.3.

<b>Parameter</b>	<b>Description</b>
Permission-Error	Count of error message sent to Controller due permission error. Available only in OpenFlow 1.3.
<b>Port-Mod-Failed</b>	
Bad-Port	Count of error messages sent due to invalid port in <code>port_mod</code> message.
Bad-hw-addr	Count of error messages sent due to wrong hardware address specified in <code>port_mod</code> message.
Bad-Config	Count of error messages sent due to invalid <code>config</code> in the <code>port_mod</code> message. Available only in OpenFlow 1.3.
Bad-Advertise	Count of error messages sent due to invalid <code>advertise</code> in the <code>port_mod</code> message. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the <code>port_mod</code> message. Available only in OpenFlow 1.3.
<b>Switch-Config-Failed</b>	Available only in OpenFlow 1.3
Bad-Flags	Count of error messages sent due to invalid flags in the <code>switch-config</code> message. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the <code>switch-config</code> message. Available only in OpenFlow 1.3.

---

## Management Processor Statistics

The following commands display Management Processor statistics.

**Table 133.** *Management Processor Statistics Commands*

Command Syntax and Usage
<b>show mp i2c</b> Displays i2c statistics. <b>Command mode:</b> All
<b>show mp memory</b> Displays memory utilization statistics. <b>Command mode:</b> All
<b>show mp packet counters</b> Displays packet statistics, to check for leads and load. To view a sample output and a description of the statistics, see <a href="#">page 292</a> . <b>Command mode:</b> All
<b>show mp tcp-block</b> Displays all TCP control blocks that are in use. To view a sample output and a description of the statistics, see <a href="#">page 303</a> . <b>Command mode:</b> All
<b>show mp thread</b> Displays STEM thread statistics. This command is used by Technical Support personnel. <b>Command mode:</b> All
<b>show mp udp-block</b> Displays all UDP control blocks that are in use. To view a sample output, see <a href="#">page 304</a> . <b>Command mode:</b> All
<b>show processes cpu</b> Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see <a href="#">page 304</a> . <b>Command mode:</b> All
<b>show processes cpu history</b> Displays history of CPU utilization. To view a sample output, see <a href="#">page 306</a> . <b>Command mode:</b> All

## Packet Statistics

The following commands display Packet statistics.

**Table 134.** *Packet Statistics Commands*

Command Syntax and Usage
<b>show mp packet counters</b> Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see <a href="#">page 292</a> . <b>Command mode:</b> All
<b>clear mp packet logs</b> Clears all CPU packet statistics and logs. <b>Command mode:</b> Privileged EXEC

## MP Packet Statistics

The following command displays MP packet statistics:

**show mp packet counters**

**Command mode:** All

```
CPU packet statistics at 8:21:54 Tue Jan 8, 2013

Packet rate:          Incoming          Outgoing
-----
1-second:             8              7
4-seconds:            7              5
64-seconds:           4              3

Packet counters:      Received          Sent
-----
Total packets:        109056          148761
Since bootup:         109056          148768
BPDUs:                6415           19214
Cisco packets:        0              0
ARP Requests:         15             10061
ARP Replies:          8545           14
LACP packets:         3414           3420
IPv4 packets:         60130          116101
ICMP Requests:        0              21
ICMP Replies:         21             0
IGMP packets:         0              0
PIM packets:          0              0
VRRP packets:         0              0
TCP packets:          60088          116113
  FTP                  0              0
  HTTP                 0              0
  SSH                  3              3
  TACACS               0              0
  TELNET               60095          116145
TCP other              0              0
UDP packets:          24             9
  DHCP                0              0
  NTP                  0              0
  PTP                  0              0
```

```

RADIUS                0                0
SNMP                  0                0
TFTP                  0                0
UDP other             24                8
RIP packets:         0                1
OSPF packets:        0                0
BGP packets:         0                0
IPV6 packets:        0                0
LLDP PDUs:           3987               6876
FCoE FIP PDUs:       0                0
ECP PDUs:            0                0
MgmtSock Packets:    919               932
Other:                26549             0

Packet Buffer Statistics:
-----
allocs:                265803
frees:                 265806
failures:              0
dropped:               0

small packet buffers:
-----
current:                1
max:                    1024
threshold:              128
hi-watermark:          3
hi-water time:         3:39:12 Tue Jan  8, 2013

medium packet buffers:
-----
current:                0
max:                    2048
threshold:              50
hi-watermark:          1
hi-water time:         3:37:12 Tue Jan  8, 2013

jumbo packet buffers:
-----
current:                0
max:                    16
hi-watermark:          0

pkt_hdr statistics:
-----
current      :          0
max          :         3072
hi-watermark :          180
dropped     :          0
prio-dropped:          0

```

**Table 135.** *Packet Statistics*

Statistics	Description
<b>Packet Rate</b>	
1-second	The rate of incoming and outgoing packets over 1 second.
4-seconds	The rate of incoming and outgoing packets over 4 seconds.
64-seconds	The rate of incoming and outgoing packets over 64 seconds.

**Table 135.** *Packet Statistics (continued)*

<b>Statistics</b>	<b>Description</b>
<b>Packets Counters</b>	
Total packets	Total number of packets received.
Since bootup	Total number of packets received and sent since the last switch reboot.
BPDUs	Total number of spanning-tree Bridge Protocol Data Units received.
Cisco packets	Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received.
ARP packets	Total number of Address Resolution Protocol packets received.
IPv4 packets	Total number of IPv4 packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> <li>○ IGMP</li> <li>○ PIM</li> <li>○ ICMP requests</li> <li>○ ICMP replies</li> </ul>
TCP packets	Total number of TCP packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> <li>○ FTP</li> <li>○ HTTP</li> <li>○ SSH</li> <li>○ TACACS+</li> <li>○ Telnet</li> <li>○ Other</li> </ul>
UDP packets	Total number of UDP packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> <li>○ DHCP</li> <li>○ NTP</li> <li>○ RADIUS</li> <li>○ SNMP</li> <li>○ TFTP</li> <li>○ Other</li> </ul>
RIP packets	Total number of Routing Information Protocol packets received and sent.
OSPF packets	Total number of Open Shortest Path First packets received and sent.

**Table 135.** *Packet Statistics (continued)*

<b>Statistics</b>	<b>Description</b>
BGP packets	Total number of Border Gateway Protocol packets received and sent.
IPv6 packets	Total number of IPv6 packets received.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received.
ECP PDUs	Total number of Edge Control Protocol data units received and sent.
MgmtSock Packets	Total number of packets received and transmitted through the management port.
Other	Total number of other packets received.
<b>Packet Buffer Statistics</b>	
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
dropped	Total number of packets dropped by the packet buffer pool.
<b>small packet buffers</b>	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of small packet allocations supported.
threshold	Threshold value for small packet allocations, beyond which only high-priority small packets are allowed.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.

**Table 135.** *Packet Statistics (continued)*

<b>Statistics</b>	<b>Description</b>
<b>medium packet buffers</b>	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of medium packet allocations supported.
threshold	Threshold value for medium packet allocations, beyond which only high-priority medium packets are allowed.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
<b>jumbo packet buffers</b>	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of jumbo packet allocations supported.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
<b>pkt_hdr statistics</b>	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.



## Packet Statistics Log

These commands allow you to display a log of all packets received by CPU. The following table describes the Packet Statistics Log options.

**Table 136.** *Packet Statistics Log Options*

Command Syntax and Usage
<b>show mp packet logs all</b> Displays all packet logs received by and sent from the CPU. To view a sample output and a description of the log entries, see <a href="#">“Packet Log example” on page 297</a> . <b>Command mode:</b> All
<b>show mp packet logs rx</b> Displays all packets logs received by the CPU. <b>Command mode:</b> All
<b>show mp packet logs tx</b> Displays all packet logs sent from the CPU. <b>Command mode:</b> All

### *Packet Log example*

The following command displays all packet logs received by and sent from the CPU.

**show mp packet logs all**

Command mode: All

```
358. Type: BPDU, sent 1:01:11 Tue Mar 20, 2012
    Port EXT2, VLAN 201, Length 57, Reason 0x0, Flags 0x0
    Dst MAC: 01:80:c2:00:00:00, Src MAC: 08:17:f4:a7:57:2c

357. Type: ICMP ECHO Req, sent 1:01:09 Tue Mar 20, 2012
    Port MGT1, VLAN 4095, Length 16, Reason 0x0, Flags 0x0 FromMgmtSock
    Src IP: 9.43.98.125, Dst IP: 9.43.98.254
```

Each packet log entry includes the following information:

- Entry ID
- Packet type
- Date and time
- Port number
- VLAN number
- Packet length
- Reason code
- Flags
- Source and destination address

## Packet Statistics Last Packet

These commands allow you to display a specified number (*N*) of the most recent packet logs received by or sent from the CPU. The following table describes the Packet Statistics Last Packet options.

**Table 137.** *Last Packet Options*

Command Syntax and Usage
<b>show mp packet last both</b> <1-1000> Displays a specified number of recent packet logs received by and sent from the CPU. To view a sample output and a description, see <a href="#">“Packet Log example” on page 297</a> . <b>Command mode:</b> All
<b>show mp packet last rx</b> <1-1000> Displays a specified number of recent packet logs received by the CPU. <b>Command mode:</b> All
<b>show mp packet last tx</b> <1-1000> Displays a specified number of recent packet logs sent from the CPU. <b>Command mode:</b> All

## Packet Statistics Dump

The following table describes the Packet Statistics Dump options.

**Table 138.** *Packet Statistics Dump Options*

Command Syntax and Usage
<b>show mp packet dump all</b> Displays all packet statistics and logs received by and sent from the CPU. <b>Command mode:</b> All
<b>show mp packet dump rx</b> Displays all packet statistics and logs received by the CPU. <b>Command mode:</b> All
<b>show mp packet dump tx</b> Displays all packet statistics and logs sent from the CPU. <b>Command mode:</b> All

## Logged Packet Statistics

The following command displays logged packets that have been received or sent, based on the specified filter:

```
show mp packet parse {rx|tx} <arsing_option>
```

The filter options are described in [Table 139](#).

**Table 139.** *Packet Log Parsing Options*

<b>Command Syntax and Usage</b>
<pre><b>show mp packet parse {rx tx} arp</b> Displays only ARP packets logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} bgp</b> Displays only BGP packets logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} bpdud</b> Displays only BPDUs logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} cisco</b> Displays only Cisco packets (BPDU/CDP/UDLD) logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} dhcp</b> Displays only DHCP packets logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} ecp</b> Displays only ECP packets logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} fcoe</b> Displays only FCoE FIP PDUs logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} ftp</b> Displays only FTP packets logged. <b>Command mode:</b> All</pre>
<pre><b>show mp packet parse {rx tx} http</b> Displays only HTTP packets logged. <b>Command mode:</b> All</pre>

**Table 139.** *Packet Log Parsing Options (continued)*

<b>Command Syntax and Usage</b>
<b>show mp packet parse {rx tx} https</b> Displays only HTTPS packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} icmp</b> Displays only ICMP packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} igmp</b> Displays only IGMP packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} ip-addr &lt;IPv4_address&gt;</b> Displays only logged packets with the specified IPv4 address. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} ipv4</b> Displays only IPv4 packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} ipv6</b> Displays only IPv6 packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} lacp</b> Displays only LACP PDUs logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} lldp</b> Displays only LLDP PDUs logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} mac &lt;MAC_address&gt;</b> Displays only logged packets with the specified MAC address. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} mgmtsock</b> Displays only packets logged on management ports. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} ntp</b> Displays only NTP packets logged. <b>Command mode:</b> All

**Table 139.** *Packet Log Parsing Options (continued)*

<b>Command Syntax and Usage</b>
<b>show mp packet parse {rx tx} ospf</b> Displays only OSPF packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} other</b> Displays logs of all packets not explicitly selectable. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} pim</b> Displays only PIM packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} port &lt;port_number&gt;</b> Displays only logged packets with the specified port. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} radius</b> Displays only RADIUS packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} rarp</b> Displays only Reverse-ARP packets. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} raw</b> Displays raw packet buffer in addition to headers. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} rip</b> Displays only RIP packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} snmp</b> Displays only SNMP packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} ssh</b> Displays only SSH packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} tacacs</b> Displays only TACACS packets logged. <b>Command mode:</b> All

**Table 139.** *Packet Log Parsing Options (continued)*

<b>Command Syntax and Usage</b>
<b>show mp packet parse {rx tx} tcp</b> Displays only TCP packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} tcpother</b> Displays only TCP other-port packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} telnet</b> Displays only TELNET packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} tftp</b> Displays only TFTP packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} udp</b> Displays only UDP packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} udpother</b> Displays only UDP other-port packets logged. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} vlan &lt;VLAN_number&gt;</b> Displays only logged packets with the specified VLAN. <b>Command mode:</b> All
<b>show mp packet parse {rx tx} vrrp</b> Displays only VRRP logged packets. <b>Command mode:</b> All

## TCP Statistics

The following command displays TCP statistics:

**show mp tcp-block**

Command mode: All

```

Data Ports:
-----
All TCP allocated control blocks:
14835bd8:  0.0.0.0                0 <=>
           172.31.38.107         80 listen MGT up
147c6eb8:  0:0:0:0:0:0:0:0             0 <=>
           0:0:0:0:0:0:0:0             80 listen
147c6d68:  0.0.0.0                0 <=>
           0.0.0.0                80 listen
14823918:  172.31.37.42             55866 <=>
           172.31.38.107         23 established 0 ??
11af2394:  0.0.0.0                0 <=>
           172.31.38.107         23 listen MGT up
147e6808:  0.0.0.0                0 <=>
           0.0.0.0                23 listen
147e66b8:  0:0:0:0:0:0:0:0             0 <=>
           0:0:0:0:0:0:0:0             23 listen
147e6568:  0.0.0.0                0 <=>
           0.0.0.0                23 listen

Mgmt Ports:
-----
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 172.31.38.107:http     *:*                     LISTEN
tcp      0      0 172.31.38.107:telnet   *:*                     LISTEN
tcp      0      0 *:11000                 *:*                     LISTEN
tcp      0  1274 172.31.38.107:telnet   172.31.37.42:55866     ESTABLISHED

```

**Table 140.** *MP Specified TCP Statistics*

Statistics	Description
14835bd8	Memory
0.0.0.0	Destination IP address
0	Destination port
172.31.38.107	Source IP
80	Source port
listen MGT1 up	State

## UDP Statistics

The following command displays UDP statistics:

**show mp udp-block**

**Command mode:** All

```

Data Ports:
-----
All UDP allocated control blocks:
 68: listen
161: listen
500: listen
546: listen

Mgmt Ports:
-----
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 9.43.95.121:snmp        *:.*
0.0.0.0          0 <=> 9.43.95.121          161 accept MGT1 up
  
```

## CPU Statistics

The following commands display CPU utilization statistics:

**show mp cpu**

**Command mode:** All

CPU utilization	Highest	Thread	Time
-----	-----	-----	-----
cpuUtil1Second: 3%	83%	58 (I2C )	12:02:14 Fri Oct 14, 2011
cpuUtil4Seconds: 5%			
cpuUtil64Seconds: 5%			

**Table 141.** CPU Statistics

Statistics	Description
cpuUtil1Second	The use of MP CPU over 1 second. It shows the percentage, highest rate, thread, and time the highest utilization occurred.
cpuUtil4Seconds	The use of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The use of MP CPU over 64 seconds. It shows the percentage.
Highest	The highest percent of CPU use.
Thread	The thread ID and name of the thread that caused the highest CPU use.
Time	The time when the highest CPU use was reached.



## show processes cpu

Command mode: All

```

CPU Utilization at 8:25:55 Tue Jan 8, 2013

Total CPU Utilization: For 1 second: 2.92%
                       For 5 second: 3.38%
                       For 1 minute: 7.88%
                       For 5 minute: 8.93%

Highest CPU Utilization: thread 2 (STP ) at 6:44:56 Tue Jan 8, 2013

-----
Thread  Thread      Utilization      Status
  ID    Name         1sec      5sec      1Min      5Min
-----
  1     STEM         0.00%     0.00%     0.00%     0.00%     idle
  2     STP            0.00%     0.05%     0.10%     0.10%     idle
  3     MFDB           0.00%     0.00%     5.06%     5.22%     idle
  4     TND            0.00%     0.00%     0.00%     0.00%     idle
  5     CONS           0.00%     0.00%     0.00%     0.15%     suspended
  6     TNET           0.11%     0.58%     0.17%     0.27%     running
  7     TNET           0.00%     0.00%     0.00%     0.00%     idle
  8     TNET           0.00%     0.00%     0.00%     0.00%     idle
  9     TNET           0.00%     0.00%     0.00%     0.00%     idle
 10     LOG            0.00%     0.00%     0.00%     0.00%     idle
 11     TRAP           0.00%     0.00%     0.00%     0.00%     idle
 13     NTP            0.00%     0.00%     0.00%     0.00%     idle
 14     IP             0.04%     0.04%     0.06%     0.06%     idle
 17     IP             0.01%     0.08%     0.04%     0.04%     idle
 18     RIP            0.00%     0.00%     0.00%     0.00%     idle
 19     AGR            0.00%     0.00%     0.00%     0.00%     idle
 20     EPI            0.16%     0.27%     0.12%     0.10%     runnable
 22     PORT           0.00%     0.00%     0.00%     0.00%     idle
 24     BGP            0.18%     0.04%     0.00%     0.00%     idle
 32     SCAN           0.00%     0.00%     0.00%     0.00%     idle
 34     OSPF           0.20%     0.04%     0.02%     0.01%     idle
 36     SNMP           0.00%     0.00%     0.00%     0.00%     idle
 37     SNMP           0.00%     0.00%     0.00%     0.00%     idle
 38     SNMP           0.00%     0.00%     0.00%     0.00%     idle
 40     SSHD           0.00%     0.00%     0.00%     0.00%     idle
...
 120    VDPT           0.00%     0.00%     0.00%     0.00%     idle
 124    HIST           0.00%     0.00%     0.00%     0.00%     runnable
 128    NORM           0.00%     0.00%     0.00%     0.00%     idle
 129    NORM           0.00%     0.00%     0.00%     0.00%     idle
 130    DONE           0.00%     0.00%     0.00%     0.00%     idle

```

**Table 142.** CPU Statistics

Statistics	Description
Thread ID	The thread ID number.
Thread Name	The name of the thread.
1sec	The percent of CPU use over 1 second.
5sec	The percent of CPU use over 5 seconds.
1Min	The percent of CPU use over 1 minute.

**Table 142.** CPU Statistics

Statistics	Description
5Min	The percent of CPU use over 5 minutes.
Status	The status of the process.

## *CPU Statistics History*

The following command display a history of CPU use statistics:

**show processes cpu history**

**Command mode:** All

CPU Utilization History					
-----					
17	(IP )	98%	at	22:17:24	Mon Feb 20, 2012
59	(LACP)	9%	at	22:17:33	Mon Feb 20, 2012
110	(ETMR)	12%	at	22:17:34	Mon Feb 20, 2012
110	(ETMR)	12%	at	22:17:36	Mon Feb 20, 2012
110	(ETMR)	12%	at	22:17:40	Mon Feb 20, 2012
110	(ETMR)	12%	at	22:17:45	Mon Feb 20, 2012
110	(ETMR)	17%	at	22:17:47	Mon Feb 20, 2012
110	(ETMR)	18%	at	22:17:49	Mon Feb 20, 2012
110	(ETMR)	25%	at	22:20:28	Mon Feb 20, 2012
110	(ETMR)	26%	at	22:39:08	Mon Feb 20, 2012
37	(SNMP)	28%	at	22:46:20	Mon Feb 20, 2012
94	(PROX)	57%	at	23:29:36	Mon Feb 20, 2012
94	(PROX)	63%	at	23:29:37	Mon Feb 20, 2012
94	(PROX)	63%	at	23:29:39	Mon Feb 20, 2012
58	(I2C )	64%	at	16:21:54	Tue Feb 21, 2012
5	(CONS)	86%	at	18:41:54	Tue Feb 21, 2012
58	(I2C )	88%	at	18:41:55	Tue Feb 21, 2012
58	(I2C )	88%	at	21:29:41	Sat Feb 25, 2012
58	(I2C )	98%	at	12:04:59	Tue Feb 28, 2012
58	(I2C )	100%	at	11:31:32	Sat Mar 10, 2012

---

## Access Control List Statistics

The following commands display and change ACL statistics.

**Table 143.** *ACL Statistics Commands*

Command Syntax and Usage
<b>show access-control counters</b> Displays all ACL statistics. For output sample, see <a href="#">page 308</a> . <b>Command mode:</b> All
<b>show access-control list &lt;1-640&gt; counters</b> Displays the Access Control List Statistics for a specific ACL. <b>Command mode:</b> All
<b>show access-control list6 &lt;1-128&gt; counters</b> Displays the IPv6 ACL statistics for a specific ACL. <b>Command mode:</b> All
<b>show access-control macl &lt;1-128&gt; counters</b> Displays the ACL statistics for a specific management ACL (MACL). <b>Command mode:</b> All
<b>show access-control meter &lt;1-127&gt; counters</b> Displays ACL meter statistics. For output sample, see <a href="#">page 308</a> . <b>Command mode:</b> All
<b>show access-control vmap &lt;1-128&gt; counters</b> Displays VLAN Map statistics for the selected VMAP. For details, see <a href="#">page 308</a> . <b>Command mode:</b> All
<b>clear access-control list {&lt;1-640&gt; all} counters</b> Clears ACL statistics. <b>Command mode:</b> Privileged EXEC
<b>clear access-control list6 {&lt;1-128&gt; all}</b> Clears IPv6 ACL statistics. <b>Command mode:</b> Privileged EXEC
<b>clear access-control meter &lt;1-127&gt; counters</b> Clears ACL meter statistics. <b>Command mode:</b> Privileged EXEC

## ACL Statistics

The following command displays ACL statistics.

**show access-control counters**

Command mode: All

Hits for ACL 1:	26057515
Hits for ACL 2:	26057497

## ACL Meter Statistics

This option displays ACL meter statistics.

**show access-control meter <meter number> counters**

Command mode: All

Out of profile hits for Meter 1, Port EXT1:	0
Out of profile hits for Meter 2, Port EXT1:	0

## VMAP Statistics

The following command displays VLAN Map statistics.

**show access-control vmap <vmap number> counters**

Command mode: All

Hits for VMAP 1:	57515
------------------	-------

---

## Fibre Channel over Ethernet Statistics

The following command displays Fibre Channel over Ethernet (FCoE) statistics:

**show fcoe counters**

**Command mode:** All

```
FCF-keepalives statistics:
FCF 54:7f:ee:8f:d4:2a keepalives received : 62
FCOE statistics:
FCFAdded:                5   FCFRemoved:                1
FCOEAdded:               81  FCOERemoved:               24
```

Fibre Channel over Ethernet (FCoE) statistics are described in the following table:

**Table 144.** *FCoE Statistics*

Statistic	Description
FCFAdded	Total number of FCoE Forwarders (FCF) added.
FCFRemoved	Total number of FCoE Forwarders (FCF) removed.
FCOEAdded	Total number of FCoE connections added.
FCOERemoved	Total number of FCoE connections removed.

The total can accumulate over several FCoE sessions, until the statistics are cleared.

The following command clears Fibre Channel over Ethernet (FCoE) statistics:

**clear fcoe counters**

**Command mode:** All

## SNMP Statistics

The following command displays SNMP statistics:

**show snmp-server counters**

**Command mode:** All except User EXEC

SNMP statistics:			
snmpInPkts:	150097	snmpInBadVersions:	0
snmpInBadC'tyNames:	0	snmpInBadC'tyUses:	0
snmpInASNParseErrs:	0	snmpEnableAuthTraps:	0
snmpOutPkts:	150097	snmpInBadTypes:	0
snmpInTooBig:	0	snmpInNoSuchNames:	0
snmpInBadValues:	0	snmpInReadOnlys:	0
snmpInGenErrs:	0	snmpInTotalReqVars:	798464
snmpInTotalSetVars:	2731	snmpInGetRequests:	17593
snmpInGetNexts:	131389	snmpInSetRequests:	615
snmpInGetResponses:	0	snmpInTraps:	0
snmpOutTooBig:	0	snmpOutNoSuchNames:	1
snmpOutBadValues:	0	snmpOutReadOnlys:	0
snmpOutGenErrs:	1	snmpOutGetRequests:	0
snmpOutGetNexts:	0	snmpOutSetRequests:	0
snmpOutGetResponses:	150093	snmpOutTraps:	4
snmpSilentDrops:	0	snmpProxyDrops:	0

**Table 145.** *SNMP Statistics*

Statistic	Description
snmpInPkts	The total number of Messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadC'tyNames	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
snmpInBadC'tyUses	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.

**Table 145.** *SNMP Statistics (continued)*

Statistic	Description
snmpInASNParseErrs	<p>The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received.</p> <p><b>Note:</b> OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.</p>
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
snmpInTooBig	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>too big</i> .
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>noSuchName</i> .
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> .
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>'read-Only'</i> . It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value <i>'read-Only'</i> in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.

**Table 145.** *SNMP Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is <code>genErr</code> .
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBig	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <code>too big</code> .
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is <code>noSuchName</code> .
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <code>badValue</code> .
snmpOutReadOnly	Not in use.



**Table 145.** *SNMP Statistics (continued)*

<b>Statistic</b>	<b>Description</b>
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <code>genErr</code> .
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -PDUs delivered to the SNMPv2 entity which were silently dropped because the size of a reply containing an alternate <code>Response</code> -PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	The total number of <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no <code>Response</code> -PDU could be returned.

---

## NTP Statistics

Enterprise NOS uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

The following command displays NTP statistics:

**show ntp counters**

**Command mode:** All

```
NTP statistics:
  Primary Server:
    Requests Sent:           17
    Responses Received:     17
    Updates:                 1
  Secondary Server:
    Requests Sent:           0
    Responses Received:     0
    Updates:                 0

Last update based on response from primary/secondary server.
Last update time: 18:04:16 Tue Jul 13, 2010
Current system time: 18:55:49 Tue Jul 13, 2010
```

**Table 146.** *NTP Statistics*

Field	Description
Primary Server	<ul style="list-style-type: none"><li>● <b>Requests Sent:</b> The total number of NTP requests the switch sent to the primary NTP server to synchronize time.</li><li>● <b>Responses Received:</b> The total number of NTP responses received from the primary NTP server.</li><li>● <b>Updates:</b> The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.</li></ul>
Secondary Server	<ul style="list-style-type: none"><li>● <b>Requests Sent:</b> The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.</li><li>● <b>Responses Received:</b> The total number of NTP responses received from the secondary NTP server.</li><li>● <b>Updates:</b> The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.</li></ul>
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.

**Table 146.** *NTP Statistics (continued)*

Field	Description
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the command was issued.

The following command displays information about NTP associated peers:

**show ntp associations**

**Command mode:** All

address	ref clock	st	when(s)	offset(s)
*12.200.151.18	198.72.72.10	3	35316	-2
*synced, #unsynced				

**Table 147.** *NTP Associations*

Field	Description
address	Peer address
ref clock	Peer reference clock address
st	Peer stratum
when(s)	Time in seconds since the latest NTP packet was received from the peer
offset(s)	Offset in seconds between the peer clock and local clock

---

## PTP Statistics

The following table displays Precision Time Protocol statistics commands:

**Table 148.** *Precision Time Protocol Statistics Commands*

Command Syntax and Usage
<b>show ptp counters</b> Displays Precision Time Protocol statistics. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; ptp-counters</b> Displays Precision Time Protocol statistics for the port. <b>Command mode:</b> All
<b>clear ptp counters</b> Resets PTP packet counters. <b>Command mode:</b> Privileged EXEC

Use the following command to display Precision Time Protocol traffic statistics:

**show ptp counters**

**Command mode:** All

```
Precision time protocol counters:
+-----+
|Received Announce messages:      0|
|Received Sync messages:          0|
|Received Follow-Up messages:     0|
|Received Delay-Request messages:  0|
|Received Delay-Response messages: 0|
+-----+
|Sent Announce messages:          0|
|Sent Sync messages:              0|
|Sent Follow-Up messages:         0|
|Sent Delay-Request messages:     0|
|Sent Delay-Response messages:    0|
+-----+
```

PTP statistics include the following:

- total number of Announce messages transmitted and received.
- total number of Sync transmitted and received.
- total number of Follow\_Up messages transmitted and received
- total number of Delay\_Req messages transmitted and received
- total number of Delay\_Resp messages transmitted and received

---

## SLP Statistics

The following table displays SLP statistics commands:

**Table 149.** *SLP Statistics Commands*

Command Syntax and Usage
<b>show ip slp counter</b> Displays SLP packet counters. <b>Command mode:</b> All
<b>clear ip slp counters</b> Clears SLP packet counters. <b>Command mode:</b> Privileged EXEC

Use the following command to display SLP packet counters:

**show ip slp counter**

**Command mode:** All

SLP Send Counters:	
SLP DAAdvert	: 0
SLP SrvRqst	: 0
SLP SrvRply	: 0
SLP SrvAck	: 0
SLP AttrRqst	: 0
SLP AttrRply	: 0
SLP SrvTypeRqst	: 0
SLP SrvReg	: 0
SLP SrvDeReg	: 0
SLP SrvTypeRply	: 0
SLP SAAdvert	: 0
SLP Unknown	: 0
SLP Receive Counters:	
SLP DAAdvert	: 0
SLP SrvRqst	: 0
SLP SrvRply	: 0
SLP SrvAck	: 0
SLP AttrRqst	: 0
SLP AttrRply	: 0
SLP SrvTypeRqst	: 0
SLP SrvReg	: 0
SLP SrvDeReg	: 0
SLP SrvTypeRply	: 0
SLP SAAdvert	: 0
SLP Dropped	: 0
Incorect pkt/dest	: 0
Scopes mismatch	: 0
Others	: 0

## Statistics Dump

The following command dumps switch statistics:

**show counters**

**Command mode:** All

```
CPU Utilization at 12:13:08 Thu Mar 12, 2015

Total CPU Utilization: For 1 second: 0.06%
                       For 5 second: 0.33%
                       For 1 minute: 0.12%
                       For 5 minute: 0.11%

Highest CPU Utilization: thread 16 (IP ) at 14:12:23 Wed Feb 25, 2015

-----
Thread  Thread          Utilization          Status
  ID    Name             1sec      5sec      1Min      5Min
-----
  1     STEM             0.00%     0.00%     0.00%     0.00%     idle
  2     STP                 0.00%     0.00%     0.00%     0.00%     idle
  3     MFDB                 0.00%     0.00%     0.00%     0.00%     idle
  4     TND                  0.00%     0.00%     0.00%     0.00%     idle
  5     CONS                 0.01%     0.02%     0.00%     0.01%     running
  6     TNET                 0.00%     0.00%     0.00%     0.00%     idle
  7     TNET                 0.00%     0.00%     0.00%     0.00%     idle
  8     TNET                 0.00%     0.00%     0.00%     0.00%     idle
  9     TNET                 0.00%     0.00%     0.00%     0.00%     idle
 10     LOG                  0.00%     0.00%     0.00%     0.00%     idle
 11     TRAP                 0.00%     0.00%     0.00%     0.00%     idle
 12     NTP                  0.00%     0.00%     0.00%     0.00%     idle
 13     RMON                 0.00%     0.00%     0.00%     0.00%     idle
 16     IP                   0.00%     0.01%     0.01%     0.01%     idle
 18     AGR                  0.00%     0.00%     0.00%     0.00%     idle
 19     EPI                  0.00%     0.00%     0.00%     0.00%     idle
 20     PORT                 0.00%     0.00%     0.00%     0.00%     idle
 25     MGMT                 0.01%     0.01%     0.01%     0.02%     idle
 28     SNMP                 0.00%     0.00%     0.01%     0.00%     idle
 29     SNMP                 0.00%     0.00%     0.00%     0.00%     idle
 31     SSHD                 0.00%     0.00%     0.00%     0.00%     idle
 33     TEAM                 0.00%     0.00%     0.00%     0.00%     idle
 34     I2C                  0.00%     0.00%     0.00%     0.00%     idle
 35     LACP                 0.01%     0.25%     0.04%     0.02%     idle
 36     SFP                  0.00%     0.00%     0.00%     0.00%     idle
 37     L3HS                 0.00%     0.00%     0.00%     0.00%     idle
 38     HLNK                 0.00%     0.00%     0.00%     0.00%     idle
 39     LLDP                 0.00%     0.00%     0.01%     0.02%     idle
 40     IPV6                 0.00%     0.01%     0.00%     0.00%     idle
...

```

Use the dump command to dump all switch statistics (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

---

## Chapter 4. Configuration Commands

This chapter discusses how to use the Command Line Interface (CLI) for making, viewing, and saving switch configuration changes. Many of the commands, although not new, display more or different information than in the previous version. Important differences are called out in the text.

**Table 150.** *General Configuration Commands*

<b>Command Syntax and Usage</b>
<p><b>show running-config [diff]</b></p> <p>Dumps current configuration to a script file. The <b>diff</b> option displays only the running configuration changes that have been applied but not saved to flash memory. For details, see <a href="#">page 605</a>.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>copy running-config backup-config</b></p> <p>Copy the current (running) configuration from switch memory to the backup-config partition. For details, see <a href="#">page 606</a>.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>copy running-config startup-config</b></p> <p>Copy the current (running) configuration from switch memory to the startup-config partition.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>copy running-config {ftp sftp tftp} [data-port extm-port  mgt-port]</b></p> <p>Backs up current configuration to a file on the selected FTP/TFTP/SFTP server. Select a management port, or press <b>Enter</b> to use the default (management) port.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>copy {ftp sftp tftp} running-config [data-port extm-port  mgt-port]</b></p> <p>Restores current configuration from a FTP/TFTP/SFTP server. Select a management port, or press <b>Enter</b> to use the default (management) port. For details, see <a href="#">page 607</a>.</p> <p><b>Command mode:</b> All except User EXEC</p>

**Table 150.** *General Configuration Commands*

<b>Command Syntax and Usage</b>
<p><b>copy {sftp tftp} {ca-cert host-key host-cert host-cert-only public-key} [data-port extm-port mgt-port]</b></p> <p>Imports interface used by NIST certified test laboratories for USGv6 (NIST SP 500-267) certification purposes. Required for RSA digital signature authentication verification during IKEv2 interoperability testing. Uses TFTP or SFTP to import:</p> <ul style="list-style-type: none"><li>o ca-cert: Certificate Authority root certificate</li><li>o host-key: host private key</li><li>o host-cert: host public key</li><li>o host-cert-only: host private key generated on the switch</li><li>o public-key: client public key</li><li>o data-port: data port</li><li>o extm-port: external management port</li><li>o mgt-port: management port</li></ul> <p><b>Command mode:</b> All except User EXEC</p>



---

## Viewing and Saving Changes

As you use the configuration commands to set switch parameters, the changes you make take effect immediately. You do not need to apply them. Configuration changes are lost the next time the switch boots, unless you save the changes.

You can view all running configuration changes that have been applied but not saved to flash memory using the `show running-config diff` command in Privileged EXEC mode.

**Note:** Some operations can override the settings of the Configuration commands. Therefore, settings you view using the Configuration commands (for example, port status) might differ from run-time information that you view using the Information commands. The Information commands display current run-time information of switch parameters.

## Saving the Configuration

You must save configuration settings to flash memory, so the EN4093R reloads the settings after a reset.

**Note:** If you do not save the changes, they will be lost the next time the system is rebooted.

To save the new configuration, enter one of the following commands:

```
EN 4093# copy running-config startup-config
```

or

```
EN 4093# write
```

**Note:** The `write` command doesn't prompt the user for confirmation.

When you save configuration changes, the changes are saved to the *active* configuration block. For instructions on selecting the configuration to run at the next system reset, see [“Selecting a Configuration Block” on page 636](#).

---

## System Configuration

These commands provide configuration of switch management parameters such as user and administrator privilege mode passwords, Web-based management settings, and management access lists.

**Table 151.** *System Configuration Commands*

Command Syntax and Usage
<p><b>[no] banner</b> &lt;1-80 characters&gt;</p> <p>Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the <code>show sys-info</code> command.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] boot strict enable</b></p> <p>Enables or disables switch operation in security strict mode. When enabled, the authentication and privacy protocols and algorithms of the device are compliant with NIST SP-800-131A, with non-compliant protocols and algorithms disabled.</p> <p>Setting will be applied and device will be reset to default factory configuration after reboot.</p> <p>The default setting is <code>disabled</code>.</p> <p><b>Note:</b> Ensure NIST Strict compliance is enabled on the Chassis Management Module before enabling Strict mode operation on the device.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] boot siom</b></p> <p>Enables or disables SIOM on the switch.</p> <p>You must reboot the switch for this change to take effect.</p> <p>The default setting is <code>disabled</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>easyconnect</b></p> <p>Allows to apply a series of customizable and predefined configurations based on common deployment scenarios. The EasyConnect (EZC) wizard will display the available configuration options. For more details on using the EZC wizard, see the <i>Lenovo Flex System EN4093R 10Gb Ethernet Scalable Switch Application Guide for Lenovo Enterprise Network Operating System 8.4</i>.</p> <p><b>Note:</b> Not available in stacking.</p> <p>Command mode: Privileged EXEC</p>
<p><b>[no] hostname</b> &lt;character string&gt;</p> <p>Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).</p> <p><b>Command mode:</b> Global configuration</p>

**Table 151.** *System Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>line console length</b> &lt;0-300&gt;</p> <p>Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging.</p> <p>The default value is 28.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no line console</b></p> <p>Sets <code>line console length</code> to the default value of 28.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>line vty length</b> &lt;0-300&gt;</p> <p>Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging.</p> <p>The default value is 28.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no line vty</b></p> <p>Sets <code>line vty length</code> to the default value of 28.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>system date</b> &lt;yyyy&gt; &lt;mm&gt; &lt;dd&gt;</p> <p>Prompts the user for the system date. The date retains its value when the switch is reset.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] system daylight</b></p> <p>Enables or disables daylight saving time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock.</p> <p>By default, this option is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] system dhcp [extm mgt]</b></p> <p>Enables or disables Dynamic Host Control Protocol for setting the IP address on the selected interface. When enabled, the IP address obtained from the DHCP server overrides the static IP address.</p> <p>The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] system dhcp {hostname syslog}</b></p> <p>Enables or disables hostname or log server options support for DHCP/BOOTP client.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 151.** *System Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>system idle</b> &lt;0-60&gt;</p> <p>Sets the idle timeout for CLI sessions in minutes. A value of 0 disables system idle.</p> <p>The default value is 10 minutes.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>system linkscan {fast normal slow}</b></p> <p>Configures the link scan interval used to poll the status of ports.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] system notice</b> &lt;maximum 1024 character multi-line login notice&gt; &lt;'.' to end&gt;</p> <p>Enables or disables the display of a login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] system packet-logging</b></p> <p>Enables or disables logging of packets that come to the CPU.</p> <p>The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] system reset-control</b></p> <p>Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>system time</b> &lt;hh&gt;:&lt;mm&gt;:&lt;ss&gt;</p> <p>Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>system timezone</b></p> <p>Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Saving Time, etc.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 151.** *System Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>terminal dont-ask</b></p> <p>Disables CLI confirmation prompts for the current session. The switch will choose the default answer.</p> <p><b>Note:</b> When using this command any settings configured through the <b>prompting</b> command will be temporarily disregarded for the duration of the current session.</p> <p><b>Command mode:</b> All</p>
<p><b>no terminal dont-ask</b></p> <p>Enables CLI confirmation prompts for the current session.</p> <p><b>Note:</b> When using this command any settings configured through the <b>prompting</b> command will be temporarily disregarded for the duration of the current session.</p> <p><b>Command mode:</b> All</p>
<p><b>terminal-length</b> &lt;0-300&gt;</p> <p>Configures the number of lines per screen displayed in the CLI for the current session. A value of 0 disables paging. By default, it is set to the corresponding line vty length or line console length value in effect at login.</p> <p><b>Command mode:</b> All</p>
<p><b>show boot strict</b></p> <p>Displays the current security strict mode status.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show boot security-policy</b></p> <p>Displays the current security policy configuration.</p> <p><b>Note:</b> The security policy is configurable only through the CMM tool.</p> <p><b>Command mode:</b> All</p>
<p><b>show boot siom</b></p> <p>Displays the current SIOM setting and the SIOM setting that will take effect after reboot.</p> <p><b>Command mode:</b> All</p>
<p><b>show system</b></p> <p>Displays the current system parameters.</p> <p><b>Command mode:</b> All</p>

## System Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

**Table 152.** *Error Disable Configuration Commands*

Command Syntax and Usage
<p><b>[no] errdisable recovery</b></p> <p>Globally enables or disables automatic error-recovery for error-disabled ports. The default setting is <b>disabled</b>.</p> <p><b>Note:</b> Each port must have error-recovery enabled to participate in automatic error recovery.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>errdisable timeout</b> &lt;30-86400&gt;</p> <p>Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port.</p> <p>The default value is 300 seconds.</p> <p><b>Note:</b> When you change the timeout value, all current error-recovery timers are reset.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show errdisable</b></p> <p>Displays the current system Error Disable configuration.</p> <p><b>Command mode:</b> All</p>

## Link Flap Dampening Configuration

The Link Flap Dampening feature allows the switch to automatically disable a port if too many link flaps (link up/link down) are detected on the port during a specified time interval. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed.

**Table 153.** *Link Flap Dampening Configuration Options*

<b>Command Syntax and Usage</b>
<b>[no] errdisable link-flap enable</b> Enables or disables Link Flap Dampening. <b>Command mode:</b> Global configuration
<b>errdisable link-flap max-flaps &lt;1-100&gt;</b> Configures the maximum number of link flaps allowed in the configured time period. The default value is 5. <b>Command mode:</b> Global configuration
<b>errdisable link-flap time &lt;5-500&gt;</b> Configures the time period, in seconds. The default value is 30 seconds. <b>Command mode:</b> Global configuration
<b>show errdisable link-flap</b> Displays the current Link Flap Dampening parameters. <b>Command mode:</b> All

## System Host Log Configuration

The following table displays System Host Log configuration commands.

**Table 154.** *Host Log Configuration Commands*

Command Syntax and Usage
<p><b>[no] logging buffer severity</b> &lt;0-7&gt;</p> <p>Sets the severity level of system log messages that are written to flash buffer. The system saves only messages with the selected severity level and above. For example, if you set the buffer severity to 2, only messages with severity level of 1 and 2 are saved.</p> <p>The default is 7, which means log all severity levels.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] logging console</b></p> <p>Enables or disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages.</p> <p>The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>logging console severity</b> &lt;0-7&gt;</p> <p>Sets the severity level of system log messages to display via the console, Telnet, and SSH. The system displays only messages with the selected severity level and above. For example, if you set the console severity to 2, only messages with severity level of 1 and 2 are displayed.</p> <p>The default is 7, which means log all severity levels.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no logging console severity</b></p> <p>Disables delivering syslog messages to the console based on severity.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>logging host</b> &lt;1-2&gt; <b>address</b> &lt;IP address&gt; [<b>data-port</b>   <b>extm-port</b>   <b>mgt-port</b>]</p> <p>Sets the IPv4 address of the first or second syslog host.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>logging host</b> &lt;1-2&gt; <b>address6</b> &lt;IPv6 address&gt; [<b>data-port</b>   <b>extm-port</b>   <b>mgt-port</b>]</p> <p>Sets the IPv6 address of the first or second syslog host.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>logging host</b> &lt;1-2&gt; <b>facility</b> &lt;0-7&gt;</p> <p>This option sets the facility level of the first or second syslog host displayed.</p> <p>The default is 0.</p> <p><b>Command mode:</b> Global configuration</p>



**Table 154.** Host Log Configuration Commands

Command Syntax and Usage
<p><b>logging host</b> &lt;1-2&gt; <b>severity</b> &lt;0-7&gt;</p> <p>This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all severity levels.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no logging host</b> &lt;1-2&gt;</p> <p>Removes the specified syslog host.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] logging log {all &lt;feature&gt;}</b></p> <p>Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as vlans, stg, or ssh), or enable/disable syslog on all available features.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] logging pdrop enable</b></p> <p>Enables or disables packet drop logging.</p> <p>By default, the switch generates these messages once every 30 minutes.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>logging pdrop interval</b> &lt;0-30&gt;</p> <p>Sets the packet drop logging interval, in minutes.</p> <p>The default value is 30.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] logging synchronous [level &lt;0-7&gt;   all]</b></p> <p>Enables or disables synchronous logging messages. When <b>enabled</b>, logging messages are displayed asynchronously.</p> <p>The <b>level</b> parameter sets the message severity level. Messages with a severity level equal to or higher than this value are displayed asynchronously. Low numbers indicate greater severity. <b>All</b> displays all messages asynchronously, regardless the severity level.</p> <p>The default setting is 2.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>logging source-interface loopback</b> &lt;1-5&gt;</p> <p>Sets the loopback interface number for syslogs.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 154.** *Host Log Configuration Commands*

<b>Command Syntax and Usage</b>
<p><b>no logging source-interface loopback</b></p> <p>Removes the loopback interface for syslogs.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show logging [severity &lt;severity level&gt;] [reverse]</b></p> <p>Displays the current syslog settings, followed by the most recent 2000 syslog messages, as displayed by the <code>show logging messages</code> command. For details, see <a href="#">page 47</a>.</p> <p>The <code>reverse</code> option displays the output in reverse order, from the newest entry to the oldest.</p> <p><b>Command mode:</b> All</p>

## SSH Server Configuration

For the EN4093R 10Gb Ethernet Scalable Switch, these commands enable Secure Shell access from any SSH client.

**Table 155.** *SSH Server Configuration Commands*

Command Syntax and Usage
<p><b>[no] ssh enable</b>            Enables or disables the SSH server.  <b>Command mode:</b> Global configuration</p>
<p><b>ssh generate-host-key</b>            Generate the RSA host key.  <b>Command mode:</b> Global configuration</p>
<p><b>ssh maxauthattempts &lt;1-20&gt;</b>            Sets the maximum number of SSH authentication attempts.            The default value is 2.  <b>Command mode:</b> Global configuration</p>
<p><b>no ssh maxauthattempts</b>            Resets the maximum number of SSH authentication attempts to its default value of 2.  <b>Command mode:</b> Global configuration</p>
<p><b>ssh port &lt;TCP port number&gt;</b>            Sets the SSH server port number.            The default port number is 22.  <b>Command mode:</b> Global configuration</p>
<p><b>no ssh port</b>            Resets the SSH server port to the default port number 22.  <b>Command mode:</b> Global configuration</p>
<p><b>ssh public-key index &lt;1-100&gt; {adduser deluser} username &lt;user name&gt;</b>            Assigns another user name for existing public keys or removes a user name.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] ssh scp-enable</b>            Enables or disables the SCP apply and save.  <b>Command mode:</b> Global configuration</p>
<p><b>ssh scp-password</b>            Set the administration password for SCP access.  <b>Command mode:</b> Global configuration</p>

**Table 155.** SSH Server Configuration Commands

Command Syntax and Usage
<p><b>show ssh</b></p> <p>Displays the current SSH server configuration.</p> <p><b>Command mode:</b> All</p>
<p><b>show ssh-clienthostkey {address &lt;SFTP server IP address&gt; all}</b></p> <p>Displays the current SFTP/SSH host key configuration.</p> <ul style="list-style-type: none"><li>o address : Displays a specific SFTP/SSH host key</li><li>o all : Displays all SFTP/SSH host keys</li></ul> <p><b>Commands mode:</b> All</p>
<p><b>show ssh-clientpubkey {all index &lt;1-100&gt; username &lt;user name&gt;}</b></p> <p>Displays the current SSH public key configuration.</p> <ul style="list-style-type: none"><li>o all : Displays all SSH public keys</li><li>o index : Displays a specific SSH public key</li><li>o username : Displays all the SSH public keys of a particular user</li></ul> <p><b>Command mode:</b> All</p>
<p><b>clear ssh-clienthostkey {address &lt;SFTP server IP address&gt; all}</b></p> <p>Clears stored SFTP/SSH host key configuration.</p> <ul style="list-style-type: none"><li>o address : Clears a specific SFTP/SSH host key</li><li>o all : Clears all SFTP/SSH host keys</li></ul> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>clear ssh-clientpubkey {all index &lt;1-100&gt; username &lt;user name&gt;}</b></p> <p>Clears stored SSH public key configuration.</p> <ul style="list-style-type: none"><li>o all : Clears all SSH public keys</li><li>o index : Clears a specific SSH public key</li><li>o username : Clears a particular username from all the SSH public keys</li></ul> <p><b>Command mode:</b> All except User EXEC</p>

## RADIUS Server Configuration

The following table displays RADIUS Server configuration commands.

**Table 156.** RADIUS Server Configuration Commands

Command Syntax and Usage
<p><b>[no] radius-server backdoor</b></p> <p>Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is <b>disabled</b>.</p> <p>To obtain the RADIUS backdoor password for your switch, contact your Service and Support line.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] radius-server enable</b></p> <p>Enables or disables the RADIUS server.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[default] radius-server port &lt;UDP port number&gt;</b></p> <p>Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] radius-server primary-host &lt;IP address&gt;</b></p> <p>Sets the primary RADIUS server address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] radius-server secondary-host &lt;IP address&gt;</b></p> <p>Sets the secondary RADIUS server address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>radius-server primary-host &lt;hostname or IP address&gt;</b> <b>[key &lt;1-32 characters&gt;]</b></p> <p>This is the primary shared secret between the switch and the RADIUS server(s). The key option sets the RADIUS server secret key.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no radius-server primary-host [key]</b></p> <p>Removes the primary RADIUS server. The key option removes only the RADIUS server secret key.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>radius-server retransmit &lt;1-3&gt;</b></p> <p>Sets the number of failed authentication requests before switching to a different RADIUS server.</p> <p>The default is 3 requests.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 156.** RADIUS Server Configuration Commands

Command Syntax and Usage
<p><b>radius-server secondary-host</b> &lt;hostname or IP address&gt; <b>[key</b> &lt;1-32 characters&gt;]</p> <p>This is the secondary shared secret between the switch and the RADIUS server(s). The key option sets the RADIUS server secret key.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no radius-server secondary-host [key]</b></p> <p>Removes the secondary RADIUS server. The key option removes only the RADIUS server secret key.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] radius-server secure-backdoor</b></p> <p>Enables or disables the RADIUS backdoor using secure password for Telnet/SSH/HTTP/HTTPS.</p> <p><b>Note:</b> This command does not apply when RADIUS backdoor is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>radius-server timeout</b> &lt;1-10&gt;</p> <p>Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed.</p> <p>The default is 3 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip radius source-interface loopback</b> &lt;1-5&gt;</p> <p>Sets the RADIUS source loopback interface.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show radius-server</b></p> <p>Displays the current RADIUS server parameters.</p> <p><b>Command mode:</b> All</p>

## TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is not an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. Both TACACS and TACACS+ are described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

**Table 157.** TACACS+ Server Configuration Commands

Command Syntax and Usage
<p><b>[no] tacacs-server accounting-enable</b>            Enables or disables TACACS+ accounting.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server attempts &lt;1-10&gt;</b>            Sets the number of failed login attempts before disconnecting the user.            The default is 2 attempts.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server backdoor</b>            Enables or disables the TACACS+ back door for Telnet, SSH/SCP or HTTP/HTTPS.            Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding.            The default setting is <b>disabled</b>.            To obtain the TACACS+ backdoor password for your EN4093R, contact your Service and Support line.  <b>Command mode:</b> Global configuration</p>
<p><b>tacacs-server chpassp &lt;1-32 characters&gt;</b>            Defines the password for the primary TACACS+ server.  <b>Command mode:</b> Global configuration</p>

**Table 157.** TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
<p><b>tacacs-server chpass</b> &lt;1-32 characters&gt;</p> <p>Defines the password for the secondary TACACS+ server.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server command-authorization</b></p> <p>Enables or disables TACACS+ command authorization.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server command-logging</b></p> <p>Enables or disables TACACS+ command logging.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server directed-request</b> <b>[restricted no-truncate]</b></p> <p>Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, username@hostname) during login.</p> <p>This command allows the following options:</p> <ul style="list-style-type: none"><li>o <b>Restricted:</b> Only the username is sent to the specified TACACS+ server.</li><li>o <b>No-truncate:</b> The entire login string is sent to the TACACS+ server.</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server enable</b></p> <p>Enables or disables the TACACS+ server.</p> <p>By default, the server is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server enable-bypass</b></p> <p>Enables or disables the enable-bypass for administrator privilege.</p> <p>By default, enable-bypass is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server encryption-enable</b></p> <p>Enables or disables encryption for TACACS+ traffic packets.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server password-change</b></p> <p>Enables or disables TACACS+ password change.</p> <p>The default value is disabled.</p> <p><b>Command mode:</b> Global configuration</p>



**Table 157.** TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
<p><b>primary-password</b></p> <p>Configures the password for the primary TACACS+ server. The CLI will prompt you for input.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>secondary-password</b></p> <p>Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[default] tacacs-server port</b> &lt;TCP port number&gt;</p> <p>Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server primary-host</b> &lt;IP address&gt;</p> <p>Defines the primary TACACS+ server address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server primary-host</b> &lt;IP address&gt; <b>key</b> &lt;1-32 characters&gt;</p> <p>This is the primary shared secret key between the switch and the TACACS+ server(s).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server privilege-mapping</b></p> <p>Enables or disables TACACS+ privilege-level mapping. The default value is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>tacacs-server retransmit</b> &lt;1-3&gt;</p> <p>Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server secondary-host</b> &lt;IP address&gt;</p> <p>Defines the secondary TACACS+ server address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server secondary-host</b> &lt;IP address&gt; <b>key</b> &lt;1-32 characters&gt;</p> <p>This is the secondary shared secret key between the switch and the TACACS+ server(s).</p> <p><b>Command mode:</b> Global configuration</p>

**Table 157.** TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
<p><b>[no] tacacs-server secure-backdoor</b></p> <p>Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding.</p> <p>This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port.</p> <p>The default is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>tacacs-server timeout</b> &lt;4-15&gt;</p> <p>Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed.</p> <p>The default is 5 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] tacacs-server user-mapping</b> {&lt;0-15&gt; user oper admin}</p> <p>Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip tacacs-server source-interface loopback</b> &lt;1-5&gt;</p> <p>Sets the TACACS+ source loopback interface.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show tacacs-server</b></p> <p>Displays current TACACS+ configuration parameters.</p> <p><b>Command mode:</b> All</p>

## LDAP Server Configuration

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

The following commands will take effect only if the switch is in Legacy Input/Output Module (LIOM) mode.

When the switch is in Secure Input/Output Module (SIOM) mode, these commands are not applicable, as the LDAP configuring is made through CMM (Chassis Management Module) tool.

By default, LDAP is enabled using local LDAP. To login, enter the same credentials (user/password) used to login to CMM tool.

**Table 158.** *LDAP Server Configuration Commands*

Command Syntax and Usage
<p><b>ldap-server attribute username</b> &lt;1-128 characters&gt;</p> <p>Sets a customized LDAP user attribute.</p> <p>The default value is uid.</p> <p><b>Note:</b> The user attribute needs to be set to cn if LDAP server is MS active directory.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ldap-server attribute [username]</b></p> <p>Sets LDAP attributes back to their default values. The username option sets the LDAP user attribute back to its default value of uid.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ldap-server backdoor</b></p> <p>Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS.</p> <p>The default setting is disabled.</p> <p><b>Note:</b> To obtain the LDAP back door password for your EN4093R, contact your Service and Support line.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ldap-server domain</b> [&lt;1-128 characters&gt; none]</p> <p>Sets the domain name for the LDAP server. Enter the full path for your organization. For example:</p> <p>ou=people, dc=mydomain, dc=com</p> <p><b>Command mode:</b> Global configuration</p>

**Table 158.** LDAP Server Configuration Commands (continued)

Command Syntax and Usage
<p><b>[no] ldap-server enable</b> Enables or disables the LDAP server. <b>Command mode:</b> Global configuration</p>
<p><b>[default] ldap-server port</b> &lt;UDP port number&gt; Enter the number of the UDP port to be configured, between 1 - 65000. The default is 389. <b>Command mode:</b> Global configuration</p>
<p><b>[no] ldap-server primary-host</b> &lt;IP address&gt; Sets the primary LDAP server address. <b>Command mode:</b> Global configuration</p>
<p><b>ldap-server retransmit</b> &lt;1-3&gt; Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests. <b>Command mode:</b> Global configuration</p>
<p><b>[no] ldap-server secondary-host</b> &lt;IP address&gt; Sets the secondary LDAP server address. <b>Command mode:</b> Global configuration</p>
<p><b>ldap-server timeout</b> &lt;4-15&gt; Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds. <b>Command mode:</b> Global configuration</p>
<p><b>show ldap-server</b> Displays the current LDAP server parameters configured in LIOM mode. <b>Command mode:</b> All</p>
<p><b>show ldap-server siom-configure</b> Displays the current LDAP server parameters configured in SIOM mode. <b>Command mode:</b> All <b>Note:</b> This command is applicable only when if switch is running in SIOM mode.</p>

## NTP Server Configuration

These commands allow you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

**Table 159.** *NTP Server Configuration Commands*

Command Syntax and Usage
<p><b>[no] ntp authenticate</b></p> <p>Enables or disables NTP authentication. When authentication is enabled, the switch transmits NTP packets with the MAC address appended.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ntp enable</b></p> <p>Enables or disables the NTP synchronization service.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ntp interval</b> &lt;5-44640&gt;</p> <p>Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server.</p> <p>The default value is 1440.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ntp offset</b> &lt;0-86400&gt;</p> <p>Configures the minimum offset in seconds between the switch clock and the NTP server that triggers a system log message.</p> <p>The default value is 300.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ntp offset</b></p> <p>Resets the NTP offset to the default 300 seconds value.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ntp primary-key</b> &lt;1-65534&gt;</p> <p>Adds the NTP primary server key, which specifies which MD5 key is used by the primary server.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ntp secondary-key</b> &lt;1-65534&gt;</p> <p>Adds the NTP secondary server key, which specifies which MD5 key is used by the secondary server.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 159.** NTP Server Configuration Commands

Command Syntax and Usage
<p><b>ntp primary-server</b> &lt;IP address&gt; [<b>data-port</b>   <b>extm-port</b>   <b>mgt-port</b>]</p> <p>Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none"><li>o data port (<b>data</b>)</li><li>o external management port (<b>extm</b>)</li><li>o internal management port (<b>mgt</b>)</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ntp primary-server</b></p> <p>Removes the primary NTP server address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ntp secondary-server</b> &lt;IP address&gt; [<b>data-port</b>   <b>extm-port</b>   <b>mgt-port</b>]</p> <p>Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none"><li>o data port (<b>data</b>)</li><li>o external management port (<b>extm</b>)</li><li>o internal management port (<b>mgt</b>)</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ntp secondary-server</b></p> <p>Removes the secondary NTP server address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ntp ipv6 primary-server</b> &lt;IPv6 address&gt; [<b>data-port</b>   <b>extm-port</b>   <b>mgt-port</b>]</p> <p>Prompts for the IPv6 addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none"><li>o data port (<b>data</b>)</li><li>o external management port (<b>extm</b>)</li><li>o internal management port (<b>mgt</b>)</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ntp ipv6 primary-server</b></p> <p>Removes the IPv6 primary NTP server address.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 159.** NTP Server Configuration Commands

Command Syntax and Usage
<p><b>ntp ipv6 secondary-server</b> &lt;IPv6 address&gt; [<b>data-port</b>   <b>extm-port</b>   <b>mgt-port</b>]</p> <p>Prompts for the IPv6 addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none"><li>o data port (<b>data</b>)</li><li>o external management port (<b>extm</b>)</li><li>o internal management port (<b>mgt</b>)</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ntp ipv6 secondary-server</b></p> <p>Removes the IPv6 secondary NTP server address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ntp sync-logs</b></p> <p>Enables or disables informational logs for NTP synchronization failures. The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ntp source loopback</b> &lt;1-5&gt;</p> <p>Sets the NTP source loopback interface.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ntp trusted-key</b> &lt;1-65534&gt;</p> <p>Adds or removes an MD5 key code to the list of trusted keys. Enter 0 (zero) to remove the selected key code.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ntp</b></p> <p>Displays the current NTP service settings.</p> <p><b>Command mode:</b> All</p>

## NTP MD5 Key Commands

The following table displays NTP MD5 Key configuration commands.

**Table 160.** NTP MD5 Key Configuration Options

Command Syntax and Usage
<p><b>ntp message-digest-key</b> &lt;1-65534&gt; <b>md5-key</b> &lt;1-16 characters&gt;</p> <p>Configures the selected MD5 key code.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ntp message-digest-key</b> &lt;1-65534&gt;</p> <p>Deletes the selected MD5 key code.</p> <p><b>Command mode:</b> Global configuration</p>

## System SNMP Configuration

Enterprise NOS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

**Table 161.** *System SNMP Commands*

Command Syntax and Usage
<p><b>[no] snmp-server authentication-trap</b></p> <p>Enables or disables the use of the system authentication trap facility. The default setting is <code>disabled</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] snmp-server contact</b> &lt;1-64 characters&gt;</p> <p>Configures the name of the system contact. The contact can have a maximum of 64 characters.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server host</b> &lt;trap host IP address&gt; &lt;trap host community string&gt;</p> <p>Adds a trap host server.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no snmp-server host</b> &lt;trap host IP address&gt;</p> <p>Removes the trap host server.</p> <p><b>Command mode:</b> Global configuration</p>



**Table 161.** *System SNMP Commands*

<b>Command Syntax and Usage</b>
<p><b>[no] snmp-server link-trap</b> <i>&lt;port alias or number&gt;</i> <b>enable</b></p> <p>Enables or disables the sending of SNMP link up and link down traps for the specified port.</p> <p>The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] snmp-server location</b> <i>&lt;1-64 characters&gt;</i></p> <p>Configures the name of the system location. The location can have a maximum of 64 characters.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] snmp-server name</b> <i>&lt;1-64 characters&gt;</i></p> <p>Configures the name for the system. The name can have a maximum of 64 characters.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server read-community</b> <i>&lt;1-32 characters&gt;</i></p> <p>Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters.</p> <p>The default read community string is <b>public</b>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] snmp-server read-community-additional</b> <i>&lt;1-32 characters&gt;</i></p> <p>Adds or removes an additional SNMP read community string. Up to 7 additional read community strings are supported.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server timeout</b> <i>&lt;1-30&gt;</i></p> <p>Sets the timeout value for the SNMP state machine, in minutes.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] snmp-server trap-source</b> {<i>&lt;interface number&gt;</i> <b>loopback</b> <i>&lt;1-5&gt;</i>}</p> <p>Configures the source interface for SNMP traps.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server write-community</b> <i>&lt;1-32 characters&gt;</i></p> <p>Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. It can have a maximum of 32 characters.</p> <p>The default write community string is <b>private</b>.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 161.** *System SNMP Commands*

Command Syntax and Usage
<b>[no] snmp-server write-community-additional</b> <1-32 characters> Adds or removes an additional SNMP write community string. Up to 7 additional write community strings are supported. <b>Command mode:</b> Global configuration
<b>show snmp-server</b> Displays the current SNMP configuration. <b>Command mode:</b> All

## SNMPv3 Configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC3411 to RFC3418.

**Table 162.** *SNMPv3 Configuration Commands*

Command Syntax and Usage
<b>snmp-server access</b> <1-32> This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view command options, see <a href="#">page 350</a> . <b>Command mode:</b> Global configuration
<b>snmp-server community</b> <1-16> The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view command options, see <a href="#">page 352</a> . <b>Command mode:</b> Global configuration
<b>snmp-server group</b> <1-17> A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view command options, see <a href="#">page 351</a> . <b>Command mode:</b> Global configuration

**Table 162.** *SNMPv3 Configuration Commands (continued)*

<p><b>snmp-server notify</b> &lt;1-16&gt;</p> <p>A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. To view command options, see <a href="#">page 355</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-address</b> &lt;1-16&gt;</p> <p>This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view command options, see <a href="#">page 353</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-parameters</b> &lt;1-16&gt;</p> <p>This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view command options, see <a href="#">page 354</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server user</b> &lt;1-17&gt;</p> <p>This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. To view command options, see <a href="#">page 348</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server version</b> {v1v2v3 v3only}</p> <p>This command allows you to enable or disable the access to SNMP versions 1, 2 or 3.</p> <p>The default value is v1v2v3.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server view</b> &lt;1-128&gt;</p> <p>This command allows you to create different MIB views. To view command options, see <a href="#">page 349</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show snmp-server v3</b></p> <p>Displays the current SNMPv3 configuration.</p> <p><b>Command mode:</b> All</p>

## User Security Model Configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

**Table 163.** User Security Model Configuration Commands

Command Syntax and Usage
<p><b>snmp-server user</b> &lt;1-17&gt; <b>authentication-protocol</b> {md5 sha none} <b>authentication-password</b> &lt;password value&gt;</p> <p>This command allows you to configure the authentication protocol and password.</p> <p>The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96 for compatibility mode, HMAC-SHA-96 for security strict mode, or none. The default algorithm is none.</p> <p>MD5 authentication protocol is not available in security strict mode if you do not select SNMPv3 account backward compatibility.</p> <p>When you configure an authentication algorithm, you must provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server user</b> &lt;1-17&gt; <b>name</b> &lt;1-32 characters&gt;</p> <p>This command allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server user</b> &lt;1-17&gt; <b>privacy-protocol</b> {aes des none} <b>privacy-password</b> &lt;password value&gt;</p> <p>This command allows you to configure the type of privacy protocol and the privacy password.</p> <p>The privacy protocol protects messages from disclosure. The options are <b>des</b> (CBC-DES Symmetric Encryption Protocol), <b>aes</b> (AES-128 Advanced Encryption Standard Protocol) or <b>none</b>. If you specify <b>des</b> as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). In security strict mode, if you do not select SNMPv3 account backward compatibility, make sure to disable <b>des</b> privacy protocol. If you specify <b>aes</b> as the privacy protocol, make sure that you have selected HMAC-SHA-256 authentication protocol. If you select <b>none</b> as the authentication protocol, you will get an error message.</p> <p>You can create or change the privacy password.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 163.** *User Security Model Configuration Commands*

Command Syntax and Usage
<b>no snmp-server user</b> <1-17> Deletes the USM user entries. <b>Command mode:</b> Global configuration
<b>show snmp-server v3 user</b> <1-17> Displays the USM user entries. <b>Command mode:</b> All

## SNMPv3 View Configuration

Note that the first five default `vacmViewTreeFamily` entries cannot be removed, and their names cannot be changed.

**Table 164.** *SNMPv3 View Configuration Commands*

Command Syntax and Usage
<b>[no] snmp-server view</b> <1-128> <b>mask</b> <1-32 characters> This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. <b>Command mode:</b> Global configuration
<b>snmp-server view</b> <1-128> <b>name</b> <1-32 characters> This command defines the name for a family of view subtrees. <b>Command mode:</b> Global configuration
<b>snmp-server view</b> <1-128> <b>tree</b> <1-64 characters> This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees. <b>Command mode:</b> Global configuration
<b>snmp-server view</b> <1-128> <b>type</b> { <b>included excluded</b> } This command indicates whether the corresponding instances of <code>vacmViewTreeFamilySubtree</code> and <code>vacmViewTreeFamilyMask</code> define a family of view subtrees, which is included in or excluded from the MIB view. <b>Command mode:</b> Global configuration
<b>no snmp-server view</b> <1-128> Deletes the <code>vacmViewTreeFamily</code> group entry. <b>Command mode:</b> Global configuration
<b>show snmp-server v3 view</b> <1-128> Displays the current <code>vacmViewTreeFamily</code> configuration. <b>Command mode:</b> All

## View-based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

**Table 165.** *View-based Access Control Model Commands*

Command Syntax and Usage
<p><b>snmp-server access</b> &lt;1-32&gt; <b>level</b> {noAuthNoPriv authNoPriv authPriv}</p> <p>Defines the minimum level of security required to gain access rights. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server access</b> &lt;1-32&gt; <b>match</b> {exact prefix}</p> <p>If the value is set to <code>exact</code>, then all the rows whose <code>contextName</code> exactly matches the prefix are selected. If the value is set to <code>prefix</code> then the all the rows where the starting octets of the <code>contextName</code> exactly match the prefix are selected.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server access</b> &lt;1-32&gt; <b>name</b> &lt;1-32 characters&gt;</p> <p>Defines the name of the group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server access</b> &lt;1-32&gt; <b>notify-view</b> &lt;1-32 characters&gt;</p> <p>Defines a notify view name that allows you notify access to the MIB view.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server access</b> &lt;1-32&gt; <b>prefix</b> &lt;1-32 characters&gt;</p> <p>Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document. The view-based Access Control Model defines a table that lists the locally available contexts by <code>contextName</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server access</b> &lt;1-32&gt; <b>read-view</b> &lt;1-32 characters&gt;</p> <p>Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 165.** *View-based Access Control Model Commands (continued)*

Command Syntax and Usage
<b>snmp-server access &lt;1-32&gt; security {usm snmpv1 snmpv2}</b> Allows you to select the security model to be used. <b>Command mode:</b> Global configuration
<b>snmp-server access &lt;1-32&gt; write-view &lt;1-32 characters&gt;</b> Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. <b>Command mode:</b> Global configuration
<b>no snmp-server access &lt;1-32&gt;</b> Deletes the View-based Access Control entry. <b>Command mode:</b> Global configuration
<b>show snmp-server v3 access &lt;1-32&gt;</b> Displays the View-based Access Control configuration. <b>Command mode:</b> All

## SNMPv3 Group Configuration

The following table displays SNMPv3 Group configuration commands.

**Table 166.** *SNMPv3 Group Configuration Commands*

Command Syntax and Usage
<b>snmp-server group &lt;1-17&gt; group-name &lt;1-32 characters&gt;</b> The name for the access group as defined in the following command: snmp-server access <1-32> name <1-32 characters> on <a href="#">page 348</a> . <b>Command mode:</b> Global configuration
<b>snmp-server group &lt;1-17&gt; security {usm snmpv1 snmpv2}</b> Defines the security model. <b>Command mode:</b> Global configuration
<b>snmp-server group &lt;1-17&gt; user-name &lt;1-32 characters&gt;</b> Sets the user name as defined in the following command on <a href="#">page 348</a> : snmp-server user <1-17> name <1-32 characters> <b>Command mode:</b> Global configuration
<b>no snmp-server group &lt;1-17&gt;</b> Deletes the vacmSecurityToGroup entry. <b>Command mode:</b> Global configuration
<b>show snmp-server v3 group &lt;1-17&gt;</b> Displays the current vacmSecurityToGroup configuration. <b>Command mode:</b> All

## SNMPv3 Community Table Configuration

These commands are used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

**Table 167.** *SNMPv3 Community Table Configuration Commands*

Command Syntax and Usage
<b>snmp-server community</b> <1-16> <b>index</b> <1-32 characters> Allows you to configure the unique index value of a row in this table. <b>Command string:</b> Global configuration
<b>snmp-server community</b> <1-16> <b>name</b> <1-32 characters> Defines the user name as defined in the following command on <a href="#">page 348</a> : <code>snmp-server user &lt;1-17&gt; name &lt;1-32 characters&gt;</code> <b>Command string:</b> Global configuration
<b>snmp-server community</b> <1-16> <b>tag</b> <1-255 characters> Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. <b>Command mode:</b> Global configuration
<b>snmp-server community</b> <1-16> <b>user-name</b> <1-32 characters> Defines a readable string that represents the corresponding value of an SNMP community name in a security model. <b>Command mode:</b> Global configuration
<b>no snmp-server community</b> <1-16> Deletes the community table entry. <b>Command mode:</b> Global configuration
<b>show snmp-server v3 community</b> <1-16> Displays the community table configuration. <b>Command mode:</b> All



## SNMPv3 Target Address Table Configuration

These commands are used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

**Table 168.** Target Address Table Configuration Commands

Command Syntax and Usage
<p><b>snmp-server target-address</b> &lt;1-16&gt; {<b>address address6</b>} &lt;IP address&gt; <b>name</b> &lt;1-32 characters&gt;</p> <p>Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-address</b> &lt;1-16&gt; <b>name</b> &lt;1-32 characters&gt; {<b>address address6</b>} &lt;transport IP address&gt;</p> <p>Configures a transport IPv4/IPv6 address that can be used in the generation of SNMP traps.</p> <p><b>Note:</b> IPv6 addresses are not displayed in the configuration, but they do receive traps.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-address</b> &lt;1-16&gt; <b>parameters-name</b> &lt;1-32 characters&gt;</p> <p>Defines the name as defined in the following command on <a href="#">page 354</a>:  <b>snmp-server target-parameters</b> &lt;1-16&gt; <b>name</b> &lt;1-32 characters&gt;</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-address</b> &lt;1-16&gt; <b>port</b> &lt;port number&gt;</p> <p>Allows you to configure a transport address port that can be used in the generation of SNMP traps.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-address</b> &lt;1-16&gt; <b>taglist</b> &lt;1-255 characters&gt;</p> <p>Allows you to configure a list of tags that are used to select target addresses for a particular operation.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no snmp-server target-address</b> &lt;1-16&gt;</p> <p>Deletes the Target Address Table entry.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show snmp-server v3 target-address</b> &lt;1-16&gt;</p> <p>Displays the current Target Address Table configuration.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 Target Parameters Table Configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthNoPriv`, `authNoPriv`, or `authPriv`).

**Table 169.** Target Parameters Table Configuration Commands

Command Syntax and Usage
<p><b>snmp-server target-parameters &lt;1-16&gt; level {noAuthNoPriv authNoPriv authPriv}</b></p> <p>Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-parameters &lt;1-16&gt; message {snmpv1 snmpv2c snmpv3}</b></p> <p>Allows you to configure the message processing model that is used to generate SNMP messages.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-parameters &lt;1-16&gt; name &lt;1-32 characters&gt;</b></p> <p>Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-parameters &lt;1-16&gt; security {usm snmpv1 snmpv2}</b></p> <p>Allows you to select the security model to be used when generating the SNMP messages.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>snmp-server target-parameters &lt;1-16&gt; user-name &lt;1-32 characters&gt;</b></p> <p>Defines the name that identifies the user in the USM table (<a href="#">page 348</a>) on whose behalf the SNMP messages are generated using this entry.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 169.** *Target Parameters Table Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<b>no snmp-server target-parameters</b> <1-16> Deletes the targetParamsTable entry. <b>Command mode:</b> Global configuration
<b>show snmp-server v3 target-parameters</b> <1-16> Displays the current targetParamsTable configuration. <b>Command mode:</b> All

## SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

**Table 170.** *Notify Table Commands*

<b>Command Syntax and Usage</b>
<b>snmp-server notify</b> <1-16> <b>name</b> <1-32 characters> Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry. <b>Command mode:</b> Global configuration
<b>snmp-server notify</b> <1-16> <b>tag</b> <1-255 characters> Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the snmpTargetAddrTable that matches the value of this tag is selected. <b>Command mode:</b> Global configuration
<b>no snmp-server notify</b> <1-16> Deletes the notify table entry. <b>Command mode:</b> Global configuration
<b>show snmp-server v3 notify</b> <1-16> Displays the current notify table configuration. <b>Command mode:</b> All

## System Access Configuration

The following table describes system access configuration commands.

**Table 171.** *System Access Configuration Commands*

Command Syntax and Usage
<p><b>[no] access http enable</b>            Enables or disables HTTP (Web) access to the Browser-Based Interface.            The default settings is disabled.  <b>Command mode:</b> Global configuration</p>
<p><b>[default] access http port [&lt;port number&gt;]</b>            Sets the switch port used for serving switch Web content.            The default setting is HTTP port 80.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access snmp {read-only read-write}</b>            Enables or disables read-only/write-read SNMP access.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access telnet enable</b>            Enables or disables Telnet access.            The default settings is disabled.  <b>Command mode:</b> Global configuration</p>
<p><b>[default] access telnet port [&lt;1-65535&gt;]</b>            Sets an optional Telnet server port number for cases where the server listens for Telnet sessions on a non-standard port.  <b>Command mode:</b> Global configuration</p>
<p><b>[default] access tftp-port [&lt;1-65535&gt;]</b>            Sets the TFTP port for the switch.            The default is port 69.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access tsbbi enable</b>            Enables or disables Telnet/SSH configuration through the Browser-Based Interface (BBI).  <b>Command mode:</b> Global configuration</p>

**Table 171.** *System Access Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>access user administrator-password</b></p> <p>Sets the administrator (<code>admin</code>) password. The administrator has complete access to all menus, information, and configuration commands on the EN4093R, including the ability to change both the user and administrator passwords.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Access includes “oper” functions.</p> <p><b>Note:</b> You cannot disable the administrator password.</p> <p><b>Command Mode:</b> Global configuration</p>
<p><b>access user operator-password</b></p> <p>Sets the operator (<code>oper</code>) password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p><b>Note:</b> To disable the operator account, set the password to null (no password). The default setting is <code>disabled</code> (no password).</p> <p><b>Command Mode:</b> Global configuration</p>
<p><b>access user user-password</b></p> <p>Sets the user (<code>user</code>) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p><b>Note:</b> To disable the user account, set the password to null (no password).</p> <p><b>Command Mode:</b> Global configuration</p>
<p><b>[no] access userbbi enable</b></p> <p>Enables or disables user configuration access through the Browser-Based Interface (BBI).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show access</b></p> <p>Displays the current system access parameters.</p> <p><b>Command mode:</b> All</p>

## Management Network Configuration

These commands are used to define IP address ranges which are allowed to access the switch for management purposes.

**Table 172.** Management Network Configuration Commands

Command Syntax and Usage
<p><b>[no] access management-network</b> &lt;mgmt network IPv4 or IPv6 address&gt; &lt;mgmt network mask or prefix length&gt;</p> <p>Adds or removes a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the Enterprise NOS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.</p> <p><b>Note:</b> If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a “Network Down” state on the network.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access management-network</b> &lt;mgmt network IPv4 address&gt; &lt;mgmt network mask&gt; {snmp-ro snmp-rw}</p> <p>Adds a defined IPv4 network through which SNMP read-only or SNMP read/write switch access is allowed. Specify an IP address and mask address in dotted-decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no access management-network</b> {snmp-ro snmp-rw}</p> <p>Clears the IPv4 SNMP read-only or SNMP read/write access control list for management purposes.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access management-network6</b> &lt;mgmt network IPv6 address&gt; &lt;IPv6 prefix length&gt; {snmp-ro snmp-rw}</p> <p>Adds a defined IPv6 network through which SNMP read-only or SNMP read/write switch access is allowed.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no access management-network6</b> {snmp-ro snmp-rw}</p> <p>Clears the IPv6 SNMP read-only or SNMP read/write access control list for management purposes.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show access management-network</b></p> <p>Displays the current management network configuration and SNMP access management IP list.</p> <p><b>Command mode:</b> All</p>
<p><b>clear access management-network</b></p> <p>Removes all defined management networks.</p> <p><b>Command mode:</b> All except User EXEC</p>

## NETCONF Configuration

This menu allows you to configure support for Network Configuration Protocol (NETCONF), which provides mechanisms to install, manipulate, and delete the configuration of network devices. NETCONF is described in RFC 4741.

**Table 173.** *NETCONF Configuration Options*

<b>Command Syntax and Usage</b>
<b>[no] access netconf enable</b> Enables or disables NETCONF access to the switch. <b>Command mode:</b> Global configuration
<b>access netconf timeout &lt;30-3600&gt;</b> Configures the timeout value for NETCONF sessions, in seconds. The default value is 300 seconds. <b>Command mode:</b> Global configuration
<b>default access netconf timeout</b> Configures the timeout value for NETCONF sessions to the default value of 300 seconds. <b>Commands mode:</b> Global configuration
<b>show access</b> Displays the current configuration. <b>Command mode:</b> All

## NETCONF over SSH Configuration

This menu allows you to enable NETCONF access over Secure Shell (SSH). NETCONF over SSH is described in RFC 4742.

**Table 174.** *NETCONF over SSH Configuration Options*

<b>Command Syntax and Usage</b>
<b>[no] access netconf ssh enable</b> Enables or disables NETCONF access over SSH. <b>Command mode:</b> Global configuration
<b>access netconf ssh port &lt;TCP port number&gt;</b> Configures the TCP port used for NETCONF. The default port number is 830. <b>Command mode:</b> Global configuration
<b>default access netconf ssh port</b> Configures the TCP port used for NETCONF to the default port number of 830. <b>Command mode:</b> Global configuration

## User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

**Table 175.** *User Access Control Configuration Commands*

Command Syntax and Usage
<p><b>access user</b> &lt;1-20&gt;</p> <p>Configures the User ID.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access user administrator-enable</b></p> <p>Enables or disables the default administrator account.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access user administrator-password</b> &lt;1-128 characters&gt;</p> <p>Sets the administrator (admin) password. The super user administrator has complete access to all information and configuration commands on the EN4093R, including the ability to change both the user and administrator passwords.</p> <p><b>Note:</b> Access includes “oper” functions.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access user operator-password</b> &lt;1-128 characters&gt;</p> <p>Sets the operator (oper) password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access user user-password</b> &lt;1-128 characters&gt;</p> <p>Sets the user (user) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access user eject</b> {&lt;user name&gt; &lt;session ID&gt;}</p> <p>Ejects the specified user from the EN4093R.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>clear line</b> &lt;1-12&gt;</p> <p>Ejects the user with the corresponding session ID from the EN4093R.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>show access user</b></p> <p>Displays the current user status.</p> <p><b>Command mode:</b> All</p>



## System User ID Configuration

The following table describes user ID configuration commands.

**Table 176.** *User ID Configuration Commands*

<b>Command Syntax and Usage</b>
<p><b>[no] access user &lt;1-20&gt; enable</b>            Enables or disables the user ID.  <b>Command mode:</b> Global configuration</p>
<p><b>access user &lt;1-20&gt; level {user operator administrator}</b>            Sets the Class-of-Service to define the user's authority level. Enterprise NOS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.  <b>Command mode:</b> Global configuration</p>
<p><b>access user &lt;1-20&gt; name &lt;1-8 characters&gt;</b>            Defines the user name of maximum eight characters.  <b>Command mode:</b> Global configuration</p>
<p><b>access user &lt;1-20&gt; password</b>            Sets the user (user) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.  <b>Command mode:</b> Global configuration</p>
<p><b>no access user &lt;1-20&gt;</b>            Deletes the user ID.  <b>Command mode:</b> Global configuration</p>
<p><b>show access user</b>            Displays the current user ID configuration.  <b>Command mode:</b> All</p>

## Strong Password Configuration

The following table describes strong password configuration commands.

**Table 177.** *Strong Password Configuration Commands*

<b>Command Syntax and Usage</b>
<p><b>[no] access user strong-password enable</b> Enables or disables Strong Password requirement. <b>Command mode:</b> Global configuration</p>
<p><b>access user strong-password clear local user {lockout fail-attempts} {&lt;username&gt; all}</b> Enables locked out accounts or resets failed login counters for all users or for a specific user. <b>Command mode:</b> Global configuration</p>
<p><b>access user strong-password expiry &lt;1-365&gt;</b> Configures the number of days allowed before the password must be changed. The default value is 60. <b>Command mode:</b> Global configuration</p>
<p><b>access user strong-password faillock &lt;1-10&gt;</b> Configures the number of failed login attempts that trigger the account lockout. The default value is 6. <b>Command mode:</b> Global configuration</p>
<p><b>access user strong-password faillog &lt;1-255&gt;</b> Configures the number of failed login attempts allowed before a security notification is logged. The default value is 3. <b>Command mode:</b> Global configuration</p>
<p><b>[no] access user strong-password lockout</b> Enables or disables account lockout after a specified number of failed login attempts. The default setting is disabled. <b>Command mode:</b> Global configuration</p>

**Table 177.** *Strong Password Configuration Commands*

Command Syntax and Usage
<b>access user strong-password warning</b> <1-365> Configures the number of days before password expiration, that a warning is issued to users. The default value is 15. <b>Command mode:</b> Global configuration
<b>show access user strong-password</b> Displays the current Strong Password configuration. <b>Command mode:</b> All

## HTTPS Access Configuration

The following table describes HTTPS access configuration commands.

**Table 178.** *HTTPS Access Configuration Commands*

Command Syntax and Usage
<b>[no] access https enable</b> Enables or disables BBI access (Web access) using HTTPS. The default setting is enabled. <b>Command mode:</b> Global configuration
<b>access https generate-certificate</b> Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: <ul style="list-style-type: none"><li>o Country Name (2 letter code): CA</li><li>o State or Province Name (full name): Ontario</li><li>o Locality Name (for example, city): Ottawa</li><li>o Organization Name (for example, company): Lenovo</li><li>o Organizational Unit Name (for example, section): Operations</li><li>o Common Name (for example, user's name): Mr Smith</li><li>o Email (for example, email address): info@lenovo.com</li></ul> You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent. <b>Command mode:</b> Global configuration

**Table 178.** *HTTPS Access Configuration Commands*

<b>Command Syntax and Usage</b>
<p><b>access https generate-csr</b></p> <p>Allows you to generate a CSR (Certificate Signing Request) to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:</p> <ul style="list-style-type: none"><li>o Country Name (2 letter code): CA</li><li>o State or Province Name (full name): Ontario</li><li>o Locality Name (for example, city): Ottawa</li><li>o Organization Name (for example, company): Lenovo</li><li>o Organizational Unit Name (for example, section): Operations</li><li>o Common Name (for example, user's name): Mr Smith</li><li>o Email (for example, email address): info@lenovo.com</li></ul> <p>Unlike the <b>generate-certificate</b> command, this command will generate a certificate request that needs to be signed by a certificate authority (CA) recognized by both parties.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[default] access https port [<i>&lt;TCP port number&gt;</i>]</b></p> <p>Defines the HTTPS Web server port number.</p> <p>The default port is 443.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access https save-certificate</b></p> <p>Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>copy cert-request {tftp ftp sftp} address <i>&lt;hostname or server IP address&gt;</i> filename <i>&lt;server-filename&gt;</i></b> <b>[data-port  mgt-port  extm-port]</b></p> <p>Enables you to export a CSR to an external server using TFTP/SFTP/FTP.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show https host-csr pem-format</b></p> <p>Displays the generated CSR in PEM format.</p> <p><b>Command mode:</b> Privileged EXEC</p>

**Table 178.** *HTTPS Access Configuration Commands*

<b>Command Syntax and Usage</b>
<b>show https host-csr txt-format</b> Displays the generated CSR in TXT format. <b>Command mode:</b> Privileged EXEC
<b>show access</b> Displays the current SSL Web Access configuration. <b>Command mode:</b> All

## Custom Daylight Saving Time Configuration

Use these commands to configure custom Daylight Saving Time. The DST is defined by two rules, the start rule and end rule. The rules specify the dates when the DST starts and finishes. These dates are represented as specific calendar dates or as relative offsets in a month (for example, 'the second Sunday of September').

Relative offset example:

2070901 = Second Sunday of September, at 1:00 a.m.

Calendar date example:

0070901 = September 7, at 1:00 a.m.

**Table 179.** *Custom DST Configuration Commands*

Command Syntax and Usage
<p><b>[no] system custom-dst enable</b></p> <p>Enables or disables the Custom Daylight Saving Time settings.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>system custom-dst start-rule</b> &lt;WDDMMhh&gt;</p> <p>Configures the start date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date)</p> <p>D = day of the week (01-07, where 01 is Monday)</p> <p>MM = month (1-12)</p> <p>hh = hour (0-23)</p> <p><b>Note:</b> Week 5 is always considered to be the last week of the month.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>system custom-dst end-rule</b> &lt;WDDMMhh&gt;</p> <p>Configures the end date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date)</p> <p>D = day of the week (01-07, where 01 is Monday)</p> <p>MM = month (1-12)</p> <p>hh = hour (0-23)</p> <p><b>Note:</b> Week 5 is always considered to be the last week of the month.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show custom-dst</b></p> <p>Displays the current Custom DST configuration.</p> <p><b>Command mode:</b> All</p>

---

## sFlow Configuration

Enterprise NOS supports sFlow version 5. sFlow is a sampling method used for monitoring high speed switched networks. Use these commands to configure the sFlow agent on the switch.

**Table 180.** *sFlow Configuration Commands*

Command Syntax and Usage
<b>[no] sflow enable</b> Enables or disables the sFlow agent. <b>Command mode:</b> Global configuration
<b>sflow port</b> <1-65535> Configures the UDP port for the sFlow server. The default value is 6343. <b>Command mode:</b> Global configuration
<b>sflow server</b> <IP address> Defines the sFlow server address. <b>Command mode:</b> Global configuration
<b>show sflow</b> Displays sFlow configuration parameters. <b>Command mode:</b> All

## sFlow Port Configuration

Use the following commands to configure the sFlow port on the switch.

**Table 181.** *sFlow Port Configuration Commands*

Command Syntax and Usage
<b>[no] sflow polling</b> <5-60> Configures the sFlow polling interval, in seconds. The default setting is disabled. <b>Command mode:</b> Interface port
<b>[no] sflow sampling</b> <256-65536> Configures the sFlow sampling rate, in packets per sample. The default setting is disabled. <b>Command mode:</b> Interface port

---

## Port Configuration

Use the Port Configuration commands to configure settings for switch ports (INTx) and (EXTx). If you are configuring management ports (MGT1), see [“Management Port Configuration” on page 380](#).

**Table 182.** *Port Configuration Commands*

<b>Command Syntax and Usage</b>
<b>interface port</b> <port alias or number> Enter Interface port mode. <b>Command mode:</b> Global configuration
<b>[no] bpdu-guard</b> Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled. <b>Command mode:</b> Interface port
<b>description</b> <1-64 characters> Sets a description for the port. The assigned port name appears next to the port description on some information and statistics screens. The default is set to the port number. <b>Command mode:</b> Interface port
<b>dot1p</b> <0-7> Configures the port's 802.1p priority level. <b>Command mode:</b> Interface port
<b>[no] dscp-marking</b> Enables or disables DSCP re-marking on a port. <b>Command mode:</b> Interface port
<b>[no] flood-blocking</b> Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port. <b>Command mode:</b> Interface port
<b>ip dhcp snooping limit rate</b> <1-2048> Configures the maximum number of DHCP packets allowed per second. <b>Command mode:</b> Interface port
<b>no ip dhcp snooping limit rate</b> Unlimits the maximum number of DHCP packets allowed per second. <b>Command mode:</b> Interface port



**Table 182.** *Port Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>[no] ip dhcp snooping trust</b>          Configures this port as a trusted port for DHCP packets from the server.  <b>Command mode:</b> Interface port</p>
<p><b>[no] learning</b>          Enables or disables FDB learning on the port.  <b>Command mode:</b> Interface port</p>
<p><b>port-channel min-links &lt;1-32&gt;</b>          Set the minimum number of links for the LACP LAG to which this port belongs. If the specified minimum number of ports are not available, the LAG is placed in the down state.  <b>Command mode:</b> Interface port</p>
<p><b>[no] reflective-relay force</b>          Enables or disables constraint to always keep reflective relay active.          The default setting is disabled.  <b>Command mode:</b> Interface port</p>
<p><b>[no] rmon</b>          Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.  <b>Command mode:</b> Interface port</p>
<p><b>shutdown</b>          Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to <a href="#">“Temporarily Disabling a Port” on page 374.</a>)  <b>Command mode:</b> Interface port</p>
<p><b>no shutdown</b>          Enables the port.  <b>Command mode:</b> Interface port</p>
<p><b>[no] storm-control broadcast level rate &lt;0-2097151&gt;</b>          Limits the number of broadcast packets per second to the specified value. If disabled, the port forwards all broadcast packets.  <b>Command mode:</b> Interface port</p>
<p><b>[no] storm-control multicast level rate &lt;0-2097151&gt;</b>          Limits the number of multicast packets per second to the specified value. If disabled, the port forwards all multicast packets.  <b>Command mode:</b> Interface port</p>

**Table 182.** Port Configuration Commands (continued)

<p><b>Command Syntax and Usage</b></p>
<p><b>[no] storm-control unicast level rate</b> &lt;0-2097151&gt;</p> <p>Limits the number of unknown unicast packets per second to the specified value. If disabled, the port forwards all unknown unicast packets.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>switchport mode {access trunk private-vlan}</b></p> <p>Configures the port's trunking mode:</p> <ul style="list-style-type: none"> <li>o access allows association to a single VLAN</li> <li>o trunk automatically adds the port to all created VLANs. To configure a specific allowed VLAN range for the port use the command: switchport trunk allowed vlan</li> <li>o private-vlan allows association to a private VLAN</li> </ul> <p>The default mode is access.</p> <p><b>Note:</b> When switching from access to trunk mode, the port inherits the access VLAN as the trunk Native-VLAN.</p> <p><b>Note:</b> When switching from trunk to access mode, the port inherits the trunk Native-VLAN as the access VLAN.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>switchport trunk allowed vlan</b> &lt;VLAN ID range&gt;</p> <p>Configures the allowed VLANs in trunk mode for the current port or portchannel. If the allowed range does not have any existing VLANs, the lowest-numbered VLAN is created and becomes the Native-VLAN. If the allowed range contains an existing VLAN(s), but the Native-VLAN is not in the allowed range, the Native-VLAN is changed to the lowest-numbered existing VLAN. If a new VLAN is created and it is part of the allowed VLAN range, the port will also be added to that VLAN.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>switchport trunk allowed vlan {add remove}</b> &lt;VLAN ID range&gt;</p> <p>Updates the associated VLANs in trunk mode.</p> <ul style="list-style-type: none"> <li>o add enables the VLAN range in addition to the current configuration. If any VLAN in the range does not exist, it will not be created and enabled automatically.</li> <li>o remove eliminates the VLAN range from the current configuration.</li> </ul> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>switchport trunk allowed vlan {all none}</b></p> <p>Updates the associated VLANs in trunk mode.</p> <ul style="list-style-type: none"> <li>o all associates the port to all existing regular VLANs and to any other VLAN that gets created afterwards.</li> <li>o none removes the port from all currently associated VLANs and assigns the port to the default Native-VLAN (VLAN 1 for data ports).</li> </ul> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

**Table 182.** Port Configuration Commands (continued)

<p><b>Command Syntax and Usage</b></p>
<p><b>no switchport trunk allowed vlan</b></p> <p>Assigns the port to all available data VLANs.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>switchport trunk native vlan</b> &lt;1-4094&gt;</p> <p>Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. If the VLAN does not exist, it will be created and enabled automatically.</p> <p>Default value is 1 for data ports and 4095 for the management port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>switchport access vlan</b> &lt;1-4094&gt;</p> <p>Configures the associated VLAN used in access mode. If the VLAN does not exist, it will be created and enabled automatically.</p> <p>Default value is 1 for data ports and 4095 for the management port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>no switchport access vlan</b></p> <p>Resets the access VLAN to its default value.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] switchport private-vlan mapping</b> &lt;primary VLAN&gt;</p> <p>Enables or disables a private VLAN promiscuous port to/from a primary VLAN.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] switchport private-vlan host-association</b> &lt;primary VLAN&gt; &lt;secondary VLAN&gt;</p> <p>Adds or removes a private VLAN host port to/from a secondary VLAN.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] tagpvid-ingress</b></p> <p>Enables or disables tagging the ingress frames with the port's VLAN ID. When enabled, the PVID tag is inserted into untagged and 802.1Q single-tagged ingress frames as outer VLAN ID.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] tagskip-egress</b></p> <p>Enables or disables egress VLAN tag enforcement to be skipped.</p> <p><b>Note:</b> STP must be globally disabled on the switch and all VLANs must be assigned to the default STG.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

**Table 182.** Port Configuration Commands (continued)

<b>Command Syntax and Usage</b>
<b>[no] tagskip-ingress</b> Enables or disables ingress VLAN tag enforcement to be skipped. <b>Command mode:</b> Interface port/Interface portchannel
<b>unicast-bandwidth &lt;10-100&gt;</b> Configures the allocated bandwidth percentage for unicast traffic on the port. The remaining bandwidth is automatically allocated to multicast traffic. The default value is 50. <b>Command mode:</b> Interface port
<b>unicast-bandwidth global &lt;10-100&gt;</b> Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic. The default value is 50. <b>Note:</b> This applies to all ports. <b>Command mode:</b> Interface port
<b>[no] vlan dot1q tag native</b> Enables or disables VLAN tag persistence. When disabled, the VLAN tag is removed at egress from packets whose VLAN tag matches the port PVID/Native-vlan. The default setting is disabled. <b>Note:</b> In global configuration mode, this is an operational command used to set the VLAN tag persistence on all ports currently tagged at the moment of execution. VLAN tag persistence will not be set automatically for ports tagged afterward. Also, as an operational command, it will not be dumped into the configuration file. <b>Command mode:</b> Global configuration/Interface port/Interface portchannel
<b>show interface port &lt;port alias or number&gt;</b> Displays current port parameters. <b>Command mode:</b> All

## Port Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

**Table 183.** *Port Error Disable Commands*

Command Syntax and Usage
<p><b>[no] errdisable link-flap enable</b></p> <p>Enables or disables Link Flap Dampening on the port. For more information, see <a href="#">“Link Flap Dampening Configuration” on page 327</a>.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>[no] errdisable recovery</b></p> <p>Enables or disables automatic error-recovery for the port.</p> <p>The default setting is enabled.</p> <p><b>Note:</b> Error-recovery must be <b>enabled</b> globally before port-level commands become active.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port &lt;port alias or number&gt; errdisable</b></p> <p>Displays current port Error Disable parameters.</p> <p><b>Command mode:</b> All</p>

## Port Link Configuration

Use these commands to set flow control for the port link.

**Table 184.** *Port Link Configuration Commands*

<b>Command Syntax and Usage</b>
<b>[no] auto</b> Enables or disables auto-negotiation on the port. <b>Command mode:</b> Interface port
<b>duplex {full half auto}</b> Sets the operating mode. The choices include: <ul style="list-style-type: none"><li>– Auto negotiation (default)</li><li>– Half-duplex</li><li>– Full-duplex</li></ul> <b>Command mode:</b> Interface port
<b>flowcontrol {receive send} {on off}</b> Enables or disables flow control receive or transmit. <b>Note:</b> For external ports (EXTx) the default setting is <code>no flow control</code> , and for internal ports (INTx) the default setting is both receive and transmit. <b>Command mode:</b> Interface port
<b>speed {1000 10000 auto}</b> Sets the link speed. Some options are not valid on all ports. The choices include: <ul style="list-style-type: none"><li>– 1000 Mbps</li><li>– 10000 Mbps</li><li>– any (auto negotiate port speed)</li></ul> <b>Command mode:</b> Interface port
<b>show interface port</b> <port alias or number> Displays current port parameters. <b>Command mode:</b> All

## Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
EN 4093# interface port <port alias or number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the EN4093R 10Gb Ethernet Scalable Switch is reset. See the [“Operations Commands” on page 609](#) for other operations-level commands.

## Unidirectional Link Detection Configuration

UDLD commands are described in the following table.

**Table 185.** *Port UDLD Configuration Commands*

Command Syntax and Usage
<p><b>[no] udld</b></p> <p>Enables or disables UDLD on the port.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>[no] udld aggressive</b></p> <p>Configures the UDLD mode for the selected port, as follows:</p> <ul style="list-style-type: none"><li>o <b>Normal:</b> Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the "no" form to select normal operation.</li><li>o <b>Aggressive:</b> In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds.</li></ul> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port &lt;port number&gt; udld</b></p> <p>Displays current port UDLD parameters.</p> <p><b>Command mode:</b> All</p>

## Port OAM Configuration

Operation, Administration, and Maintenance (OAM) protocol allows the switch to detect faults on the physical port links. OAM is described in the IEEE 802.3ah standard. OAM Discovery commands are described in the following table.

**Table 186.** *Port OAM Configuration Commands*

Command Syntax and Usage
<p><b>oam [passive]</b></p> <p>Configures the OAM discovery mode, as follows:</p> <ul style="list-style-type: none"><li>o <b>Passive:</b> This port allows its peer link to initiate OAM discovery.</li></ul> <p>If OAM determines that the port is in an anomalous condition, the port is disabled.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>no oam [passive]</b></p> <p>Disables OAM discovery on the port.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port &lt;port number&gt; oam</b></p> <p>Displays current port OAM parameters.</p> <p><b>Command mode:</b> All</p>



## Port ACL Configuration

The following table describes port ACL configuration commands.

**Table 187.** *Port ACL/QoS Configuration Commands*

Command Syntax and Usage
<p><b>[no] access-control group</b> &lt;1-640&gt; Adds or removes the specified ACL group. You can add multiple ACL groups to a port. <b>Command mode:</b> Interface port</p>
<p><b>[no] access-control list</b> &lt;1-640&gt; Adds or removes the specified ACL. You can add multiple ACLs to a port. <b>Command mode:</b> Interface port</p>
<p><b>[no] access-control list6</b> &lt;1-128&gt; Adds or removes the specified IPv6 ACL. You can add multiple ACLs to a port. <b>Command mode:</b> Interface port</p>
<p><b>show interface port</b> &lt;port alias or number&gt; <b>access-control</b> Displays current ACL QoS parameters. <b>Command mode:</b> All</p>

## Port WRED Configuration

These commands allow you to configure Weighted Random Early Detection (WRED) parameters for a selected port. For global WRED configuration, see [“Weighted Random Early Detection Configuration” on page 388](#).

**Table 188.** *Port WRED Options*

Command Syntax and Usage
<p><b>[no] random-detect ecn enable</b></p> <p>Enables or disables Explicit Congestion Notification (ECN). When ECN is enabled, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions.</p> <p><b>Note:</b> ECN functions only on TCP traffic.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>[no] random-detect enable</b></p> <p>Enables or disables Random Detection and avoidance.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>random-detect</b></p> <p>Displays current Random Detection and avoidance parameters.</p> <p><b>Command mode:</b> All</p>

## Port WRED Transmit Queue Configuration

Use this menu to define WRED thresholds for the port's transmit queues. Set each threshold between 1% and 100%. When the average queue size grows beyond the minimum threshold, packets begin to be dropped. When the average queue size reaches the maximum threshold, all packets are dropped. The probability of packet-drop between the thresholds is defined by the drop rate.

**Table 189.** Port WRED Transmit Queue Options

Command Syntax and Usage
<p><b>[no] random-detect transmit-queue &lt;0-7&gt; enable</b> Sets the WRED transmit queue configuration to on or off. <b>Command mode:</b> Interface port</p>
<p><b>[no] random-detect transmit-queue &lt;0-7&gt; tcp &lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt;</b> Configures the WRED thresholds for TCP traffic. <b>Note:</b> Use the no form to clear the WRED threshold value. <b>Command mode:</b> Interface port</p>
<p><b>[no] random-detect transmit-queue &lt;0-7&gt; non-tcp &lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt;</b> Configures the WRED thresholds for non-TCP traffic. <b>Note:</b> Use the no form to clear the WRED threshold value. <b>Command mode:</b> Interface port</p>

## Management Port Configuration

You can use these commands to set port parameters for management ports (MGT1 and EXTM). Use these commands to set port parameters for the port link. For MGT1, only LLDP settings are configurable.

**Table 190.** *Management Port Configuration Commands*

Command Syntax and Usage
<p><b>[no] auto</b></p> <p>Enables or disables auto-negotiation on the port.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>duplex {full half auto}</b></p> <p>Sets the operating mode. The choices include:</p> <ul style="list-style-type: none"> <li>– Full-duplex</li> <li>– Half-duplex</li> <li>– Auto — for auto negotiation (default)</li> </ul> <p><b>Command mode:</b> Interface port</p>
<p><b>flowcontrol {receive send} {on off}</b></p> <p>Activates or deactivates one type of flow control. The choices include:</p> <ul style="list-style-type: none"> <li>– Receive flow control</li> <li>– Transmit flow control</li> </ul> <p><b>Command mode:</b> Interface port</p>
<p><b>shutdown</b></p> <p>Disables the port.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>no shutdown</b></p> <p>Enables the port.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>speed {10 100 1000 auto}</b></p> <p>Sets the link speed. The choices include:</p> <ul style="list-style-type: none"> <li>– 10 Mbps</li> <li>– 100 Mbps</li> <li>– 1000 Mbps</li> <li>– Auto — for auto negotiation</li> </ul> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port</b> &lt;port alias or number&gt;</p> <p>Displays current port parameters.</p> <p><b>Command mode:</b> All</p>

---

## Stacking Configuration

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. The Stacking Configuration menu is used to configure a stack, and to define the Backup switch.

The Stacking Configuration menu is available only after Stacking is enabled and the switch is reset. For more information, see [“Stacking Boot Options” on page 624](#).

**Table 191.** *Stacking Commands*

Command Syntax and Usage
<b>connect</b> <attached switch number (1-16)> Provides console access to member switches from the master switch. <b>Command mode:</b> Privileged EXEC
<b>[no] stack backup</b> <csnum (1-8)> Defines the backup switch in the stack, based on its configured switch number (csnum). <b>Command mode:</b> Global configuration
<b>[no] stack name</b> <1-63 characters> Defines a name for the stack. <b>Command mode:</b> Global configuration
<b>show stack switch-number</b> <csnum (1-8)> Displays UUID and slot ID for all the configured switches from the stack. <b>Command mode:</b> All

## Stacking Switch Configuration

The following table describes stacking switch configuration commands.

**Table 192.** *Stacking Switch Commands*

Command Syntax and Usage
<p><b>stack switch-number</b> &lt;csnum (1-8)&gt; <b>bay</b> &lt;1-4&gt;</p> <p>Binds the selected switch to the stack, based on its bay number in the chassis. You also must enter the UUID to specify the chassis in which the switch resides.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>stack switch-number</b> &lt;csnum (1-8)&gt; <b>bind</b> &lt;asnum (1-16)&gt;</p> <p>Binds the selected switch to the stack, based on its attached switch number (asnum).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>stack switch-number</b> &lt;csnum (1-8)&gt; <b>description</b> &lt;1-63 characters&gt;</p> <p>Defines a description for each configured switch number of the stack.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>stack switch-number</b> &lt;csnum (1-8)&gt; <b>universal-unic-id</b> &lt;UUID&gt;</p> <p>Binds the selected switch to the stack, based on the UUID of the chassis in which the switch resides. You also must enter the bay number to specify a switch within the chassis. Following is an example UUID:</p> <p>uuid 49407441b1a511d7b95df58f4b6f99fe</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no stack switch-number</b> &lt;csnum (1-8)&gt;</p> <p>Deletes the selected switch from the stack.</p> <p><b>Command mode:</b> Global configuration</p>

## Management Interface Configuration

To provide continuous Management IP reachability in the event of a Master node failover, an additional floating Management IP address can be set up on the management IP interface. The floating Management IP address will be used by the backup switch when taking over management from the failed master node.

**Note:** Floating IP is not supported on EN4093 models.

To configure the floating Management IP address, use the following commands:

**Table 193.** *Management Interface Options*

Command Syntax and Usage
<b>floating ip address</b> <IP address> [<IP netmask>] Configures the specified IPv4 address as a floating Management IP address. <b>Command mode:</b> Interface IP
<b>floating ip netmask</b> <IP netmask> Configures the floating IP subnet mask address. <b>Command mode:</b> Interface IP
<b>no floating</b> Removes all floating IP addresses. <b>Command mode:</b> Interface IP
<b>show interface ip</b> Displays current IP address floating information. <b>Command mode:</b> Global configuration

---

## Quality of Service Configuration

Quality of Service (QoS) commands configure the 802.1p priority value and DiffServ Code Point value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

### 802.1p Configuration

This feature provides the EN4093R the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

**Table 194.** *802.1p Configuration Commands*

Command Syntax and Usage
<p><b>qos transmit-queue mapping</b> &lt;priority (0-7)&gt; &lt;COSq number&gt;</p> <p>Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue that handles the matching traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>qos transmit-queue weight-cos</b> &lt;COSq number&gt; &lt;weight (0-15)&gt;</p> <p>Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>qos unicast-bandwidth</b> &lt;10-100&gt;</p> <p>Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic.</p> <p>The default value is 50.</p> <p><b>Note:</b> This applies to all ports.</p> <p><b>Command mode:</b> All</p>
<p><b>show qos transmit-queue</b></p> <p>Displays the current 802.1p parameters.</p> <p><b>Command mode:</b> All</p>



## DSCP Configuration

These commands map the DiffServ Code Point (DSCP) value of incoming packets to a new value or to an 802.1p priority value.

**Table 195.** *DSCP Configuration Commands*

Command Syntax and Usage
<p><b>qos dscp dot1p-mapping</b> &lt;DSCP (0-63)&gt; &lt;priority (0-7)&gt;</p> <p>Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>qos dscp dscp-mapping</b> &lt;DSCP (0-63)&gt; &lt;new DSCP (0-63)&gt;</p> <p>Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] qos dscp re-marking</b></p> <p>Enables or disables DSCP re-marking globally.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show qos dscp</b></p> <p>Displays the current DSCP parameters.</p> <p><b>Command mode:</b> All</p>

## Control Plane Protection

To prevent switch instability if the switch is unable to process a high rate of control-plane traffic, the switch now supports CoPP. CoPP, allows you to assign control-plane traffic protocols to one of 48 queues, and can set bandwidth limits for each queue.

**Table 196.** *CoPP Commands*

Command Syntax and Usage
<p><b>qos protocol-packet-control packet-queue-map</b> <i>&lt;packet queue number (0-47)&gt; &lt;packet type&gt;</i></p> <p>Configures a packet type to associate with each packet queue number. Enter a queue number, followed by the packet type. You may map multiple packet types to a single queue. The following packet types are allowed:</p> <ul style="list-style-type: none"><li>– <b>802.1x</b> (IEEE 802.1x packets)</li><li>– <b>application-cri-packets</b> (critical packets of various applications, such as Telnet, SSH)</li><li>– <b>arp-bcast</b> (ARP broadcast packets)</li><li>– <b>arp-ucast</b> (ARP unicast reply packets)</li><li>– <b>bgp</b> (BGP packets)</li><li>– <b>bpdu</b> (Spanning Tree Protocol packets)</li><li>– <b>cisco-bpdu</b> (Cisco STP packets)</li><li>– <b>dest-unknown</b> (packets with destination not yet learned)</li><li>– <b>dhcp</b> (DHCP packets)</li><li>– <b>ecp</b> (ECP packets)</li><li>– <b>fips</b> (FIPS packets)</li><li>– <b>icmp</b> (ICMP packets)</li><li>– <b>icmp6</b> (ICMPv6 packets)</li><li>– <b>igmp</b> (IGMP packets)</li><li>– <b>ipv4-miscellaneous</b> (IPv4 packets with IP options and TTL exception)</li><li>– <b>ipv6-nd</b> (IPv6 Neighbor Discovery packets)</li><li>– <b>lACP</b> (LACP/Link Aggregation protocol packets)</li><li>– <b>lldp</b> (LLDP packets)</li><li>– <b>oflow-cntrlr</b> (packets hit openflow send-to-controller filter)</li><li>– <b>oflow-default</b> (packets hit openflow default filter)</li><li>– <b>oflow-mgmt</b> (packets hit openflow management filter)</li><li>– <b>ospf</b> (OSPF packets)</li><li>– <b>ospf3</b> (OSPF3 Packets)</li><li>– <b>pim</b> (PIM packets)</li><li>– <b>ptp</b> (PTP packets)</li><li>– <b>rip</b> (RIP packets)</li><li>– <b>system</b> (system protocols, such as tftp, ftp, telnet, ssh)</li><li>– <b>udld</b> (UDLD packets)</li><li>– <b>vlag</b> (vLAG packets)</li><li>– <b>vrrp</b> (VRRP packets)</li></ul> <p><b>Command mode:</b> Global configuration</p>

**Table 196.** CoPP Commands

<b>Command Syntax and Usage</b>
<p><b>no qos protocol-packet-control packet-queue-map</b> <i>&lt;packet type&gt;</i> Clears the selected packet type from its associated packet queue. <b>Command mode:</b> Global configuration</p>
<p><b>qos protocol-packet-control rate-limit-packet-queue</b> <i>&lt;packet queue number (0-47)&gt;</i> <i>&lt;1-10000&gt;</i> Configures the number of packets per second allowed for each packet queue. <b>Command mode:</b> Global configuration</p>
<p><b>no qos protocol-packet-control rate-limit-packet-queue</b> <i>&lt;packet queue number (0-47)&gt;</i> Clears the packet rate configured for the selected packet queue. <b>Command mode:</b> Global configuration</p>
<p><b>show qos protocol-packet-control information protocol</b> Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. <b>Command mode:</b> All</p>
<p><b>show qos protocol-packet-control information queue</b> Displays the packet rate configured for each packet queue. <b>Command mode:</b> All</p>

## Weighted Random Early Detection Configuration

Weighted Random Early Detection (WRED) provides congestion avoidance by pre-emptively dropping packets before a queue becomes full. EN4093R implementation of WRED defines TCP and non-TCP traffic profiles on a per-port, per COS queue basis. For each port, you can define a transmit-queue profile with thresholds that define packet-drop probability.

These commands allow you to configure global WRED parameters. For port WRED commands, see [“Port WRED Configuration” on page 378](#).

**Table 197.** *WRED Configuration Options*

Command Syntax and Usage
<p><b>[no] qos random-detect ecn</b></p> <p>Enables or disables Explicit Congestion Notification (ECN). When ECN is enabled, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions.</p> <p><b>Note:</b> ECN functions only on TCP traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] qos random-detect enable</b></p> <p>Enables or disables Random Detection and avoidance.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show qos random-detect</b></p> <p>Displays current Random Detection and avoidance parameters.</p> <p><b>Command mode:</b> All</p>

## WRED Transmit Queue Configuration

The following table displays WRED Transmit Queue configuration commands.

**Table 198.** *WRED Transmit Queue Options*

Command Syntax and Usage
<p><b>[no] qos random-detect transmit-queue &lt;0-7&gt; enable</b></p> <p>Sets the WRED transmit queue configuration to on or off.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>qos random-detect transmit-queue &lt;0-7&gt; tcp</b> <i>&lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt;</i></p> <p>Configures the WRED thresholds for TCP traffic.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 198.** *WRED Transmit Queue Options*

<b>Command Syntax and Usage</b>
<p><b>qos random-detect transmit-queue</b> &lt;0-7&gt; <b>non-tcp</b> &lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt; Configures the WRED thresholds for non-TCP traffic. <b>Command mode:</b> Global configuration</p>
<p><b>no qos random-detect transmit-queue</b> &lt;0-7&gt; <b>{tcp non-tcp}</b> Clears the specified WRED threshold value. <b>Command mode:</b> Global configuration</p>

---

## Access Control Configuration

Use these commands to create Access Control Lists and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

For information about assigning ACLs to ports, see [“Port ACL Configuration” on page 377](#).

**Table 199.** *General ACL Configuration Commands*

Command Syntax and Usage
<b>[no] access-control group</b> <1-640> Configures an ACL Group. To view command options, see <a href="#">page 407</a> . <b>Command mode:</b> Global configuration
<b>[no] access-control list</b> <1-640> Configures an Access Control List. To view command options, see <a href="#">page 391</a> . <b>Command mode:</b> Global configuration
<b>[no] access-control list6</b> <1-128> Configures an IPv6 Access Control List. To view command options, see <a href="#">page 396</a> . <b>Command mode:</b> Global configuration
<b>show access-control</b> Displays the current ACL parameters. <b>Command mode:</b> All

## Access Control List Configuration

These commands allow you to define filtering criteria for each Access Control List (ACL).

**Table 200.** *ACL Configuration Commands*

Command Syntax and Usage
<p><b>access-control list</b> &lt;1-640&gt; <b>action</b> {<b>permit</b> <b>deny</b>  <b>set-priority</b> &lt;0-7&gt;}</p> <p>Configures a filter action for packets that match the ACL definitions. You can choose to <b>permit</b> (pass) or <b>deny</b> (drop) packets, or set the 802.1p priority level (0-7).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access-control list</b> &lt;1-640&gt; <b>action redirect</b> {<b>port</b> &lt;port number&gt; <b>portchannel</b> &lt;1-24&gt;}</p> <p>Configures the redirection of packets that match the ACL definitions. You can choose to redirect packets either through an ethernet port or a Link Aggregation Group (LAG).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list</b> &lt;1-640&gt; <b>egress-port port</b> &lt;port alias or number&gt;</p> <p>Configures the ACL to function on egress packets.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list</b> &lt;1-640&gt; <b>log</b></p> <p>Enables or disables logging for the Access Control List.</p> <p><b>Note:</b> Enabling the LOG feature neutralizes ACL deny filter actions for Telnet and SSH traffic that is addressed to the switch's Layer 3 interfaces.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list</b> &lt;1-640&gt; <b>statistics</b></p> <p>Enables or disables the statistics collection for the Access Control List.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>default access-control list</b> &lt;1-640&gt;</p> <p>Resets the ACL parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show access-control list</b> &lt;1-640&gt;</p> <p>Displays the current ACL parameters.</p> <p><b>Command mode:</b> All</p>
<p><b>[no] access-control list6</b> &lt;1-128&gt;</p> <p>Configures an IPv6 Access Control List. To view command options, see <a href="#">page 396</a>.</p> <p><b>Command mode:</b> Global configuration</p>

## Ethernet Filtering Configuration

These commands allow you to define Ethernet matching criteria for an ACL.

**Table 201.** *Ethernet Filtering Configuration Commands*

Command Syntax and Usage
<p><b>[no] access-control list &lt;1-640&gt; ethernet destination-mac-address &lt;MAC address&gt; [&lt;MAC mask&gt;]</b>            Defines the destination MAC address for this ACL.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list &lt;1-640&gt; ethernet source-mac-address &lt;MAC address&gt; [&lt;MAC mask&gt;]</b>            Defines the source MAC address for this ACL.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list &lt;1-640&gt; ethernet ethernet-type {any arp ip ipv6 mpls rarp &lt;other (0x600-0xFFFF)&gt;}</b>            Defines the Ethernet type for this ACL.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list &lt;1-640&gt; ethernet vlan &lt;VLAN ID&gt; [&lt;VLAN mask&gt;]</b>            Defines a VLAN number and mask for this ACL.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list &lt;1-640&gt; ethernet priority &lt;0-7&gt;</b>            Defines the Ethernet priority value for the ACL.  <b>Command mode:</b> Global configuration</p>
<p><b>default access-control list &lt;1-640&gt; ethernet</b>            Resets Ethernet parameters for the ACL to their default values.  <b>Command mode:</b> Global configuration</p>
<p><b>no access-control list &lt;1-640&gt; ethernet</b>            Removes Ethernet parameters for the ACL.  <b>Command mode:</b> Global configuration</p>
<p><b>show access-control list &lt;1-640&gt; ethernet</b>            Displays the current Ethernet parameters for the ACL.  <b>Command mode:</b> All</p>



## IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an ACL.

**Table 202.** *IP version 4 Filtering Configuration Commands*

Command Syntax and Usage															
<p><b>[no] access-control list &lt;1-640&gt; ipv4 destination-ip-address &lt;IP address&gt; [&lt;IP mask&gt;]</b></p> <p>Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>															
<p><b>[no] access-control list &lt;1-640&gt; ipv4 source-ip-address &lt;IP address&gt; [&lt;IP mask&gt;]</b></p> <p>Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>															
<p><b>[no] access-control list &lt;1-640&gt; ipv4 protocol &lt;0-255&gt;</b></p> <p>Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>icmp</td> </tr> <tr> <td>2</td> <td>igmp</td> </tr> <tr> <td>6</td> <td>tcp</td> </tr> <tr> <td>17</td> <td>udp</td> </tr> <tr> <td>89</td> <td>ospf</td> </tr> <tr> <td>112</td> <td>vrrp</td> </tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	1	icmp	2	igmp	6	tcp	17	udp	89	ospf	112	vrrp	
Number	Name														
1	icmp														
2	igmp														
6	tcp														
17	udp														
89	ospf														
112	vrrp														
<p><b>[no] access-control list &lt;1-640&gt; ipv4 type-of-service &lt;0-255&gt;</b></p> <p>Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.</p> <p><b>Command mode:</b> Global configuration</p>															
<p><b>default access-control list &lt;1-640&gt; ipv4</b></p> <p>Resets the IPv4 parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>															
<p><b>show access-control list &lt;1-640&gt; ipv4</b></p> <p>Displays the current IPv4 parameters.</p> <p><b>Command mode:</b> All</p>															

## TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

**Table 203.** TCP/UDP Filtering Configuration Commands

Command Syntax and Usage																													
<p><b>[no] access-control list</b> &lt;1-640&gt; <b>tcp-udp source-port</b>            &lt;1-65535&gt; [<i>&lt;mask (0xFFFF)&gt;</i>]</p> <p>Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	20	ftp-data	21	ftp	22	ssh	23	telnet	25	smtp	37	time	42	name	43	whois	53	domain	69	tftp	70	gopher	79	finger	80	http	
Number	Name																												
20	ftp-data																												
21	ftp																												
22	ssh																												
23	telnet																												
25	smtp																												
37	time																												
42	name																												
43	whois																												
53	domain																												
69	tftp																												
70	gopher																												
79	finger																												
80	http																												
<p><b>[no] access-control list</b> &lt;1-640&gt; <b>tcp-udp destination-port</b>            &lt;1-65535&gt; [<i>&lt;mask (0xFFFF)&gt;</i>]</p> <p>Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>source-port</code> above.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>[no] access-control list</b> &lt;1-640&gt; <b>tcp-udp flags</b> &lt;value (0x0-0x3f)&gt;            [<i>&lt;mask (0x0-0x3f)&gt;</i>]</p> <p>Defines a TCP/UDP flag for the ACL.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>default access-control list</b> &lt;1-640&gt; <b>tcp-udp</b></p> <p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>show access-control list</b> &lt;1-640&gt; <b>tcp-udp</b></p> <p>Displays the current TCP/UDP Filtering parameters.</p> <p><b>Command mode:</b> All</p>																													

## Packet Format Filtering Configuration

These commands allow you to define Packet Format matching criteria for an ACL.

**Table 204.** *Packet Format Filtering Configuration Commands*

Command Syntax and Usage
<b>[no] access-control list &lt;1-640&gt; packet-format ethernet {ethertype2 llc snap}</b> Defines the Ethernet format for the ACL. <b>Command mode:</b> Global configuration
<b>[no] access-control list &lt;1-640&gt; packet-format ip {ipv4 ipv6}</b> Defines the IP format for the ACL. <b>Command mode:</b> Global configuration
<b>[no] access-control list &lt;1-640&gt; packet-format tagging {any none tagged}</b> Defines the tagging format for the ACL. <b>Command mode:</b> Global configuration
<b>default access-control list &lt;1-640&gt; packet-format</b> Resets Packet Format parameters for the ACL to their default values. <b>Command mode:</b> Global configuration
<b>show access-control list &lt;1-640&gt; packet-format</b> Displays the current Packet Format parameters for the ACL. <b>Command mode:</b> All

## ACL IPv6 Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL).

**Table 205.** *IPv6 ACL Options*

Command Syntax and Usage
<p><b>access-control list6</b> &lt;1-128&gt; <b>action</b> {permit deny   set-priority &lt;0-7&gt;}</p> <p>Configures a filter action for packets that match the ACL definitions. You can choose to <b>permit</b> (pass) or <b>deny</b> (drop) packets, or set the 802.1p priority level (0-7).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list6</b> &lt;1-128&gt; <b>egress-port port</b> &lt;port alias or number&gt;</p> <p>Configures the ACL to function on egress packets.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list6</b> &lt;1-128&gt; <b>statistics</b></p> <p>Enables or disables the statistics collection for the Access Control List.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>default access-control list6</b> &lt;1-128&gt;</p> <p>Resets the ACL parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show access-control list6</b> &lt;1-128&gt;</p> <p>Displays the current ACL parameters.</p> <p><b>Command mode:</b> All</p>

## IPv6 Filtering Configuration

These commands allow you to define IPv6 matching criteria for an ACL.

**Table 206.** *IP version 6 Filtering Options*

Command Syntax and Usage
<p><b>[no] access-control list6 &lt;1-128&gt; ipv6 destination-address</b>            &lt;IPv6 address&gt; [<i>&lt;prefix length (1-128)&gt;</i>]</p> <p>Defines a destination IPv6 address for the ACL. If defined, traffic with this destination address will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list6 &lt;1-128&gt; ipv6 source-address</b>            &lt;IPv6 address&gt; [<i>&lt;prefix length (1-128)&gt;</i>]</p> <p>Defines a source IPv6 address for the ACL. If defined, traffic with this source address will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list6 &lt;1-128&gt; ipv6 flow-label &lt;0-1048575&gt;</b></p> <p>Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list6 &lt;1-128&gt; ipv6 next-header &lt;0-255&gt;</b></p> <p>Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list6 &lt;1-128&gt; ipv6 traffic-class &lt;0-255&gt;</b></p> <p>Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>default access-control list6 &lt;1-128&gt; ipv6</b></p> <p>Resets the IPv6 parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show access-control list6 &lt;1-128&gt; ipv6</b></p> <p>Displays the current IPv6 parameters.</p> <p><b>Command mode:</b> All</p>

## IPv6 TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

**Table 207.** IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage																													
<p><b>[no] access-control list6</b> &lt;1-128&gt; <b>tcp-udp source-port</b> &lt;1-65535&gt; [<i>&lt;mask (0xFFFF)&gt;</i>]</p> <p>Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	20	ftp-data	21	ftp	22	ssh	23	telnet	25	smtp	37	time	42	name	43	whois	53	domain	69	tftp	70	gopher	79	finger	80	http	
Number	Name																												
20	ftp-data																												
21	ftp																												
22	ssh																												
23	telnet																												
25	smtp																												
37	time																												
42	name																												
43	whois																												
53	domain																												
69	tftp																												
70	gopher																												
79	finger																												
80	http																												
<p><b>[no] access-control list6</b> &lt;1-128&gt; <b>tcp-udp destination-port</b> &lt;1-65535&gt; [<i>&lt;mask (0xFFFF)&gt;</i>]</p> <p>Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>source-port</code> above.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>[no] access-control list6</b> &lt;1-128&gt; <b>tcp-udp flags</b> &lt;value (0x0-0x3f)&gt; [<i>&lt;mask (0x0-0x3f)&gt;</i>]</p> <p>Defines a TCP/UDP flag for the ACL.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>default access-control list6</b> &lt;1-128&gt; <b>tcp-udp</b></p> <p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>show access-control list6</b> &lt;1-128&gt; <b>tcp-udp</b></p> <p>Displays the current TCP/UDP Filtering parameters.</p> <p><b>Command mode:</b> All</p>																													

## IPv6 Metering Configuration

These commands define the Access Control profile for the selected ACL.

**Table 208.** IPv6 Metering Options

Command Syntax and Usage
<b>access-control list6 &lt;1-128&gt; meter action {drop pass}</b> Configures the ACL Meter to either drop or pass out-of-profile traffic. <b>Command mode:</b> Global configuration
<b>access-control list6 &lt;1-128&gt; meter committed-rate &lt;64-4000000&gt;</b> Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64. <b>Command mode:</b> Global configuration
<b>[no] access-control list6 &lt;1-128&gt; meter enable</b> Enables or disables ACL Metering. <b>Command mode:</b> Global configuration
<b>access-control list6 &lt;1-128&gt; meter maximum-burst-size &lt;32-4096&gt;</b> Configures the maximum burst size, in kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096. <b>Command mode:</b> Global configuration
<b>default access-control list6 &lt;1-128&gt; meter</b> Sets the ACL meter configuration to its default values. <b>Command mode:</b> Global configuration
<b>no access-control list6 &lt;1-128&gt; meter</b> Deletes the selected ACL meter. <b>Command mode:</b> Global configuration
<b>show access-control list6 &lt;1-128&gt; meter</b> Displays current ACL Metering parameters. <b>Command mode:</b> All

## Management ACL Filtering Configuration

These commands allow you to define matching criteria for a Management ACL.

**Note:** Management ACLs filter traffic received through data interfaces only. The management interface is not monitored.

**Table 209.** Management ACL Filtering Configuration Commands

Command Syntax and Usage	
<b>[no] access-control macl &lt;1-128&gt; ipv4</b>	Enables or disables the Management ACL. <b>Command mode:</b> Global configuration
<b>[no] access-control macl &lt;1-128&gt; ipv4 &lt;destination IP address&gt; [&lt;address mask&gt;]</b>	Sets IPv4 filtering to filter on the destination IP address. <b>Command mode:</b> Global configuration
<b>[no] access-control macl &lt;1-128&gt; ipv4 &lt;source IP address&gt; [&lt;address mask&gt;]</b>	Sets IPv4 filtering to filter on the source IP address. <b>Command mode:</b> Global configuration
<b>[no] access-control macl &lt;1-128&gt; ipv4 protocol &lt;0-255&gt;</b>	Defines an IP protocol for the MACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed here are some of the well-known protocols. <b>Number</b> <b>Name</b> 1            icmp 2            igmp 6            tcp 17          udp 89          ospf 112         vrrp <b>Command mode:</b> Global configuration
<b>default access-control list &lt;1-128&gt; ipv4</b>	Resets the IPv4 parameters for the ACL to their default values. <b>Command mode:</b> Global configuration
<b>show access-control list &lt;1-128&gt; packet-format</b>	Displays the current Packet Format parameters for the ACL. <b>Command mode:</b> All



## TCP/UDP Filtering Configuration

The following commands allow you to define TCP/UDP matching criteria for a Management ACL.

**Table 210.** Management ACL TCP/UDP Filtering Configuration Commands

Command Syntax and Usage																													
<p><b>[no] access-control mac1 &lt;1-128&gt; tcp-udp source-port &lt;1-65535&gt; [&lt;mask (0x0-0x3f)&gt;]</b></p> <p>Defines a source port for the Management ACL. If defined, traffic with the specified TCP or UDP source port will match this Management ACL. Specify the port number. Listed here are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	20	ftp-data	21	ftp	22	ssh	23	telnet	25	smtp	37	time	42	name	43	whois	53	domain	69	tftp	70	gopher	79	finger	80	http	
Number	Name																												
20	ftp-data																												
21	ftp																												
22	ssh																												
23	telnet																												
25	smtp																												
37	time																												
42	name																												
43	whois																												
53	domain																												
69	tftp																												
70	gopher																												
79	finger																												
80	http																												
<p><b>[no] access-control mac1 &lt;1-128&gt; tcp-udp destination-port &lt;1-65535&gt; [&lt;mask (0xFFFF)&gt;]</b></p> <p>Defines a destination port for the Management ACL. If defined, traffic with the specified TCP or UDP destination port will match this Management ACL. Specify the port number, just as with <code>source-port</code>.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>default access-control list &lt;1-640&gt; tcp-udp</b></p> <p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>																													
<p><b>show access-control list &lt;1-640&gt; tcp-udp</b></p> <p>Displays the current TCP/UDP Filtering parameters.</p> <p><b>Command mode:</b> All</p>																													

## VMAP Configuration

A VLAN Map is an Access Control List (ACL) that can be assigned to a VLAN or a VM group instead of a port. In a virtualized environment where Virtual Machines move between physical servers, VLAN Maps allow you to create traffic filtering and metering policies associated with a VM's VLAN.

For more information about VLAN Map configuration commands, see [“Access Control List Configuration” on page 391](#).

For more information about assigning VLAN Maps to a VLAN, see [“VLAN Configuration” on page 458](#).

For more information about assigning VLAN Maps to a VM group, see [“VM Group Configuration” on page 571](#).

[Table 211](#) lists the general VMAP configuration commands.

**Table 211.** *VMAP Configuration Commands*

Command Syntax and Usage
<p><b>access-control vmap</b> &lt;1-128&gt; <b>action</b> {<b>permit</b> <b>deny</b>} <b>set-priority</b> &lt;0-7&gt;}</p> <p>Configures a filter action for packets that match the VMAP definitions. You can choose to <b>permit</b> (pass) or <b>deny</b> (drop) packets, or set the 802.1p priority level (0-7).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap</b> &lt;1-128&gt; <b>egress-port</b> &lt;port alias or number&gt;</p> <p>Configures the VMAP to function on egress packets.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap</b> &lt;1-128&gt; <b>ethernet destination-mac-address</b> &lt;MAC address&gt; &lt;MAC mask&gt;</p> <p>Enables or disables filtering of VMAP statistics collection based on destination MAC.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap</b> &lt;1-128&gt; <b>ethernet source-mac-address</b> &lt;MAC address&gt; &lt;MAC mask&gt;</p> <p>Enables or disables filtering of VMAP statistics collection based on source MAC.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 211.** VMAP Configuration Commands (continued)

Command Syntax and Usage
<p><b>[no] access-control vmap &lt;1-128&gt; ethernet ethernet-type {&lt;0x600-0xFFF&gt; any arp rarp ip ipv6 mpls}</b></p> <p>Enables or disables filtering of VMAP statistics collection based on the encapsulated protocol:</p> <ul style="list-style-type: none"> <li>o &lt;0x600-0xFFF&gt; filters Ethernet frames with the specified EtherType</li> <li>o any filters all frames</li> <li>o arp filters Address Resolution Protocol frames</li> <li>o rarp filters Reverse Address Resolution Protocol frames</li> <li>o ip filters Internet Protocol version 4 frames</li> <li>o ipv6 filters Internet Protocol version 6 frames</li> <li>o mpls filters Multiprotocol Label Switching frames</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; ethernet priority &lt;0-7&gt;</b></p> <p>Enables or disables filtering of VMAP statistics collection based on the IEEE 802.1Q priority code point value.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; ethernet vlan &lt;1-4094&gt;</b></p> <p>Enables or disables filtering of VMAP statistics collection based on VLAN ID.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; ipv4 destination-ip-address &lt;IPv4 address&gt; &lt;IPv4 mask&gt;</b></p> <p>Enables or disables filtering of VMAP statistics collection based on destination IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; ipv4 source-ip-address &lt;IPv4 address&gt; &lt;IPv4 mask&gt;</b></p> <p>Enables or disables filtering of VMAP statistics collection based on source IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; ipv4 protocol &lt;0-255&gt;</b></p> <p>Enables or disables filtering of VMAP statistics collection based on protocol.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; ipv4 type-of-service &lt;0-255&gt;</b></p> <p>Enables or disables filtering of VMAP statistics collection based on type of service.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 211.** VMAP Configuration Commands (continued)

Command Syntax and Usage
<p><b>access-control vmap &lt;1-128&gt; meter action {drop pass}</b>  Sets ACL port metering to drop or pass out-of-profile traffic.  <b>Command mode:</b> Global configuration</p>
<p><b>access-control vmap &lt;1-128&gt; meter committed-rate &lt;64-10000000&gt;</b>  Sets the ACL port metering control rate in kilobits per second.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; meter enable</b>  Enables or disables ACL port metering.  <b>Command mode:</b> All except User EXEC</p>
<p><b>access-control vmap &lt;1-128&gt; meter maximum-burst-size &lt;32-4096&gt;</b>  Sets the ACL port metering maximum burst size in kilobytes. The following eight values are allowed:</p> <ul style="list-style-type: none"> <li>– 32</li> <li>– 64</li> <li>– 128</li> <li>– 256</li> <li>– 512</li> <li>– 1024</li> <li>– 2048</li> <li>– 4096</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>access-control vmap &lt;1-128&gt; mirror port &lt;port&gt;</b>  Sets the specified port as the mirror target.  <b>Command mode:</b> Global configuration</p>
<p><b>no access-control vmap &lt;1-128&gt; mirror</b>  Turns off ACL mirroring.  <b>Command mode:</b> Global configuration</p>
<p><b>access-control vmap &lt;1-128&gt; packet-format ethernet {ethernet-type2 llc snap}</b>  Sets to filter the specified ethernet packet format type.  <b>Command mode:</b> Global configuration</p>
<p><b>access-control vmap &lt;1-128&gt; packet-format ip {ipv4 ipv6}</b>  Sets to filter the specified IP packet format type.  <b>Command mode:</b> Global configuration</p>

**Table 211.** VMAP Configuration Commands (continued)

Command Syntax and Usage
<p><b>access-control vmap &lt;1-128&gt; packet-format tagging {any none tagged}</b></p> <p>Sets filtering based on packet tagging. The options are:</p> <ul style="list-style-type: none"> <li>– any: Filter tagged &amp; untagged packets</li> <li>– none: Filter only untagged packets</li> <li>– tagged: Filter only tagged packets</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no access-control vmap &lt;1-128&gt; packet-format {ethernet ip tagging}</b></p> <p>Disables filtering based on the specified packet format.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access-control vmap &lt;1-128&gt; re-mark dot1p &lt;0-7&gt;</b></p> <p>Sets the ACL re-mark configuration user update priority.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no access-control vmap &lt;1-128&gt; re-mark dot1p</b></p> <p>Disables the use of dot1p for in-profile traffic ACL re-mark configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access-control vmap &lt;1-128&gt; re-mark {in-profile out-profile} dscp &lt;0-63&gt;</b></p> <p>Sets the ACL re-mark configuration user update priority.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no access-control vmap &lt;1-128&gt; re-mark {in-profile out-profile}</b></p> <p>Removes all re-mark in-profile or out-profile settings.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; re-mark use-tos-precedence</b></p> <p>Enables or disables the use of the TOS precedence for in-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control vmap &lt;1-128&gt; statistics</b></p> <p>Enables or disables the statistics collection for the VMAP.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access-control vmap &lt;1-128&gt; tcp-udp {source-port destination-port} &lt;1-65535&gt; [&lt;port mask (0x0001 - 0xFFFF)&gt;]</b></p> <p>Sets the TCP/UDP filtering source port or destination port and port mask for this ACL.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 211.** *VMAP Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>access-control vmap</b> &lt;1-128&gt; <b>tcp-udp flags</b> &lt;value (0x0-0x3F)&gt; [&lt;flags mask (0x0-0x3F)&gt;] Sets the TCP flags for this ACL. <b>Command mode:</b> Global configuration</p>
<p><b>no access-control vmap</b> &lt;1-128&gt; <b>tcp-udp</b> Removes TCP/UDP filtering for this ACL. <b>Command mode:</b> Global configuration</p>
<p><b>default access-control vmap</b> &lt;1-128&gt; Resets the VMAP parameters to their default values. <b>Command mode:</b> Global configuration</p>
<p><b>show access-control vmap</b> &lt;1-128&gt; Displays the current VMAP parameters. <b>Command mode:</b> All</p>

## ACL Group Configuration

These commands allow you to compile one or more ACLs into an ACL group. Once you create an ACL group, you can assign the ACL group to one or more ports.

**Table 212.** *ACL Group Configuration Commands*

Command Syntax and Usage
<b>[no] access-control group &lt;1-640&gt; list &lt;1-640&gt;</b> Adds or removes the selected ACL to/from the ACL group. <b>Command mode:</b> Global configuration
<b>[no] access-control group &lt;1-640&gt; list6 &lt;1-128&gt;</b> Adds or removes the selected IPv6 ACL to/from the ACL group. <b>Command mode:</b> Global configuration
<b>show access-control group &lt;1-640&gt;</b> Displays the current ACL group parameters. <b>Command mode:</b> All

## ACL Metering Configuration

These commands define the Access Control profile for the selected ACL or ACL Group.

**Table 213.** *ACL Metering Configuration Commands*

Command Syntax and Usage
<p><b>access-control list</b> &lt;1-640&gt; <b>meter action</b> {drop pass}</p> <p>Configures the ACL meter to either drop or pass out-of-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access-control list</b> &lt;1-640&gt; <b>meter committed-rate</b> &lt;64-10000000&gt;</p> <p>Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] access-control list</b> &lt;1-640&gt; <b>meter enable</b></p> <p>Enables or disables ACL Metering.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>access-control list</b> &lt;1-640&gt; <b>meter maximum-burst-size</b> &lt;32-4096&gt;</p> <p>Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>default access-control list</b> &lt;1-640&gt; <b>meter</b></p> <p>Sets the ACL meter configuration to its default values.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no access-control list</b> &lt;1-640&gt; <b>meter</b></p> <p>Deletes the selected ACL meter.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show access-control list</b> &lt;1-640&gt; <b>meter</b></p> <p>Displays current ACL Metering parameters.</p> <p><b>Command mode:</b> All</p>



## ACL Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL metering profile, or out of the ACL metering profile.

**Table 214.** *ACL Re-Marking Configuration Commands*

Command Syntax and Usage
<b>access-control list &lt;1-640&gt; re-mark dot1p &lt;0-7&gt;</b> Defines 802.1p value. The value is the priority bits information in the packet structure. <b>Command mode:</b> Global configuration
<b>no access-control list &lt;1-640&gt; re-mark dot1p</b> Disables use of 802.1p value for re-marked packets. <b>Command mode:</b> Global configuration
<b>[no] access-control list &lt;1-640&gt; re-mark use-tos-precedence</b> Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value. <b>Command mode:</b> Global configuration
<b>default access-control list &lt;1-640&gt; re-mark</b> Sets the ACL Re-mark configuration to its default values. <b>Command mode:</b> Global configuration
<b>show access-control list &lt;1-640&gt; re-mark</b> Displays current Re-mark parameters. <b>Command mode:</b> All

## Re-Marking In-Profile Configuration

The following table displays Re-marking In-profile configuration commands.

**Table 215.** *ACL Re-Mark In-Profile Commands*

Command Syntax and Usage
<b>access-control list &lt;1-640&gt; re-mark in-profile dscp &lt;0-63&gt;</b> Sets the DiffServ Code Point (DSCP) of in-profile packets to the selected value. <b>Command mode:</b> Global configuration
<b>no access-control list &lt;1-640&gt; re-mark in-profile dscp</b> Disables use of DSCP value for in-profile traffic. <b>Command mode:</b> Global configuration
<b>no access-control list &lt;1-640&gt; re-mark in-profile</b> Removes all re-mark in-profile settings. <b>Command mode:</b> Global configuration
<b>show access-control list &lt;1-640&gt; re-mark</b> Displays current re-mark parameters. <b>Command mode:</b> All

## Re-Marking Out-Profile Configuration

The following table displays Re-marking Out-profile configuration commands.

**Table 216.** *ACL Re-Mark Out-of-Profile Commands*

Command Syntax and Usage
<b>access-control list &lt;1-640&gt; re-mark out-profile dscp &lt;0-63&gt;</b> Sets the DiffServ Code Point (DSCP) of out-of-profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets. <b>Command mode:</b> Global configuration
<b>no access-control list &lt;1-640&gt; re-mark out-profile</b> Removes all re-mark out-profile settings. <b>Command mode:</b> Global configuration
<b>show access-control list &lt;1-640&gt; re-mark</b> Displays current re-mark parameters. <b>Command mode:</b> All

## IPv6 Re-Marking Configuration

You can choose to re-mark IPv6 header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within or outside the ACL metering profile.

**Table 217.** IPv6 General Re-Mark Options

Command Syntax and Usage
<b>access-control list6 &lt;1-128&gt; re-mark dot1p &lt;0-7&gt;</b> Re-marks the 802.1p value. The value is the priority bits information in the packet structure. <b>Command mode:</b> Global configuration
<b>no access-control list6 &lt;1-128&gt; re-mark dot1p</b> Disables use of 802.1p value for re-marked packets. <b>Command mode:</b> Global configuration
<b>[no] no access-control list6 &lt;1-128&gt; re-mark use-tos-precedence</b> Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. <b>Command mode:</b> Global configuration
<b>default access-control list6 &lt;1-128&gt; re-mark</b> Sets the ACL re-mark parameters to their default values. <b>Command mode:</b> Global configuration
<b>show access-control list6 &lt;1-128&gt; re-mark</b> Displays current re-mark parameters. <b>Command mode:</b> All

## IPv6 Re-Marking In-Profile Configuration

The following table displays IPv6 Re-marking In-profile configuration commands.

**Table 218.** *IPv6 Re-Mark In-Profile Options*

Command Syntax and Usage
<b>access-control list6 &lt;1-128&gt; re-mark in-profile dscp &lt;0-63&gt;</b> Re-marks the DSCP value for in-profile traffic. <b>Command mode:</b> Global configuration
<b>no access-control list6 &lt;1-128&gt; re-mark in-profile dscp</b> Disables the use of DSCP for the in-profile traffic. <b>Command mode:</b> Global configuration
<b>no access-control list6 &lt;1-128&gt; re-mark in-profile</b> Removes all re-mark in-profile settings. <b>Command mode:</b> Global configuration
<b>show access-control list6 &lt;1-128&gt; re-mark</b> Displays current re-mark parameters. <b>Command mode:</b> All

## IPv6 Re-Marking Out-Profile Configuration

The following table displays IPv6 Re-marking Out-profile configuration commands.

**Table 219.** *IPv6 Re-Mark Out-of-Profile Options*

Command Syntax and Usage
<b>access-control list6 &lt;1-128&gt; re-mark out-profile dscp &lt;0-63&gt;</b> Re-marks the DSCP value on out-of-profile packets for the ACL. <b>Command mode:</b> Global configuration
<b>no access-control list6 &lt;1-128&gt; re-mark out-profile</b> Removes all re-marking out-of-profile settings. <b>Command mode:</b> Global configuration
<b>show access-control list6 &lt;1-128&gt; re-mark</b> Displays current re-mark parameters. <b>Command mode:</b> All

---

## Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the EN4093R, see “Appendix A: Troubleshooting” in the *Enterprise NOS 8.4 Application Guide*.

**Note:** Traffic on VLAN 4095 is not mirrored to the external ports.

Port Mirroring commands are used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

**Table 220.** *Port Mirroring Configuration Commands*

Command Syntax and Usage
<b>[no] port-mirroring enable</b> Enables or disables port mirroring. <b>Command mode:</b> Global configuration
<b>show port-mirroring</b> Displays current settings of the mirrored and monitoring ports. <b>Command mode:</b> All

## Port Mirroring Configuration

The following table displays Port Mirror configuration commands.

**Table 221.** *Port-Based Port Mirroring Configuration Commands*

Command Syntax and Usage
<p><b>port-mirroring monitor-port</b> <i>&lt;port alias or number&gt;</i> <b>mirroring-port</b> <i>&lt;port alias or number&gt;</i> <b>{in out both}</b></p> <p>Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:</p> <p>If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port.</p> <p>If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.</p> <p><b>Note:</b> Up to two monitor ports with 2-way mirroring or four monitor ports with 1-way mirroring are supported in stand-alone mode. In stacking mode, the switch supports one monitor port with 2-way mirroring or two monitor ports with 1-way mirroring.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no port-mirroring monitor-port</b> <i>&lt;port alias or number&gt;</i> <b>mirroring-port</b> <i>&lt;port alias or number&gt;</i></p> <p>Removes the mirrored port.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show port-mirroring</b></p> <p>Displays the current settings of the monitoring port.</p> <p><b>Command mode:</b> All</p>

---

## Layer 2 Configuration

The following table describes basic Layer 2 Configuration commands. The following sections provide more detailed information and commands.

**Table 222.** *Layer 2 Configuration Commands*

Command Syntax and Usage
<p><b>spanning-tree mode disable</b></p> <p>Globally turns Spanning Tree off (selects Spanning-Tree mode “disable”). All ports are placed into forwarding state. Any BPDU’s received are flooded. To enable Spanning-Tree, select another Spanning-Tree mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] spanning-tree stg-auto</b></p> <p>Enables or disables VLAN Automatic STG Assignment (VASA). When enabled, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool.</p> <p><b>Note:</b> VASA applies only to PVRST mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] spanning-tree pvst-compatibility</b></p> <p>Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] spanning-tree loopguard</b></p> <p>Enables or disables Spanning Tree Loop Guard.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>vlan</b> &lt;VLAN number&gt;</p> <p>Enter VLAN configuration mode. To view command options, see <a href="#">page 458</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show layer2</b></p> <p>Displays current Layer 2 parameters.</p> <p><b>Command mode:</b> All</p>

## 802.1X Configuration

These commands allow you to configure the EN4093R as an IEEE 802.1X Authenticator, to provide port-based network access control.

**Table 223.** *802.1X Configuration Commands*

Command Syntax and Usage
<b>[no] dot1x enable</b> Globally enables or disables 802.1X. <b>Command mode:</b> Global configuration
<b>show dot1x</b> Displays current 802.1X parameters. <b>Command mode:</b> All

### 802.1X Global Configuration

The global 802.1X commands allow you to configure parameters that affect all ports in the EN4093R.

**Table 224.** *802.1X Global Configuration Commands*

Command Syntax and Usage
<b>dot1x max-request</b> <1-10> Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2. <b>Command mode:</b> Global configuration
<b>dot1x mode</b> [ <b>force-unauthorized</b>   <b>auto</b>   <b>force-authorized</b> ] Sets the type of access control for all ports: <ul style="list-style-type: none"><li>o <b>force-unauthorized</b> - the port is unauthorized unconditionally.</li><li>o <b>auto</b> - the port is unauthorized until it is successfully authorized by the RADIUS server.</li><li>o <b>force-authorized</b> - the port is authorized unconditionally, allowing all traffic.</li></ul> The default value is <b>force-authorized</b> . <b>Command mode:</b> Global configuration
<b>dot1x quiet-time</b> <0-65535> Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60. <b>Command mode:</b> Global configuration



**Table 224.** 802.1X Global Configuration Commands (continued)

Command Syntax and Usage
<p><b>[no] dot1x re-authenticate</b></p> <p>Sets the re-authentication status to <b>on</b> or <b>off</b>.</p> <p>The default value is <b>off</b>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>dot1x re-authentication-interval</b> &lt;1-604800&gt;</p> <p>Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled.</p> <p>The default value is <b>3600</b>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>dot1x server-timeout</b> &lt;1-65535&gt;</p> <p>Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout.</p> <p>The default value is <b>30</b>.</p> <p>The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of <b>radius-server timeout</b> &lt;timeout-value&gt; (default is <b>3</b>).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>dot1x supplicant-timeout</b> &lt;1-65535&gt;</p> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server.</p> <p>The default value is <b>30</b>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>dot1x transmit-interval</b> &lt;1-65535&gt;</p> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame.</p> <p>The default value is <b>30</b>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] dot1x vlan-assign</b></p> <p>Sets the dynamic VLAN assignment status to <b>on</b> or <b>off</b>.</p> <p>The default value is <b>off</b>.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 224.** 802.1X Global Configuration Commands (continued)

Command Syntax and Usage
<b>default dot1x</b> Resets the global 802.1X parameters to their default values. <b>Command mode:</b> Global configuration
<b>show dot1x</b> Displays current global 802.1X parameters. <b>Command mode:</b> All

## 802.1X Guest VLAN Configuration

The 802.1X Guest VLAN commands allow you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

**Table 225.** 802.1X Guest VLAN Configuration Commands

Command Syntax and Usage
<b>[no] dot1x guest-vlan enable</b> Enables or disables the 802.1X Guest VLAN. <b>Command mode:</b> Global configuration
<b>[no] dot1x guest-vlan vlan &lt;VLAN number&gt;</b> Configures the Guest VLAN number. <b>Command mode:</b> Global configuration
<b>show dot1x</b> Displays current 802.1X parameters. <b>Command mode:</b> All

## 802.1X Port Configuration

The 802.1X port commands allows you to configure parameters that affect the selected port in the EN4093R. These settings override the global 802.1X parameters.

**Table 226.** 802.1X Port Commands

Command Syntax and Usage
<p><b>dot1x apply-global</b></p> <p>Applies current global 802.1X configuration parameters to the port.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>dot1x max-request</b> &lt;1-10&gt;</p> <p>Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client).</p> <p>The default value is 2.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>dot1x mode {force-unauthorized auto force-authorized}</b></p> <p>Sets the type of access control for the port:</p> <ul style="list-style-type: none"><li>o force-unauthorized - the port is unauthorized unconditionally.</li><li>o auto - the port is unauthorized until it is successfully authorized by the RADIUS server.</li><li>o force-authorized - the port is authorized unconditionally, allowing all traffic.</li></ul> <p>The default value is force-authorized.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>dot1x quiet-time</b> &lt;0-65535&gt;</p> <p>Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication.</p> <p>The default value is 60.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>[no] dot1x re-authenticate</b></p> <p>Sets the re-authentication status to on or off.</p> <p>The default value is off.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>dot1x re-authentication-interval</b> &lt;1-604800&gt;</p> <p>Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled.</p> <p>The default value is 3600.</p> <p><b>Command mode:</b> Interface port</p>

**Table 226.** 802.1X Port Commands (continued)

Command Syntax and Usage
<p><b>dot1x server-timeout</b> &lt;1-65535&gt;</p> <p>Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout.</p> <p>The default value is 30.</p> <p>The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of the <code>radius-server timeout</code> command.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>dot1x supplicant-timeout</b> &lt;1-65535&gt;</p> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server.</p> <p>The default value is 30.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>dot1x transmit-interval</b> &lt;1-65535&gt;</p> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame.</p> <p>The default value is 30.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>[no] dot1x vlan-assign</b></p> <p>Sets the dynamic VLAN assignment status to <code>on</code> or <code>off</code>.</p> <p>The default value is <code>off</code>.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>default dot1x</b></p> <p>Resets the 802.1X port parameters to their default values.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port</b> &lt;port alias or number&gt; <b>dot1x</b></p> <p>Displays current 802.1X port parameters.</p> <p><b>Command mode:</b> All</p>

## Spanning Tree Configuration

Lenovo Enterprise Network Operating System supports the IEEE 802.1D (2004) Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1Q (2003) Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST+). STP is used to prevent loops in the network topology.

Up to 256 Spanning Tree Groups can be configured on the switch (STG 256 is reserved for management). By default, 128 STGs are configured (STG 128 is reserved for management).

**Note:** When VRRP is used for active/active redundancy, STG must be enabled.

**Table 227.** *Spanning Tree Configuration Options*

Command Syntax and Usage
<p><b>spanning-tree mode [disable mst pvrst rstp]</b></p> <p>Selects and enables Multiple Spanning Tree mode (mst), Per VLAN Rapid Spanning Tree mode (pvrst), or Rapid Spanning Tree mode (rstp).</p> <p>The default mode is PVRST+.</p> <p>When you select <b>spanning-tree mode disable</b>, the switch globally turns Spanning Tree off. All ports are placed into forwarding state. Any BPDU's received are flooded.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] spanning-tree pvst-compatibility</b></p> <p>Enables or disables VLAN tagging of Spanning Tree BPDUs.</p> <p>The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] spanning-tree stg-auto</b></p> <p>Enables or disables VLAN Automatic STG Assignment (VASA). When <b>enabled</b>, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool.</p> <p><b>Note:</b> When using VASA, a maximum number of 127 automatically assigned STGs is supported.</p> <p><b>Note:</b> VASA applies only to PVRST mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree guard loop</b></p> <p>Enables STP loop guard. STP loop guard prevents the port from forwarding traffic if no BPDUs are received. The port is placed into a loop-inconsistent blocking state until a BPDU is received.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

**Table 227.** *Spanning Tree Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>spanning-tree guard root</b></p> <p>Enables STP root guard. STP root guard enforces the position of the root bridge. If the bridge receives a superior BPDU, the port is placed into a root-inconsistent state (listening).</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>spanning-tree guard none</b></p> <p>Disables STP loop guard and root guard.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>no spanning-tree guard</b></p> <p>Sets the Spanning Tree guard parameters to their default values.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] spanning-tree link-type {p2p shared auto}</b></p> <p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"><li>– <b>auto:</b> Configures the port to detect the link type, and automatically match its settings.</li><li>– <b>p2p:</b> Configures the port for Point-To-Point protocol.</li><li>– <b>shared:</b> Configures the port to connect to a shared medium (usually a hub).</li></ul> <p>The default link type is <b>auto</b>.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] spanning-tree portfast</b></p> <p>Enables or disables this port as portfast or edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (<b>enabled</b>).</p> <p><b>Note:</b> After you configure the port as an edge port, you must disable the port and then re-enable the port for the change to take effect.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] spanning-tree pvst-protection</b></p> <p>Enables or disables PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it is <b>error disabled</b>.</p> <p>The default setting for this feature is <b>disabled</b> (no protection).</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

**Table 227.** *Spanning Tree Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>show spanning-tree</b></p> <p>Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership.</p> <p>In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:</p> <ul style="list-style-type: none"><li>– Priority</li><li>– Hello interval</li><li>– Maximum age value</li><li>– Forwarding delay</li><li>– Aging time</li></ul> <p>You can also see the following port-specific STG information:</p> <ul style="list-style-type: none"><li>– Port alias and priority</li><li>– Cost</li><li>– State</li></ul> <p>For details, see <a href="#">page 77</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show spanning-tree blockedports</b></p> <p>Lists the ports blocked by each STP instance.</p> <p><b>Command mode:</b> All</p>
<p><b>show spanning-tree root</b></p> <p>Displays the Spanning Tree configuration on the root bridge for each STP instance. For details, see <a href="#">page 85</a>.</p> <p><b>Command mode:</b> All</p>
<p><b>show spanning-tree [vlan &lt;VLAN ID&gt;] bridge</b></p> <p>Displays Spanning Tree bridge information. For details, see <a href="#">page 84</a>.</p> <p><b>Command mode:</b> All</p>

## MSTP Configuration

Up to 32 Spanning Tree Groups can be configured in MSTP mode. MSTP is turned off by default and the default STP mode is PVRST+.

**Note:** When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 128.

**Table 228.** *Multiple Spanning Tree Configuration Options*

<b>Command Syntax and Usage</b>
<p><b>[no] spanning-tree mst &lt;MST instance or range&gt; enable</b></p> <p>Enables or disables the specified MSTP instance.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree mst forward-time &lt;4-30&gt;</b></p> <p>Configures the forward delay time in seconds. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state.</p> <p>The default value is 15.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree mst max-age &lt;6-40&gt;</b></p> <p>Configures the maximum age interval in seconds. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network.</p> <p>The default value is 20.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree mst &lt;MST instance or range&gt; priority &lt;0-65535&gt;</b></p> <p>Configures the CIST bridge priority for the specified MSTP instance. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...).</p> <p>The default value is 61440.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree mst max-hops &lt;4-60&gt;</b></p> <p>Configures the maximum number of bridge hops a packet may traverse before it is dropped.</p> <p>The default value is 20.</p> <p><b>Command mode:</b> Global configuration</p>



**Table 228.** Multiple Spanning Tree Configuration Options (continued)

<p><b>Command Syntax and Usage</b></p>
<p><b>default spanning-tree mst</b> &lt;MST instance number or range&gt; Restores the Spanning Tree instance to its default configuration. <b>Command mode:</b> Global configuration</p>
<p><b>no spanning-tree mst configuration</b> Returns the MST region to its default values: no VLAN is mapped to any MST instance. Revision number is reset to 0. <b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree mst configuration</b> Enables MSTP configuration mode. <b>Command mode:</b> Global configuration</p>
<p><b>[no] instance</b> &lt;0-32&gt; <b>vlan</b> &lt;VLAN numbers&gt; Maps or removes the specified VLANs to the Spanning Tree instance. If a VLAN does not exist, it will not be created automatically. <b>Command mode:</b> MST configuration</p>
<p><b>[no] name</b> &lt;1-32 characters&gt; Configures a name for the MSTP region. All devices within an MSTP region must have the same region name. <b>Command mode:</b> MST configuration</p>
<p><b>[no] revision</b> &lt;0-65535&gt; Configures a revision number for the MSTP region. The revision is used as a numerical identifier for the region. All devices within an MSTP region must have the same revision number. <b>Command mode:</b> MST configuration</p>
<p><b>show spanning-tree mst</b> &lt;MST instance or range&gt; <b>[information]</b> Displays the current MSTP configuration for the specified instance. <b>Command mode:</b> All</p>
<p><b>show spanning-tree mst configuration</b> Displays the current MSTP settings. <b>Command mode:</b> All</p>

## MSTP Port Configuration

MSTP port parameters are used to modify MSTP operation on an individual port basis. MSTP parameters do not affect operation of RSTP/PVRST.

**Table 229.** *MSTP Port Configuration Options*

Command Syntax and Usage
<p><b>spanning-tree mst</b> &lt;MST instance or range&gt; <b>cost</b> &lt;0-200000000&gt;</p> <p>Configures the port path cost for the specified MSTP instance. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:</p> <ul style="list-style-type: none"><li>o 1Gbps = 20000</li><li>o 10Gbps = 2000</li></ul> <p>The default value of 0 indicates that the default path cost will be computed for an auto negotiated link speed.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>[no] spanning-tree mst</b> &lt;MST instance or range&gt; <b>enable</b></p> <p>Enables or disables the specified MSTP instance on the port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>spanning-tree mst hello-time</b> &lt;1-10&gt;</p> <p>Configures the port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds.</p> <p>The default value is 2.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<p><b>spanning-tree mst</b> &lt;MST instance or range&gt; <b>port-priority</b> &lt;0-240&gt;</p> <p>Configures the port priority for the specified MSTP instance. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.</p> <p>The range is 0 to 240, in steps of 16 (0, 16, 32...).</p> <p>The default value is 128.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

**Table 229.** *MSTP Port Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>[no] spanning-tree pvst-protection</b></p> <p>Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it error disabled. PVST Protection works only in MSTP mode.</p> <p>The default setting is disabled.</p> <p><b>Note:</b> Not available in stacking.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port &lt;port alias or number&gt; spanning-tree mstp cist</b></p> <p>Displays the current CIST port configuration.</p> <p><b>Command mode:</b> All</p>

## RSTP/PVRST Configuration

Table 230 describes the commands used to configure the Rapid Spanning Tree (RSTP) and Per VLAN Rapid Spanning Tree Protocol (PVRST+) protocols.

**Table 230.** *RSTP/PVRST Configuration Options*

<b>Command Syntax and Usage</b>
<p><b>boot spanning-tree max-instances {128 256}</b></p> <p>Configures the maximum number of Spanning Tree Groups (STGs) that can be used on the switch.</p> <p>The default value is 128.</p> <p><b>Note:</b> The switch needs to be reloaded for the configuration to take effect.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no boot spanning-tree max-instances</b></p> <p>Reset the maximum number of STGs available on the switch to the default value of 128.</p> <p><b>Note:</b> The switch needs to be reloaded for the configuration to take effect.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] spanning-tree stp &lt;STP instance or range&gt; enable</b></p> <p>Enables or disables Spanning Tree instance.</p> <p>The default settings is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree stp &lt;STP instance or range&gt; vlan &lt;VLAN number&gt;</b></p> <p>Associates a VLAN with a Spanning Tree Group and requires a VLAN ID as a parameter. If the VLAN does not exist, it will be created automatically, but it will be disabled by default.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 230.** RSTP/PVRST Configuration Options (continued)

<b>Command Syntax and Usage</b>
<p><b>no spanning-tree stp</b> &lt;STP instance or range&gt; <b>vlan</b> &lt;VLAN number&gt;</p> <p>Breaks the association between a VLAN and a Spanning Tree Group and requires a VLAN ID as a parameter.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no spanning-tree stp</b> &lt;STP instance or range&gt; <b>vlan all</b></p> <p>Removes all VLANs from a Spanning Tree Group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>default spanning-tree stp</b> &lt;STP instance or range&gt;</p> <p>Restores a Spanning Tree instance to its default configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show spanning-tree stp</b> &lt;STP instance or range&gt; <b>[information]</b></p> <p>Displays current Spanning Tree Protocol parameters for the specified Spanning Tree Group. See <a href="#">page 82</a> for details about the <code>information</code> parameter.</p> <p><b>Command mode:</b> All</p>

## Bridge RSTP/PVRST Configuration

Spanning Tree bridge parameters affect the global STG operation of the switch. STG bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay

**Table 231.** *Bridge Spanning Tree Configuration Options*

Command Syntax and Usage
<p><b>spanning-tree stp</b> &lt;STP instance or range&gt; <b>bridge forward-delay</b> &lt;4-30&gt;</p> <p>Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds.</p> <p>The default value is 15.</p> <p><b>Note:</b> This command does not apply to MSTP.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree stp</b> &lt;STP instance or range&gt; <b>bridge hello-time</b> &lt;1-10&gt;</p> <p>Configures the bridge Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds.</p> <p>The default value is 2.</p> <p><b>Note:</b> This command does not apply to MSTP.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>spanning-tree stp</b> &lt;STP instance or range&gt; <b>bridge maximum-age</b> &lt;6-40&gt;</p> <p>Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds.</p> <p>The default value is 20.</p> <p><b>Note:</b> This command does not apply to MSTP.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 231.** Bridge Spanning Tree Configuration Options

Command Syntax and Usage
<p><b>spanning-tree stp</b> &lt;STP instance or range&gt; <b>bridge priority</b> &lt;0-65535&gt;</p> <p>Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...).</p> <p>The default value is 61440.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show spanning-tree</b> [vlan &lt;VLAN ID&gt;] <b>bridge</b></p> <p>Displays the current Spanning Tree parameters either globally or for a specific VLAN. See <a href="#">page 84</a> for sample output.</p> <p><b>Command mode:</b> All</p>

When configuring STG bridge parameters, the following formulas must be used:

- $2*(fwd-1) \geq mxage$
- $2*(hello+1) \leq mxage$

## RSTP/PVRST Port Configuration

By default, Spanning Tree is turned off for management ports, and turned on for data ports. STG port parameters include:

- Port priority
- Port path cost

**Table 232.** Spanning Tree Port Options

Command Syntax and Usage
<p><b>[no] spanning-tree stp</b> &lt;STP instance or range&gt; <b>enable</b></p> <p>Enables or disables STG on the port.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>spanning-tree stp link-type</b> {auto p2p shared}</p> <p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"><li>o <b>auto:</b> Configures the port to detect the link type, and automatically match its settings.</li><li>o <b>p2p:</b> Configures the port for Point-To-Point protocol.</li><li>o <b>shared:</b> Configures the port to connect to a shared medium (usually a hub).</li></ul> <p><b>Command mode:</b> Interface port</p>

**Table 232.** *Spanning Tree Port Options (continued)*

Command Syntax and Usage
<p><b>spanning-tree stp</b> &lt;STP instance or range&gt; <b>path-cost</b> &lt;1-200000000, 0 for default&gt;</p> <p>Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:</p> <ul style="list-style-type: none"> <li>o 1Gbps = 20000</li> <li>o 10Gbps = 2000</li> </ul> <p>The default value of 0 indicates that the default path cost will be computed for an auto negotiated link speed.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>spanning-tree stp</b> &lt;STP instance or range&gt; <b>priority</b> &lt;0-240&gt;</p> <p>Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...).</p> <p>The default value is 128.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>show interface port</b> &lt;port alias or number&gt; <b>spanning-tree stp</b> &lt;STP instance or range&gt;</p> <p>Displays the current STG port parameters.</p> <p><b>Command mode:</b> All</p>

## Forwarding Database Configuration

Use the following commands to configure the Forwarding Database (FDB).

**Table 233.** *FDB Configuration Commands*

Command Syntax and Usage
<p><b>mac-address-table aging</b> &lt;0-65535&gt;</p> <p>Configures the aging value for FDB entries, in seconds.</p> <p>The default value is 300.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 233.** *FDB Configuration Commands*

<b>Command Syntax and Usage</b>
<b>[no] mac-address-table mac-notification</b> Enables or disables MAC Address Notification. With MAC Address Notification <b>enabled</b> , the switch generates a syslog message when a MAC address is added or removed from the MAC address table. <b>Note:</b> This is applicable for internal ports only. <b>Command mode:</b> Global configuration
<b>show mac-address-table</b> Display current FDB configuration. <b>Command mode:</b> All



## Static Multicast MAC Configuration

The following options are available to control the forwarding of known and unknown multicast packets:

- All multicast packets are flooded to the entire VLAN. This is the default switch behavior.
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are flooded to the entire VLAN. To configure this option, define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (**mac-address-table multicast**).
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are dropped. To configure this option:
  - Define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (**mac-address-table multicast**).
  - Enable Flood Blocking on ports that are not to receive multicast packets (**interface port x**) (**flood-blocking**).

Use the following commands to configure static Multicast MAC entries in the Forwarding Database (FDB).

**Table 234.** *Static Multicast MAC Configuration Commands*

Command Syntax and Usage
<p><b>[no] mac-address-table multicast</b> &lt;MAC address&gt; &lt;VLAN number&gt; &lt;port alias or number&gt;</p> <p>Adds or deletes a permanent multicast FDB entry. You can list ports separated by a space, or enter a range of ports separated by a hyphen (-). For example:</p> <pre>mac-address-table multicast 01:00:00:23:3f:01 200 int1-int4</pre> <p><b>Command mode:</b> Global configuration</p>
<p><b>no mac-address-table multicast all</b></p> <p>Deletes all permanent multicast FDB entries.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>mac-address-table multicast reload</b></p> <p>Reloads all permanent multicast FDB entries.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show mac-address-table multicast</b></p> <p>Display the current permanent multicast FDB entries.</p> <p><b>Command mode:</b> All</p>

## Static FDB Configuration

Use the following commands to configure static entries in the Forwarding Database (FDB).

**Table 235.** FDB Configuration Commands

Command Syntax and Usage
<p><b>mac-address-table static</b> &lt;MAC address&gt; <b>vlan</b> &lt;VLAN number&gt; <b>{port</b> &lt;port alias or number&gt; <b> portchannel</b> &lt;LAG number&gt; <b> adminkey</b> &lt;1-65535&gt;}</p> <p>Adds a permanent FDB entry. Enter the MAC address using the following format, xx:xx:xx:xx:xx:xx.</p> <p>For example, 08:00:20:12:34:56.</p> <p>You can also enter the MAC address as follows: xxxxxxxxxxxx.</p> <p>For example, 080020123456.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no mac-address-table static</b> &lt;MAC address&gt; &lt;VLAN number&gt;</p> <p>Deletes a permanent FDB entry.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show mac-address-table</b></p> <p>Display current FDB configuration.</p> <p><b>Command mode:</b> All</p>

## LLDP Configuration

Use the following commands to configure Link Layer Detection Protocol (LLDP).

**Table 236.** *LLDP Configuration Commands*

Command Syntax and Usage
<p><b>[no] lldp enable</b>            Globally enables or disables LLDP.            The default setting is enabled.  <b>Command mode:</b> Global configuration</p>
<p><b>lldp holdtime-multiplier &lt;2-10&gt;</b>            Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval.            The default value is 4.  <b>Command mode:</b> Global configuration</p>
<p><b>no lldp holdtime-multiplier</b>            Sets the message hold time multiplier to its default value of 4.  <b>Command mode:</b> Global configuration</p>
<p><b>lldp refresh-interval &lt;5-32768&gt;</b>            Configures the message transmission interval, in seconds.            The default value is 30.  <b>Command mode:</b> Global configuration</p>
<p><b>no lldp refresh-interval</b>            Sets the message transmission interval to its default value of 30 seconds.  <b>Command mode:</b> Global configuration</p>
<p><b>lldp reinit-delay &lt;1-10&gt;</b>            Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages.            The default value is 2.  <b>Command mode:</b> Global configuration</p>
<p><b>no lldp reinit-delay</b>            Sets the re-initialization delay interval to its default value of 2 seconds.  <b>Command mode:</b> Global configuration</p>
<p><b>lldp transmission-delay &lt;1-8192&gt;</b>            Configures the transmission delay interval, in seconds. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port.            The default value is 2.  <b>Command mode:</b> Global configuration</p>

**Table 236.** *LLDP Configuration Commands*

<b>Command Syntax and Usage</b>
<b>no lldp transmission-delay</b> Sets the transmission delay interval to its default value of 2 seconds. <b>Command mode:</b> Global configuration
<b>lldp trap-notification-interval</b> <1-3600> Configures the trap notification interval, in seconds. The default value is 5. <b>Command mode:</b> Global configuration
<b>no lldp trap-notification-interval</b> Sets the trap notification interval to its default value of 5 seconds. <b>Command mode:</b> Global configuration
<b>show lldp</b> Display current LLDP configuration. <b>Command mode:</b> All

## *LLDP Port Configuration*

Use the following commands to configure LLDP port options.

**Table 237.** *LLDP Port Commands*

<b>Command Syntax and Usage</b>
<b>lldp admin-status {tx_only rx_only tx_rx}</b> Configures the LLDP transmission type for the port, as follows: <ul style="list-style-type: none"><li>o Transmit only</li><li>o Receive only</li><li>o Transmit and receive</li></ul> The default setting is tx_rx. <b>Command mode:</b> Interface port
<b>no lldp admin-status</b> Disables LLDP transmission for the port. <b>Command mode:</b> Interface port
<b>[no] lldp trap-notification</b> Enables or disables SNMP trap notification for LLDP messages. <b>Command mode:</b> Interface port
<b>show interface port</b> <port alias or number> <b>lldp</b> Display current LLDP port configuration. <b>Command mode:</b> All

## LLDP Optional TLV configuration

Use the following commands to configure LLDP port TLV (Type, Length, Value) options for the selected port.

**Table 238.** *Optional TLV Commands*

Command Syntax and Usage
<b>[no] lldp tlv all</b> Enables or disables all optional TLV information types. <b>Command mode:</b> Interface port
<b>[no] lldp tlv dcbx</b> Enables or disables the Data Center Bridging Capability Exchange (DCBX) information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv framesz</b> Enables or disables the Maximum Frame Size information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv linkaggr</b> Enables or disables the Link Aggregation information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv macphy</b> Enables or disables the MAC/Phy Configuration information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv mgmtaddr</b> Enables or disables the Management Address information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv portdesc</b> Enables or disables the Port Description information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv portprot</b> Enables or disables the Port and VLAN Protocol ID information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv portvid</b> Enables or disables the Port VLAN ID information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv powermdi</b> Enables or disables the Power via MDI information type. <b>Command mode:</b> Interface port

**Table 238.** *Optional TLV Commands (continued)*

<b>Command Syntax and Usage</b>
<b>[no] lldp tlv protid</b> Enables or disables the Protocol ID information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv syscap</b> Enables or disables the System Capabilities information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv sysdescr</b> Enables or disables the System Description information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv sysname</b> Enables or disables the System Name information type. <b>Command mode:</b> Interface port
<b>[no] lldp tlv vlanname</b> Enables or disables the VLAN Name information type. <b>Command mode:</b> Interface port
<b>show interface port &lt;port alias or number&gt; lldp</b> Display current LLDP port configuration. <b>Command mode:</b> All

## Link Aggregation Group (LAG) Configuration

Link Aggregation Groups (LAGs) can provide super-bandwidth connections between EN4093R or other aggregation capable devices. A LAG is a group of ports that act together, combining their bandwidth to create a single, larger port. Two types of aggregation are available: static LAGs (portchannels) and dynamic LACP LAGs (portchannels).

The two types of aggregation can be configured using the following portchannel ranges:

- static LAGs: 1-64
- LACP LAGs: 65-128

Up to 52 static LAGs can be configured on the EN4093R, with the following restrictions:

- Any physical switch port can belong to no more than one LAG.
- Up to 24 ports can belong to the same LAG.
- Configure all ports in a LAG with the same properties (speed, duplex, flow control, STG, VLAN and so on).
- Aggregation from non-Lenovo devices must comply with Cisco® EtherChannel® technology and exclude the PAgP networking protocol.

By default, each LAG is empty and disabled.

**Table 239.** LAG Configuration Commands

Command Syntax and Usage
<p><b>portchannel</b> &lt;1-52&gt; <b>port</b> &lt;port alias or number&gt; [<b>enable</b>]</p> <p>Adds a physical port or ports to the current LAG. You can add several ports, with each port separated by a comma ( , ) or a range of ports, separated by a dash ( - ). The <b>enable</b> option also enables the LAG.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no portchannel</b> &lt;1-52&gt; <b>port</b> &lt;port alias or number&gt;</p> <p>Removes a physical port or ports from the current LAG.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] portchannel</b> &lt;1-52&gt; <b>enable</b></p> <p>Enables or disables the current LAG.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no portchannel</b> &lt;1-52&gt;</p> <p>Removes the current LAG configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show portchannel</b> &lt;1-52&gt;</p> <p>Displays current LAG parameters.</p> <p><b>Command mode:</b> All</p>

## Link Aggregation Group (LAG) Hash Configuration

Use the following commands to configure Link Aggregation Group (LAG) hash settings for the EN4093R. LAG hash parameters are set globally for the EN4093R. The LAG hash settings affect both static LAGs and LACP LAGs.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in [Table 240](#) combined with the hash parameters listed in [Table 242](#).

**Table 240.** *LAG Hash Settings*

Command Syntax and Usage
<b>[no] portchannel thash ingress</b> Enables or disables use of the ingress port to compute the LAG hash value. The default setting is <code>disabled</code> . <b>Command mode:</b> Global configuration
<b>[no] portchannel thash L4port</b> Enables or disables use of Layer 4 service ports (TCP, UDP, etc.) to compute the hash value. The default setting is <code>disabled</code> . <b>Command mode:</b> Global configuration
<b>show portchannel hash</b> Display current LAG hash configuration. <b>Command mode:</b> All



## FCoE LAG Hash Configuration

Use the following commands to configure FCoE LAG Hash parameters for the EN4093R.

**Table 241.** FCoE LAG Hash Configuration Commands

Command Syntax and Usage
<b>[no] portchannel thash fcoe cntag-id</b> Enables or disables FCoE LAG hashing on the cntag id. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash fcoe destination-id</b> Enables or disables FCoE LAG hashing on the destination id. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash fcoe fabric-id</b> Enables or disables FCoE LAG hashing on the fabric id. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash fcoe originator-id</b> Enables or disables FCoE LAG hashing on the originator id. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash fcoe responder-id</b> Enables or disables FCoE LAG hashing on the responder id. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash fcoe source-id</b> Enables or disables FCoE LAG hashing on the source id. <b>Command mode:</b> Global configuration
<b>show portchannel hash</b> Display current LAG hash configuration. <b>Command mode:</b> All

## Layer 2 LAG Hash

Layer 2 LAG hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SMAC and DMAC

Use the following commands to configure Layer 2 LAG hash parameters for the switch.

**Table 242.** *Layer 2 LAG Hash Options*

Command Syntax and Usage
<b>[no] portchannel thash l2hash l2-destination-mac-address</b> Enables or disables Layer 2 LAG hashing on the destination MAC. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash l2hash l2-source-mac-address</b> Enables or disables Layer 2 LAG hashing on the source MAC. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash l2hash l2-source-destination-mac</b> Enables or disables Layer 2 LAG hashing on both the source and destination MAC. <b>Command mode:</b> Global configuration
<b>show portchannel hash</b> Displays the current LAG hash settings. <b>Command mode:</b> All

## Layer 3 LAG Hash

Layer 3 LAG hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SIP (source IP only)
- DIP (destination IP only)
- SIP and DIP

Use the following commands to configure Layer 3 LAG hash parameters for the switch.

**Table 243.** *Layer 3 LAG Hash Options*

Command Syntax and Usage
<b>[no] portchannel thash l3thash l3-destination-ip-address</b> Enables or disables Layer 3 LAG hashing on the destination IP address. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash l3thash l3-source-ip-address</b> Enables or disables Layer 3 LAG hashing on the source IP address. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash l3thash l3-source-destination-ip</b> Enables or disables Layer 3 LAG hashing on both the source and the destination IP address. <b>Command mode:</b> Global configuration
<b>[no] portchannel thash l3thash l3-use-l2-hash</b> Enables or disables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared. <b>Command mode:</b> Global configuration
<b>show portchannel hash</b> Displays the current LAG hash settings. <b>Command mode:</b> All

## Virtual Link Aggregation Control Protocol Configuration

Use the following commands to configure Virtual Link Aggregation Control Protocol (vLAG) for the EN4093R.

**Table 244.** *Virtual Link Aggregation Control Protocol Commands*

Command Syntax and Usage
<p><b>[no] vlag enable</b></p> <p>Enables or disables vLAG globally.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] vlag adminkey &lt;1-65535&gt; enable</b></p> <p>Enables or disables vLAG on the selected LACP <i>admin key</i>. LACP LAGs formed with this <i>admin key</i> will be included in the vLAG configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>vlag auto-recovery &lt;240-3600&gt;</b></p> <p>Sets the duration in seconds of the auto-recovery timer. This timer configures how long after boot-up configuration load, the switch can assume the Primary role from an unresponsive ISL peer and bring up the vLAG ports.</p> <p>The default value is 300.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no vlag auto-recovery</b></p> <p>Sets the auto-recovery timer to the default 300 seconds duration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] vlag peer-gateway</b></p> <p>Enables or disables the forwarding of packets intended for the switch's vLAG peer. If a packet is received by the switch, but has the MAC address of its vLAG peer, it will be locally forwarded without crossing the vLAG inter-switch link (ISL), thus avoiding the loss of traffic.</p> <p>If the vLAG peer gateway is disabled, packets addressed to the vLAG peer are sent across the ISL and then dropped by the vLAG peer.</p> <p>The default settings is disabled.</p> <p><b>Note:</b> The vLAG peer gateway must be configured on both vLAG peers.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] vlag portchannel &lt;1-64&gt; enable</b></p> <p>Enables or disables the vLAG underlying LAG.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>vlag priority &lt;0-65535&gt;</b></p> <p>Configures the vLAG priority for the switch, used for election of Primary and Secondary vLAG switches. The switch with lower priority is elected to the role of Primary vLAG switch.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 244.** *Virtual Link Aggregation Control Protocol Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>vlag startup-delay</b> &lt;0-3600&gt;</p> <p>Sets the vLAG startup-delay value in seconds to the specified value. The default is 120 seconds.</p> <p><b>Note:</b> Startup delay gives vLAG the ability to prevent traffic loss after a reboot. When a vLAG switch reboots, the vLAG ports are in an errdisabled state. After ISL is up, the vLAG ports are started one by one after the specified startup delay time. This specified time allows the switch to get BGP/OSFP ready through the uplinks so when the vLAG port starts up, all the traffic through those links flows smoothly. Admin status of the ports is honored by the vlag startup delay. For example, if the admin status of the vLAG port is down, those ports will be kept down even after the vLAG start-up delay.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no vlag startup-delay</b></p> <p>Sets the vLAG startup-delay to the default 120 seconds duration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] vlag tier-id</b> &lt;1-512&gt;</p> <p>Sets the vLAG peer ID.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] vlag vrrp active</b></p> <p>Enables or disables vLAG VRRP active mode.</p> <p><b>Note:</b> If active mode is disabled, the switch will be in passive mode. In active mode, Layer 3 traffic is forwarded in all vLAG related VRRP domains. In passive mode, Layer 3 traffic is forwarded in a vLAG related VRRP domain only if either the switch or its peer virtual router is the VRRP master.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show vlag</b></p> <p>Display current vLAG configuration.</p> <p><b>Command mode:</b> All</p>

## vLAG Health Check Configuration

These commands allow you to configure a health check of synchronization between vLAG peers.

**Table 245.** vLAG Health Check Configuration Options

Command Syntax and Usage
<b>[no] vlag hlthchk connect-retry-interval</b> <1-300> Sets in seconds the vLAG health check connect retry interval, in seconds. The default value is 30. <b>Command mode:</b> Global configuration
<b>[no] vlag hlthchk keepalive-attempts</b> <1-24> Sets the number of vLAG keep alive attempts. The default value is 3. <b>Command mode:</b> Global configuration
<b>[no] vlag hlthchk keepalive-interval</b> <2-300> Sets the time between vLAG keep alive attempts, in seconds. The default value is 5. <b>Command mode:</b> Global configuration
<b>vlag hlthchk peer-ip</b> {<IP address> <IPv6 address>} Configures the IP address of the vLAG peer. <b>Command mode:</b> Global configuration

## vLAG ISL Configuration

These commands allow you to configure a dedicated inter-switch link (ISL) for synchronization between vLAG peers.

**Table 246.** vLAG ISL Configuration Options

Command Syntax and Usage
<b>[no] vlag isl adminkey</b> <1-65535> Enables or disables vLAG Inter-Switch Link (ISL) on the selected LACP <i>admin key</i> . LACP LAGs formed with this <i>admin key</i> will be included in the ISL. <b>Command mode:</b> Global configuration
<b>[no] vlag isl portchannel</b> <1-64> Enables or disables vLAG Inter-Switch Link (ISL) on the selected LAG. <b>Command mode:</b> Global configuration
<b>show vlag information</b> Displays current vLAG parameters. <b>Command mode:</b> All

## Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the EN4093R.

**Table 247.** *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
<p><b>lacp system-priority</b> &lt;1-65535&gt;</p> <p>Defines the priority value for the EN4093R. Lower numbers provide higher priority.</p> <p>The default value is 32768.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>lacp timeout {short long}</b></p> <p>Defines the timeout period before invalidating LACP data from a remote partner. Choose <b>short</b> (3 seconds) or <b>long</b> (90 seconds).</p> <p>The default value is <b>long</b>.</p> <p><b>Note:</b> It is recommended that you use a timeout value of <b>long</b>, to reduce LACPDU processing. If your EN4093R's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static LAGs instead of LACP.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>default lacp [system-priority timeout]</b></p> <p>Restores either the VFSM priority value, timeout period or both to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no lacp</b> &lt;1-65535&gt;</p> <p>Deletes a selected LACP LAG, based on its <i>admin key</i>. This command is equivalent to disabling LACP on each of the ports configured with the same <i>admin key</i>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>portchannel</b> &lt;LAG ID (65-128)&gt; <b>lacp key</b> &lt;1-65535&gt;</p> <p>Enables a static LACP LAG. In this mode, ports sharing the same LACP admin key can form a single LAG, with the specified LAG ID. The active LAG is picked based on the ports which occupy first the LAG ID. Member ports that cannot join this LAG are prohibited from forming secondary LACP groups. Instead, they are set in a suspend state where they discard all non-LACP traffic.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 247.** *Link Aggregation Control Protocol Commands*

<b>Command Syntax and Usage</b>
<b>no portchannel</b> <LAG ID (65-128)> Deletes the specified static LACP LAG. <b>Command mode:</b> Global configuration
<b>show lacp</b> Display current LACP configuration. <b>Command mode:</b> All

## LACP Port Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

**Table 248.** *Link Aggregation Control Protocol Commands*

<b>Command Syntax and Usage</b>
<b>lacp key</b> <1-65535> Set the admin key for this port. Only ports with the same <i>admin key</i> and <i>oper key</i> (operational state generated internally) can form a LACP LAG. <b>Command mode:</b> Interface port
<b>lacp mode {off active passive}</b> Set the LACP mode for this port, as follows: <ul style="list-style-type: none"><li>o <b>off</b> turns LACP off for this port. You can use this port to manually configure a static LAG.</li><li>o <b>active</b> turns LACP on and set this port to active. Active ports initiate LACPDU s.</li><li>o <b>passive</b> turns LACP on and set this port to passive. Passive ports do not initiate LACPDU s, but respond to LACPDU s from active ports.</li></ul> The default value is <b>off</b> . <b>Command mode:</b> Interface port
<b>lacp priority</b> <1-65535> Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768. <b>Command mode:</b> Interface port
<b>lacp suspend-individual</b> Sets the port in LACP suspended state if it does not receive LACPDU s anymore. <b>Note:</b> The default value is <b>individual</b> for internal switch ports and <b>suspend-individual</b> for external switch ports. <b>Command mode:</b> Interface port/Interface portchannel



**Table 248.** *Link Aggregation Control Protocol Commands*

<b>Command Syntax and Usage</b>
<b>no lacp suspend-individual</b> Sets the port in LACP individual state if it does not receive LACPDUs anymore. <b>Command mode:</b> Interface port/Interface portchannel
<b>port-channel min-links &lt;1-32&gt;</b> Set the minimum number of links for the LACP LAG to which this port belongs. If the specified minimum number of ports are not available, the LAG is placed in the down state. <b>Command mode:</b> Interface port
<b>default lacp [key mode priority suspend-individual]</b> Restores the selected parameters to their default values. <b>Command mode:</b> Interface port/Interface portchannel
<b>show interface port &lt;port alias or number&gt; lacp</b> Displays the current LACP configuration for this port. <b>Command mode:</b> All

## Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the *Enterprise NOS Application Guide*.

**Table 249.** *Layer 2 Failover Configuration Commands*

Command Syntax and Usage
<p><b>[no] failover enable</b></p> <p>Globally enables or disables Layer 2 Failover.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] failover vlan</b></p> <p>Globally turns VLAN monitor on or off.</p> <p>When the VLAN Monitor is on, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger.</p> <p>When the VLAN Monitor is off, the switch automatically disables all of the internal ports.</p> <p>The default value is off.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show failover trigger [information]</b></p> <p>Displays current Layer 2 Failover parameters.</p> <p><b>Command mode:</b> All</p>

## Failover Trigger Configuration

The following table displays Failover Trigger configuration commands.

**Table 250.** *Failover Trigger Configuration Commands*

Command Syntax and Usage
<b>[no] failover trigger &lt;1-8&gt; enable</b> Enables or disables the Failover trigger. <b>Command mode:</b> Global configuration
<b>no failover trigger &lt;1-8&gt;</b> Deletes the Failover trigger. <b>Command mode:</b> Global configuration
<b>failover trigger &lt;1-8&gt; limit &lt;0-1024&gt;</b> Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational. <b>Command mode:</b> Global configuration
<b>show failover trigger &lt;1-8&gt;</b> Displays the current failover trigger settings. <b>Command mode:</b> All

## Auto Monitor Configuration

The following table displays Auto Monitor configuration commands.

**Table 251.** *Auto Monitor Configuration Commands*

Command Syntax and Usage
<b>[no] failover trigger &lt;1-8&gt; amon adminkey &lt;1-65535&gt;</b> Adds or removes an LACP <i>admin key</i> to the Auto Monitor. LACP LAGs formed with this <i>admin key</i> will be included in the Auto Monitor. <b>Command mode:</b> Global configuration
<b>[no] failover trigger &lt;1-8&gt; amon portchannel &lt;LAG number&gt;</b> Adds or removes a LAG to the Auto Monitor. <b>Command mode:</b> Global configuration

## Failover Manual Monitor Port Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor Port configuration accepts only external uplink ports.

**Note:** AMON and MMON configurations are mutually exclusive.

**Table 252.** *Failover Manual Monitor Port Commands*

Command Syntax and Usage
<p><b>[no] failover trigger &lt;1-8&gt; mmon monitor adminkey &lt;1-65535&gt;</b></p> <p>Adds or removes an LACP <i>admin key</i> to the Manual Monitor Port configuration. LACP LAGs formed with this <i>admin key</i> will be included in the Manual Monitor Port configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] failover trigger &lt;1-8&gt; mmon monitor member &lt;port alias or number&gt;</b></p> <p>Adds or removes the selected port to the Manual Monitor Port configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] failover trigger &lt;1-8&gt; mmon monitor portchannel &lt;LAG number&gt;</b></p> <p>Adds or removes the selected LAG to the Manual Monitor Port configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show failover trigger &lt;1-8&gt;</b></p> <p>Displays the current Failover settings.</p> <p><b>Command mode:</b> All</p>

## Failover Manual Monitor Control Configuration

Use these commands to define the port link(s) to control. The Manual Monitor Control configuration accepts internal and external ports, but not management ports.

**Table 253.** *Failover Manual Monitor Control Commands*

Command Syntax and Usage
<p><b>[no] failover trigger &lt;1-8&gt; mmon control adminkey &lt;1-65535&gt;</b></p> <p>Adds or removes an LACP <i>admin key</i> to the Manual Monitor Control configuration. LACP LAGs formed with this <i>admin key</i> will be included in the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] failover trigger &lt;1-8&gt; mmon control member &lt;port alias or number&gt;</b></p> <p>Adds or removes the selected port to the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] failover trigger &lt;1-8&gt; mmon control portchannel &lt;LAG number&gt;</b></p> <p>Adds or removes the selected LAG to the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] failover trigger &lt;1-8&gt; mmon control vmember &lt;UFP vport&gt;</b></p> <p>Adds or removes the specified Unified Fabric Port virtual port to the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show failover trigger &lt;1-8&gt;</b></p> <p>Displays the current Failover settings.</p> <p><b>Command mode:</b> All</p>

## Hot Links Configuration

Use these commands to configure Hot Links. For more information about Hot Links, see “Hot Links” in the *Enterprise NOS 8.4 Application Guide*.

**Table 254.** *Hot Links Configuration Commands*

Command Syntax and Usage
<p><b>[no] hotlinks bpdu</b></p> <p>Enables or disables flooding of Spanning-Tree BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned Off. This feature can prevent unintentional loop scenarios (for example, if two uplinks come up at the same time).</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] hotlinks enable</b></p> <p>Globally enables or disables Hot Links.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] hotlinks fdb-update</b></p> <p>Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.</p> <p>The default value is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>hotlinks fdb-update-rate</b> &lt;10-1000&gt;</p> <p>Configures the FDB Update rate, in packets per second.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show hotlinks</b></p> <p>Displays current Hot Links parameters.</p> <p><b>Command mode:</b> All</p>

## Hot Links Trigger Configuration

The following table displays Hot Links Trigger configuration commands.

**Table 255.** Hot Links Trigger Configuration Commands

Command Syntax and Usage
<b>[no] hotlinks trigger &lt;1-200&gt; enable</b> Enables or disables the Hot Links trigger. <b>Command mode:</b> Global configuration
<b>hotlinks trigger &lt;1-200&gt; forward-delay &lt;0-3600&gt;</b> Configures the Forward Delay interval, in seconds. The default value is 1. <b>Command mode:</b> Global configuration
<b>[no] hotlinks trigger &lt;1-200&gt; name &lt;1-32 characters&gt;</b> Defines a name for the Hot Links trigger. <b>Command mode:</b> Global configuration
<b>[no] hotlinks trigger &lt;1-200&gt; preemption</b> Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is enabled. <b>Command mode:</b> Global configuration
<b>no hotlinks trigger &lt;1-200&gt;</b> Deletes the Hot Links trigger. <b>Command mode:</b> Global configuration
<b>show hotlinks trigger &lt;1-200&gt;</b> Displays the current Hot Links trigger settings. <b>Command mode:</b> All

## Hot Links Master Configuration

Use the following commands to configure the Hot Links Master interface.

**Table 256.** Hot Links Master Configuration Commands

Command Syntax and Usage
<p><b>[no] hotlinks trigger</b> &lt;1-200&gt; <b>master adminkey</b> &lt;0-65535&gt;</p> <p>Adds or removes an LACP <i>admin key</i> to the Master interface. LACP LAGs formed with this <i>admin key</i> will be included in the Master interface.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] hotlinks trigger</b> &lt;1-200&gt; <b>master port</b> &lt;port alias or number&gt;</p> <p>Adds or removes the selected port to the Hot Links Master interface.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] hotlinks trigger</b> &lt;1-200&gt; <b>master portchannel</b> &lt;LAG number&gt;</p> <p>Adds or removes the selected LAG to the Master interface.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show hotlinks trigger</b> &lt;1-200&gt;</p> <p>Displays the current Hot Links trigger settings.</p> <p><b>Command mode:</b> All</p>



## Hot Links Backup Configuration

Use the following commands to configure the Hot Links Backup interface.

**Table 257.** Hot Links Backup Configuration Commands

Command Syntax and Usage
<p><b>[no] hotlinks trigger &lt;1-200&gt; backup adminkey &lt;0-65535&gt;</b> Adds or removes an LACP <i>admin key</i> to the Backup interface. LACP LAGs formed with this <i>admin key</i> will be included in the Backup interface. <b>Command mode:</b> Global configuration</p>
<p><b>[no] hotlinks trigger &lt;1-200&gt; backup port &lt;port alias or number&gt;</b> Adds or removes the selected port to the Hot Links Backup interface. <b>Command mode:</b> Global configuration</p>
<p><b>[no] hotlinks trigger &lt;1-200&gt; backup portchannel &lt;LAG number&gt;</b> Adds or removes the selected LAG to the Backup interface. <b>Command mode:</b> Global configuration</p>
<p><b>show hotlinks trigger &lt;1-200&gt;</b> Displays the current Hot Links trigger settings. <b>Command mode:</b> All</p>

## VLAN Configuration

These commands configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

Up to 4094 VLANs can be configured on the EN4093R. VLANs can be assigned any number between 1 and 4094, except the reserved VLANs.

**Table 258.** *VLAN Configuration Commands*

<p><b>Command Syntax and Usage</b></p>
<p><b>vlan</b> &lt;VLAN number&gt;</p> <p>Enter VLAN configuration mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cpu</b></p> <p>Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:</p> <ul style="list-style-type: none"> <li>o If no Mrouter is present, drop subsequent packets with same IPMC.</li> <li>o If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN.</li> </ul> <p>The default setting is <b>enabled</b>.</p> <p><b>Note:</b> If both <b>flood</b> and <b>cpu</b> are disabled, then the switch drops all unregistered IPMC traffic.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] flood</b></p> <p>Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is <b>enabled</b>.</p> <p><b>Note:</b> If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must enable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group.</p> <p><b>Note:</b> If both <b>flood</b> and <b>cpu</b> are disabled, then the switch drops all unregistered IPMC traffic.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] management</b></p> <p>Configures this VLAN as a management VLAN. You must have at least one internal port in each new management VLAN. Management port (MGT1) is automatically added to management VLAN.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>name</b> &lt;1-32 characters&gt;</p> <p>Assigns a name to the VLAN or changes the existing name.</p> <p>The default VLAN name is the first one.</p> <p><b>Command mode:</b> VLAN</p>

**Table 258.** *VLAN Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>no name</b></p> <p>Resets the VLAN name to its default value.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] optflood</b></p> <p>Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>protocol-vlan &lt;1-8&gt;</b></p> <p>Configures the Protocol-based VLAN (PVLAN).</p> <p><b>Command mode:</b> VLAN</p>
<p><b>shutdown</b></p> <p>Disables local traffic on the specified VLAN.</p> <p>Default setting is enabled (no shutdown).</p> <p><b>Command mode:</b> VLAN</p>
<p><b>no shutdown</b></p> <p>Enables local traffic on the specified VLAN.</p> <p>Default setting is enabled (no shutdown).</p> <p><b>Command mode:</b> VLAN</p>
<p><b>stg &lt;STG number&gt;</b></p> <p>Assigns a VLAN to a Spanning Tree Group.</p> <p><b>Note:</b> For MST, no VLAN assignment is required. VLANs are mapped from CIST.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] vmap &lt;1-128&gt; [extports intports]</b></p> <p>Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VLAN.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>show vlan information</b></p> <p>Displays the current VLAN configuration.</p> <p><b>Command mode:</b> All</p>

**Note:** All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot add a port to more than one VLAN unless the port has VLAN tagging turned **on**.

## Protocol-Based VLAN Configuration

Use the following commands to configure Protocol-based VLAN for the selected VLAN.

**Table 259.** Protocol VLAN Configuration Commands

Command Syntax and Usage
<p><b>[no] protocol-vlan &lt;1-8&gt; enable</b>            Enables or disables the selected protocol on the VLAN.  <b>Command mode:</b> VLAN</p>
<p><b>protocol-vlan &lt;1-8&gt; frame-type {ether2 llc snap} &lt;Ethernet type&gt;</b>            Configures the frame type and the Ethernet type for the selected protocol.            Ethernet type consists of a 4-digit (16 bit) hex code, such as 0080 (IPv4).  <b>Command mode:</b> VLAN</p>
<p><b>[no] protocol-vlan &lt;1-8&gt; member &lt;port alias or number&gt;</b>            Adds or removes a port to the selected PVLAN.  <b>Command mode:</b> VLAN</p>
<p><b>protocol-vlan &lt;1-8&gt; priority &lt;0-7&gt;</b>            Configures the priority value for this PVLAN.  <b>Command mode:</b> VLAN</p>
<p><b>protocol-vlan &lt;1-8&gt; protocol &lt;protocol type&gt;</b>            Selects a pre-defined protocol, as follows:</p> <ul style="list-style-type: none"> <li>o decEther2: DEC Local Area Transport</li> <li>o ipv4Ether2: Internet IP (IPv4)</li> <li>o ipv6Ether2: IPv6</li> <li>o ipx802.2: Novell IPX 802.2</li> <li>o ipx802.3: Novell IPX 802.3</li> <li>o ipxEther2: Novell IPX</li> <li>o ipxSnap: Novell IPX SNAP</li> <li>o netbios: NetBIOS 802.2</li> <li>o rarpEther2: Reverse ARP</li> <li>o sna802.2: SNA 802.2</li> <li>o snaEther2: Lenovo SNA Service on Ethernet</li> <li>o vinesEther2: Banyan VINES</li> <li>o xnsEther2: XNS Compatibility</li> </ul> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] protocol-vlan &lt;1-8&gt; tag-pvlan &lt;port alias or number&gt;</b>            Defines a port that will be tagged by the selected protocol on this VLAN.  <b>Command mode:</b> VLAN</p>

**Table 259.** *Protocol VLAN Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<b>no protocol-vlan</b> <1-8> Deletes the selected protocol configuration from the VLAN. <b>Command mode:</b> VLAN
<b>show protocol-vlan</b> <1-8> Displays current parameters for the selected PVLAN. <b>Command mode:</b> All

## Private VLAN Configuration

Use the following commands to configure Private VLAN.

**Table 260.** *Private VLAN Configuration Commands*

Command Syntax and Usage
<p><b>private-vlan association [add remove] &lt;secondary VLAN list&gt;</b></p> <p>Configures Private VLAN mapping between a primary VLAN and secondary VLANs. Enter the primary VLAN ID. If no optional parameter is specified, the list of secondary VLANs, replaces the currently associated secondary VLANs. Otherwise:</p> <ul style="list-style-type: none"><li>o add appends the secondary VLANs to the ones currently associated</li><li>o remove excludes the secondary VLANs from the ones currently associated</li></ul> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] private-vlan community</b></p> <p>Enables or disables the VLAN type as a community VLAN.</p> <p>Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] private-vlan isolated</b></p> <p>Enables or disables the VLAN type as an isolated VLAN.</p> <p>The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>[no] private-vlan primary</b></p> <p>Enables or disables the VLAN type as a Primary VLAN.</p> <p>A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN.</p> <p><b>Command mode:</b> VLAN</p>
<p><b>show vlan private-vlan [type]</b></p> <p>Displays private VLAN information. The type option lists only the VLAN type for each private VLAN: community, isolated or primary.</p> <p><b>Command mode:</b> All</p>

---

## Layer 3 Configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands.

**Table 261.** *Layer 3 Configuration Commands*

Command Syntax and Usage
<b>interface ip</b> <interface number> Configures the IP Interface. The EN4093R supports up to 128 IP interfaces. To view command options, see <a href="#">page 465</a> . <b>Command mode:</b> Global configuration
<b>ip pim component</b> <1-2> Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see <a href="#">page 549</a> . <b>Command mode:</b> Global configuration
<b>ip router-id</b> <IP address> Sets the router ID. <b>Command mode:</b> Global configuration
<b>route-map</b> <1-32> Enter IP Route Map mode. To view command options, see <a href="#">page 478</a> . <b>Command mode:</b> Global configuration
<b>router bgp</b> Configures Border Gateway Protocol. To view command options, see <a href="#">page 508</a> . <b>Command mode:</b> Global configuration
<b>router ospf</b> Configures OSPF. To view command options, see <a href="#">page 485</a> . <b>Command mode:</b> Global configuration
<b>router rip</b> Configures the Routing Interface Protocol. To view command options, see <a href="#">page 482</a> . <b>Command mode:</b> Global configuration
<b>router vrrp</b> Configures Virtual Router Redundancy. To view command options, see <a href="#">page 535</a> . <b>Command mode:</b> Global configuration

**Table 261.** *Layer 3 Configuration Commands*

<b>Command Syntax and Usage</b>
<b>ipv6 router ospf</b> Enters OSPFv3 configuration mode. To view command options, see <a href="#">page 494</a> . <b>Command mode:</b> Global configuration
<b>show layer3</b> Displays the current IP configuration. <b>Command mode:</b> All



## IP Interface Configuration

The EN4093R supports up to 128 IP interfaces. Each IP interface represents the EN4093R on an IP on your network. The Interface option is disabled by default.

IP Interfaces 127 and 128 are reserved for switch management. If the IPv6 feature is enabled on the switch, IP Interface 125 and 126 are also reserved.

**Note:** To maintain connectivity between the management module and the EN4093R, use the management module interface to change the IP address of the switch.

**Table 262.** *IP Interface Configuration Commands*

Command Syntax and Usage
<p><b>interface ip</b> &lt;interface number&gt;</p> <p>Enter IP interface mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] enable</b></p> <p>Enables or disables this IP interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip address</b> &lt;IP address&gt; [&lt;IP netmask&gt;]</p> <p>Configures the IP address of the switch interface, using dotted decimal notation.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip netmask</b> &lt;IP netmask&gt;</p> <p>Configures the IP subnet address mask for the interface, using dotted decimal notation.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip6host</b></p> <p>Enables or disables the IPv6 Host Mode on this interface.</p> <p>The default setting is <b>disabled</b> for data interfaces, and <b>enabled</b> for the management interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 address</b> &lt;IPv6 address&gt; [<b>enable</b>]</p> <p><b>ipv6 address</b> &lt;IPv6 address&gt; &lt;IPv6 prefix length (1-128)&gt; [<b>enable</b>]</p> <p><b>ipv6 address</b> &lt;IPv6 address&gt; &lt;IPv6 prefix length (1-128)&gt; <b>anycast</b> [<b>enable</b>]</p> <p>Configures the IPv6 address of the switch interface, using hexadecimal format with colons.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 prefixlen</b> &lt;IPv6 prefix length (1-128)&gt;</p> <p>Configures the subnet IPv6 prefix length.</p> <p>The default value is 0.</p> <p><b>Command mode:</b> Interface IP</p>

**Table 262.** *IP Interface Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>ipv6 secaddr6 address</b> &lt;IPv6 address&gt; &lt;IPv6 prefix length (1-128)&gt; <b>[anycast]</b></p> <p>Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>no ipv6 secaddr6</b></p> <p>Removes the secondary IPv6 address of the switch interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 unreachable</b></p> <p>Enables or disables sending of ICMP Unreachable messages. The default setting is <b>enabled</b>.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] relay</b></p> <p>Enables or disables the BOOTP relay on this interface. The default setting is <b>enabled</b>.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>vlan</b> &lt;VLAN number&gt;</p> <p>Configures the VLAN number for this interface. Each interface can belong to one VLAN.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>no interface ip</b> &lt;interface number&gt;</p> <p>Removes this IP interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>show interface ip</b> &lt;interface number&gt;</p> <p>Displays the current interface settings.</p> <p><b>Command mode:</b> All</p>

## IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery Configuration commands.

**Table 263.** *IPv6 Neighbor Discovery Configuration Options*

Command Syntax and Usage
<p><b>[no] ipv6 nd advmtu</b></p> <p>Enables or disables the MTU option in Router Advertisements. The default setting is <b>enabled</b>.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd dad-attempts &lt;1-10&gt;</b></p> <p>Configures the maximum number of duplicate address detection attempts. The default value is 1.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd hops-limit &lt;0-255&gt;</b></p> <p>Configures the Router Advertisement hop limit. The default value is 64.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd managed-config</b></p> <p>Enables or disables the managed address configuration flag of the interface. When enabled, the host IP address can be set automatically through DHCP. The default setting is <b>disabled</b>.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd other-config</b></p> <p>Enables or disables the other stateful configuration flag, which allows the interface to use DHCP for other stateful configuration. The default setting is <b>disabled</b>.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd ra-interval &lt;4-1800&gt;</b></p> <p>Configures the Router Advertisement maximum interval. The default value is 600.</p> <p><b>Note:</b> Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval.</p> <p><b>Command mode:</b> Interface IP</p>

**Table 263.** IPv6 Neighbor Discovery Configuration Options (continued)

Command Syntax and Usage
<p><b>[no] ipv6 nd ra-intervalmin</b> &lt;3-1800&gt;</p> <p>Configures the Router Advertisement minimum interval.</p> <p>The default value is 198.</p> <p><b>Note:</b> Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 nd ra-lifetime</b> &lt;0-9000&gt;</p> <p>Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (advint).</p> <p>The default value is 1800.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd reachable-time</b> &lt;1-3600&gt;</p> <p><b>[no] ipv6 nd reachable-time</b> &lt;1-3600000&gt; ms</p> <p>Configures the advertised reachability time, in seconds or milliseconds (ms).</p> <p>The default value is 30.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd retransmit-time</b> &lt;0-4294967&gt;</p> <p><b>[no] ipv6 nd retransmit-time</b> &lt;0-4294967295&gt; ms</p> <p>Configures the Router Advertisement re-transmit timer, in seconds or milliseconds (ms).</p> <p>The default value is 1.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 nd suppress-ra</b></p> <p>Enables or disables IPv6 Router Advertisements on the interface.</p> <p>The default setting is disabled (suppress Router Advertisements).</p> <p><b>Command mode:</b> Interface IP</p>

## Default Gateway Configuration

The switch can be configured with up to 4 IPv4 gateways. Gateways 1–4 are reserved for default gateways.

Default gateway indices are:

- 1-2: Data gateways
- 3: External management gateway
- 4: Internal management gateway

This option is disabled by default.

**Table 264.** *Default Gateway Configuration Commands*

Command Syntax and Usage
<p><b>ip gateway &lt;1-4&gt; address &lt;IP address&gt; [enable]</b></p> <p>Configures the IP address of the default IP gateway using dotted decimal notation. The <b>enable</b> option also enables the IP gateway for use.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip gateway &lt;1-4&gt; arp-health-check</b></p> <p>Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is <b>disabled</b>.</p> <p><b>Note:</b> The <b>arp</b> option does not apply to management gateways.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip gateway &lt;1-4&gt; enable</b></p> <p>Enables or disables the gateway for use.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip gateway &lt;1-4&gt; interval &lt;0-60&gt;</b></p> <p>The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds.</p> <p>The default is 2.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip gateway &lt;1-4&gt; retry &lt;1-120&gt;</b></p> <p>Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts.</p> <p>The default is 8 attempts.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 264.** *Default Gateway Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<b>no ip gateway</b> <1-4> Deletes the gateway from the configuration. <b>Command mode:</b> Global configuration
<b>show ip gateway</b> <1-4> Displays the current gateway settings. <b>Command mode:</b> All

## IPv4 Static Route Configuration

Up to 128 IPv4 static routes can be configured.

**Table 265.** IPv4 Static Route Configuration Commands

Command Syntax and Usage
<p><b>ip route</b> &lt;IP subnet&gt; &lt;IP netmask&gt; &lt;IP nexthop&gt; [&lt;interface number&gt;]</p> <p>Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip route</b> &lt;IP subnet&gt; &lt;IP netmask&gt; [&lt;interface number&gt;]</p> <p>Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip route destination-address</b> &lt;IP address&gt;</p> <p>Clears all IP static routes with this destination.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip route gateway</b> &lt;IP address&gt;</p> <p>Clears all IP static routes that use this gateway.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip route interval</b> &lt;1-60&gt;</p> <p>Configures the ping interval for ECMP health checks, in seconds.</p> <p>The default value is 1.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip route retries</b> &lt;1-60&gt;</p> <p>Configures the number of health check retries allowed before the switch declares that the gateway is down.</p> <p>The default value is 3.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip route static</b></p> <p>Displays the current IP static routes.</p> <p><b>Command mode:</b> All</p>

## IP Multicast Route Configuration

The following table describes the IP Multicast (IPMC) route commands.

**Note:** Before you can add an IPMC route, IGMP must be turned on, IGMP Snooping/Relay must be enabled, and the required VLANs must be added to IGMP Snooping/Relay.

**Table 266.** IP Multicast Route Configuration Commands

Command Syntax and Usage
<p><b>[no] ip mroute</b> &lt;IPMC destination&gt; &lt;VLAN number&gt; &lt;port alias or number&gt; {<b>primary backup host</b>} [<b>&lt;virtual router ID&gt; none</b>]</p> <p>Adds or removes a static multicast route. The destination address, VLAN, member port of the route and route type (primary, backup or host) must be specified.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip mroute</b> &lt;IP address&gt; &lt;VLAN number&gt; <b>adminkey</b> &lt;1-65535&gt; {<b>primary backup host</b>} [<b>&lt;virtual router ID&gt; none</b>]</p> <p>Adds or removes a static multicast route. The destination address, VLAN, member port of the route and route type (primary, backup or host) must be specified.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip mroute</b> &lt;IP address&gt; &lt;VLAN number&gt; <b>portchannel</b> &lt;LAG number&gt; {<b>primary backup host</b>} [<b>&lt;virtual router ID&gt; none</b>]</p> <p>Adds or removes a static multicast route. The destination address, VLAN, and member LAG of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip mroute all</b></p> <p>Removes all the static multicast routes configured.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip mroute</b></p> <p>Displays the current IP multicast routes.</p> <p><b>Command mode:</b> All</p>



## ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

**Table 267.** *ARP Configuration Commands*

Command Syntax and Usage
<p><b>ip arp rearp</b> &lt;2-120&gt;</p> <p>Defines re-ARP period, in minutes, for entries in the switch arp table. When ARP entries reach this value the switch will re-ARP for the address to attempt to refresh the ARP cache.</p> <p>The default value is 5.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip arp</b></p> <p>Displays the current ARP configurations.</p> <p><b>Command mode:</b> All</p>

## ARP Static Configuration

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

**Table 268.** ARP Static Configuration Commands

Command Syntax and Usage
<p><b>ip arp</b> <i>&lt;IP address&gt;</i> <i>&lt;MAC address&gt;</i> <b>vlan</b> <i>&lt;vlan number&gt;</i> <b>port</b> <i>&lt;port alias or number&gt;</i></p> <p>Adds a permanent ARP entry. To enable ARP on a LAG, add the port number of a member of the LAG.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip arp</b> <i>&lt;destination unicast IP address&gt;</i> <i>&lt;destination multicast MAC address&gt;</i> <b>vlan</b> <i>&lt;cluster vlan number&gt;</i></p> <p>Adds a static multicast ARP entry for Network Load Balancing (NLB).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip arp</b> [<i>&lt;IP address&gt;</i>   <b>all</b>]</p> <p>Deletes a specific permanent ARP entry or all ARP entries.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip arp static</b></p> <p>Displays current static ARP configuration.</p> <p><b>Command mode:</b> All</p>

## Dynamic ARP Inspection Configuration

Dynamic ARP Inspection (DAI) is a security feature that enables the device to intercept and examine all ARP request and response packets in a subnet and discard those packets with invalid IP to MAC address bindings.

DAI uses information gathered by DHCP Snooping to validate ARP information that travels through ports marked as being not trusted.

**Table 269.** *Dynamic ARP Inspection Configuration Options*

<b>Command Syntax and Usage</b>
<b>[no] ip arp inspection vlan &lt;VLAN ID (1-4094)&gt;</b> Enables or disables DAI on the selected VLANs. <b>Command mode:</b> Global configuration
<b>[no] ip arp inspection trust</b> Configures the current port to be a DAI trusted port. On a DAI trusted port, all ARP packets skip the security check. The default settings is untrusted. <b>Note:</b> Configuring trusted interfaces as being untrusted can result in a loss of connectivity. <b>Command mode:</b> Interface port
<b>[no] logging log arp-inspection</b> Enables or disables logging for DAI. The default setting is enabled. <b>Command mode:</b> Global configuration
<b>show ip arp inspection</b> Displays the current DAI configuration settings. For mode details, see <a href="#">page 99</a> . <b>Command mode:</b> All

## IP Forwarding Configuration

The following table displays IP Forwarding configuration commands.

**Table 270.** *IP Forwarding Configuration Commands*

<b>Command Syntax and Usage</b>
<b>[no] ip routing</b> Enables or disables IP forwarding (routing) on the EN4093R. The default setting is <b>enabled</b> . <b>Command mode:</b> Global configuration
<b>[no] ip routing directed-broadcasts</b> Enables or disables forwarding directed broadcasts. The default setting is <b>disabled</b> . <b>Command mode:</b> Global configuration
<b>[no] ip routing icmp6-redirect</b> Enables or disables IPv6 ICMP re-directs. The default setting is <b>disabled</b> . <b>Command mode:</b> Global configuration
<b>[no] ip routing no-icmp-redirect</b> Enables or disables ICMP re-directs. The default setting is <b>disabled</b> . <b>Command mode:</b> Global configuration
<b>show ip routing</b> Displays the current IP forwarding settings. <b>Command mode:</b> All

## Network Filter Configuration

The following table displays Network Filter configuration commands.

**Table 271.** *IP Network Filter Configuration Commands*

Command Syntax and Usage
<p><b>ip match-address</b> &lt;1-256&gt; &lt;IP address&gt; &lt;IP netmask&gt;</p> <p>Sets the starting IP address and IP Netmask for this filter to define the range of IP addresses that will be accepted by the peer when the filter is enabled.</p> <p>The default address is 0.0.0.0 0.0.0.0.</p> <p><b>Note:</b> For Border Gateway Protocol (BGP), assign the network filter to an access-list in a route map, then assign the route map to the peer.</p> <p><b>Command mode:</b> Global configuration.</p>
<p><b>[no] ip match-address</b> &lt;1-256&gt; <b>enable</b></p> <p>Enables or disables the Network Filter configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip match-address</b> &lt;1-256&gt;</p> <p>Deletes the Network Filter configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip match-address</b> [&lt;1-256&gt;]</p> <p>Displays the current the Network Filter configuration.</p> <p><b>Command mode:</b> All</p>

## Routing Map Configuration

**Note:** The *map number* (1-32) represents the routing map you wish to configure. Routing maps control and modify routing information.

**Table 272.** *Routing Map Configuration Commands*

Command Syntax and Usage
<b>route-map</b> <1-32> Enter route map configuration mode. <b>Command mode:</b> Global configuration
<b>[no] access-list</b> <1-8> Configures the Access List. For more information, see <a href="#">page 480</a> . <b>Command mode:</b> Route map
<b>[no] as-path-list</b> <1-8> Configures the Autonomous System (AS) Filter. For more information, see <a href="#">page 481</a> . <b>Command mode:</b> Route map
<b>[no] as-path-preference</b> <1-65535> Sets the AS path preference of the matched route. You can configure up to 32 path preferences. <b>Command mode:</b> Route map
<b>[no] enable</b> Enables or disables the route map. <b>Command mode:</b> Route map
<b>[no] local-preference</b> <0-4294967294> Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred. <b>Command mode:</b> Route map
<b>[no] metric</b> <1-4294967294> Sets the metric of the matched route. <b>Command mode:</b> Route map
<b>[no] metric-type {1 2}</b> Assigns the type of OSPF metric. The default is type 1. <ul style="list-style-type: none"><li>o Type 1—External routes are calculated using both internal and external metrics.</li><li>o Type 2—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2.</li><li>o none—Removes the OSPF metric.</li></ul> <b>Command mode:</b> Route map

**Table 272.** *Routing Map Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>precedence</b> &lt;1-255&gt;</p> <p>Sets the precedence of the route map. The smaller the value, the higher the precedence.</p> <p>The default value is 10.</p> <p><b>Command mode:</b> Route map</p>
<p><b>[no] weight</b> &lt;0-65534&gt;</p> <p>Sets the weight of the route map.</p> <p><b>Command mode:</b> Route map</p>
<p><b>no route-map</b> &lt;1-32&gt;</p> <p>Deletes the route map.</p> <p><b>Command mode:</b> Route map</p>
<p><b>show route-map</b> [&lt;1-32&gt;]</p> <p>Displays the current route configuration.</p> <p><b>Command mode:</b> All</p>

## IP Access List Configuration

**Note:** The *route map number* (1-32) and the *access list number* (1-8) represent the IP access list you wish to configure.

**Table 273.** *IP Access List Configuration Commands*

Command Syntax and Usage
<b>access-list</b> <1-8> <b>action</b> { <b>permit</b>   <b>deny</b> } Permits or denies action for the access list. <b>Command mode:</b> Route map
<b>[no] access-list</b> <1-8> <b>enable</b> Enables or disables the access list. <b>Command mode:</b> Route map
<b>[no] access-list</b> <1-8> <b>match-address</b> <1-256> Sets the network filter number. See <a href="#">“Network Filter Configuration” on page 477</a> for details. <b>Command mode:</b> Route map
<b>[no] access-list</b> <1-8> <b>metric</b> <1-4294967294> Sets the metric value in the AS-External (ASE) LSA. <b>Command mode:</b> Route map
<b>no access-list</b> <1-8> Deletes the access list. <b>Command mode:</b> Route map
<b>show route-map</b> <1-32> <b>access-list</b> <1-8> Displays the current Access List configuration. <b>Command mode:</b> All



## Autonomous System Filter Path Configuration

**Note:** The *rmap number* and the *path number* represent the AS path you wish to configure.

**Table 274.** AS Filter Configuration Commands

Command Syntax and Usage
<b>as-path-list</b> <1-8> <b>action</b> { <b>permit</b>   <b>deny</b> } Permits or denies Autonomous System filter action. <b>Command mode:</b> Route map
<b>as-path-list</b> <1-8> <b>as-path</b> <1-65535> Sets the Autonomous System filter's path number. <b>Command mode:</b> Route map
<b>[no] as-path-list</b> <1-8> <b>enable</b> Enables or disables the Autonomous System filter. <b>Command mode:</b> Route map
<b>no as-path-list</b> <1-8> Deletes the Autonomous System filter. <b>Command mode:</b> Route map
<b>show route-map</b> <1-32> <b>as-path-list</b> <1-8> Displays the current Autonomous System filter configuration. <b>Command mode:</b> All

## Routing Information Protocol Configuration

RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

**Table 275.** *Routing Information Protocol Commands*

Command Syntax and Usage
<b>router rip</b> Enter Router RIP configuration mode. <b>Command mode:</b> Global Configuration
<b>[no] enable</b> Globally enables or disables RIP. <b>Command mode:</b> Router RIP
<b>timers update &lt;1-120&gt;</b> Configures the time interval for sending for RIP table updates, in seconds. The default value is 30. <b>Command mode:</b> Router RIP
<b>show ip rip</b> Displays the current RIP configuration. <b>Command mode:</b> All

### *RIP Interface Configuration*

The RIP Interface commands are used for configuring Routing Information Protocol parameters for the selected interface.

**Note:** Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

**Table 276.** *RIP Interface Commands*

Command Syntax and Usage
<b>[no] ip rip authentication key &lt;password&gt;</b> Configures the authentication key password. <b>Command mode:</b> Interface IP
<b>[no] ip rip authentication type [&lt;password&gt;]</b> Configures the authentication type. The default is none. <b>Command mode:</b> Interface IP

**Table 276.** *RIP Interface Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>[no] ip rip default-action {listen supply both}</b></p> <p>When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes.</p> <p>The default value is none.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip rip enable</b></p> <p>Enables or disables this RIP interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip rip listen</b></p> <p>When enabled, the switch learns routes from other routers.</p> <p>The default value is enabled.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip rip metric [&lt;1-15&gt;]</b></p> <p>Configures the route metric, which indicates the relative distance to the destination.</p> <p>The default value is 1.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip rip multicast-updates</b></p> <p>Enables or disables multicast updates of the routing table (using address 224.0.0.9).</p> <p>The default value is enabled.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip rip poison</b></p> <p>When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon.</p> <p>The default value is disabled.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip rip split-horizon</b></p> <p>Enables or disables split horizon.</p> <p>The default value is enabled.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip rip supply</b></p> <p>When enabled, the switch supplies routes to other routers.</p> <p>The default value is enabled.</p> <p><b>Command mode:</b> Interface IP</p>

**Table 276.** *RIP Interface Commands (continued)*

Command Syntax and Usage
<p><b>[no] ip rip triggered</b></p> <p>Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message.</p> <p>The default value is <b>enabled</b>.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip rip version {1 2 both}</b></p> <p>Configures the RIP version used by this interface.</p> <p>The default value is <b>version 2</b>.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>show interface ip &lt;interface number&gt; rip</b></p> <p>Displays the current RIP configuration.</p> <p><b>Command mode:</b> All</p>

## *RIP Route Redistribution Configuration*

The following table describes the RIP Route Redistribution commands.

**Table 277.** *RIP Redistribution Commands*

Command Syntax and Usage
<p><b>[no] redistribute {fixed static ospf eospf ebgp ibgp} &lt;1-32&gt;</b></p> <p>Adds or removes the selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma ( , ). To add or removes all 32 route maps, type <b>all</b>.</p> <p>The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.</p> <p><b>Command mode:</b> Router RIP</p>
<p><b>redistribute {fixed static ospf eospf ebgp ibgp} export &lt;1-15&gt;</b></p> <p>Exports the routes of this protocol in which the metric and metric type are specified.</p> <p><b>Command mode:</b> Router RIP</p>
<p><b>no redistribute {fixed static ospf eospf ebgp ibgp} export</b></p> <p>Stops exporting the routes of the protocol.</p> <p><b>Command mode:</b> RIP</p>
<p><b>show ip rip redistribute</b></p> <p>Displays the current RIP route redistribute configuration.</p> <p><b>Command mode:</b> All</p>

## Open Shortest Path First Configuration

The following table describes the OSPF commands.

**Table 278.** *OSPF Configuration Commands*

Command Syntax and Usage
<p><b>router ospf</b></p> <p>Enter Router OSPF configuration mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip ospf</b> &lt;interface number&gt;</p> <p>Configures the OSPF interface. See <a href="#">page 489</a> to view command options.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>area</b> &lt;0-2&gt;</p> <p>Configures the OSPF area index. See <a href="#">page 486</a> to view command options.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area-virtual-link</b> &lt;1-3&gt;</p> <p>Configures the Virtual Links used to configure OSPF for a Virtual Link. See <a href="#">page 491</a> to view command options.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area-range</b> &lt;1-16&gt;</p> <p>Configures summary routes for up to 16 IP addresses. See <a href="#">page 488</a> to view command options.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>default-information</b> &lt;1-16777214&gt; &lt;AS external metric type (1-2)&gt;</p> <p>Sets one default route among multiple choices in an area.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>no default-information</b></p> <p>Removes the default route information.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>[no] enable</b></p> <p>Enables or disables OSPF on the EN4093R.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>host</b> &lt;1-128&gt;</p> <p>Configures OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See <a href="#">page 492</a> to view command options.</p> <p><b>Command mode:</b> Router OSPF</p>

**Table 278.** OSPF Configuration Commands (continued)

Command Syntax and Usage
<b>lsdb-limit</b> <LSDB limit (0-2048, 0 for no limit)> Sets the link state database limit. <b>Command mode:</b> Router OSPF
<b>message-digest-key</b> <1-255> <b>md5-key</b> <text string> Assigns a string to MD5 authentication key. <b>Command mode:</b> Router OSPF
<b>redistribute</b> Configures OSPF route redistribution. See <a href="#">page 493</a> to view command options. <b>Command mode:</b> Router OSPF
<b>show ip ospf</b> Displays the current OSPF configuration settings. <b>Command mode:</b> All

## Area Index Configuration

The following table describes the Area Index commands.

**Table 279.** Area Index Configuration Commands

Command Syntax and Usage
<b>area</b> <0-2> <b>area-id</b> <IP address> Defines the IP address of the OSPF area number. <b>Command mode:</b> Router OSPF
<b>[no] area</b> <0-2> <b>authentication-type</b> {password md5} None: No authentication required. Password: Authenticates simple passwords so that only trusted routing devices can participate. md5: This parameter is used when MD5 cryptographic authentication is required. <b>Command mode:</b> Router OSPF
<b>[no] area</b> <0-2> <b>enable</b> Enables or disables the OSPF area. <b>Command mode:</b> Router OSPF
<b>area</b> <0-2> <b>spf-interval</b> <1-255> Configures the minimum time interval, in seconds, between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm. The default value is 10. <b>Command mode:</b> Router OSPF

**Table 279.** *Area Index Configuration Commands*

<b>Command Syntax and Usage</b>
<p><b>area</b> &lt;0-2&gt; <b>stub-metric</b> &lt;1-65535&gt;</p> <p>Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions.</p> <p>Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area</b> &lt;0-2&gt; <b>type {transit stub nssa}</b></p> <p>Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.</p> <p><b>Transit area:</b> allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.</p> <p><b>Stub area:</b> is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.</p> <p><b>NSSA:</b> Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>no area</b> &lt;0-2&gt;</p> <p>Deletes the OSPF area.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>show ip ospf area</b> &lt;0-2&gt;</p> <p>Displays the current OSPF configuration.</p> <p><b>Command mode:</b> All</p>

## OSPF Summary Range Configuration

The following table describes the OSPF Summary Range commands.

**Table 280.** *OSPF Summary Range Configuration Commands*

Command Syntax and Usage
<b>area-range</b> <1-16> <b>address</b> <IP address> <IP netmask> Displays the base IP address or the IP address mask for the range. <b>Command mode:</b> Router OSPF
<b>area-range</b> <1-16> <b>area</b> <0-2> Displays the area index used by the EN4093R. <b>Command mode:</b> Router OSPF
<b>[no] area-range</b> <1-16> <b>enable</b> Enables or disables the OSPF summary range. <b>Command mode:</b> Router OSPF
<b>[no] area-range</b> <1-16> <b>hide</b> Hides or shows the OSPF summary range. <b>Command mode:</b> Router OSPF
<b>no area-range</b> <1-16> Deletes the OSPF summary range. <b>Command mode:</b> Router OSPF
<b>show ip ospf area-range</b> <1-16> Displays the current OSPF summary range. <b>Command mode:</b> Router OSPF



## OSPF Interface Configuration

The following table describes the OSPF Interface commands.

**Table 281.** *OSPF Interface Configuration Commands*

Command Syntax and Usage
<p><b>ip ospf area</b> &lt;0-2&gt;</p> <p>Configures the OSPF area index.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip ospf cost</b> &lt;1-65535&gt;</p> <p>Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip ospf dead-interval</b> &lt;1-65535&gt;  <b>ip ospf dead-interval</b> &lt;1000-65535ms&gt;</p> <p>Configures the health parameters of a hello packet, in seconds or milliseconds, before declaring a silent router to be down.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip ospf enable</b></p> <p>Enables or disables OSPF interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip ospf hello-interval</b> &lt;1-65535&gt;  <b>ip ospf hello-interval</b> &lt;50-65535ms&gt;</p> <p>Configures the interval, in seconds or milliseconds, between the hello packets for the interfaces.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip ospf message-digest-key</b> &lt;1-255&gt;</p> <p>Assigns an MD5 key to the interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip ospf key</b> &lt;key string&gt;</p> <p>Sets the authentication key to clear the password.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip ospf passive-interface</b></p> <p>Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip ospf point-to-point</b></p> <p>Sets the interface as point-to-point.</p> <p><b>Command mode:</b> Interface IP</p>

**Table 281.** *OSPF Interface Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>ip ospf priority</b> &lt;0-255&gt;</p> <p>Configures the priority value for the EN4093R's OSPF interfaces.</p> <p>A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip ospf retransmit-interval</b> &lt;1-3600&gt;</p> <p>Configures the retransmit interval in seconds.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip ospf transit-delay</b> &lt;1-3600&gt;</p> <p>Configures the transit delay in seconds.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>no ip ospf</b></p> <p>Deletes the OSPF interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>show interface ip</b> &lt;interface number&gt; <b>ospf</b></p> <p>Displays the current settings for OSPF interface.</p> <p><b>Command mode:</b> All</p>

## OSPF Virtual Link Configuration

The following table describes the OSPF Virtual Link commands.

**Table 282.** *OSPF Virtual Link Configuration Commands*

Command Syntax and Usage
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>area</b> &lt;0-2&gt;</p> <p>Configures the OSPF area index for the virtual link.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>dead-interval</b> &lt;1-65535&gt;  <b>area-virtual-link</b> &lt;1-3&gt; <b>dead-interval</b> &lt;1000-65535ms&gt;</p> <p>Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 40.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>[no] area-virtual-link</b> &lt;1-3&gt; <b>enable</b></p> <p>Enables or disables OSPF virtual link.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>hello-interval</b> &lt;1-65535&gt;  <b>area-virtual-link</b> &lt;1-3&gt; <b>hello-interval</b> &lt;50-65535ms&gt;</p> <p>Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is 10.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>[no] area-virtual-link</b> &lt;1-3&gt; <b>key</b> &lt;password&gt;</p> <p>Configures the password (up to eight characters) for each virtual link. The default setting is none.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>message-digest-key</b> &lt;1-255&gt;</p> <p>Sets MD5 key ID for each virtual link. The default setting is none.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>neighbor-router</b> &lt;IP address&gt;</p> <p>Configures the router ID of the virtual neighbor. The default value is 0.0.0.0.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>retransmit-interval</b> &lt;1-3600&gt;</p> <p>Configures the retransmit interval, in seconds. The default value is 5.</p> <p><b>Command mode:</b> Router OSPF</p>

**Table 282.** *OSPF Virtual Link Configuration Commands (continued)*

<b>Command Syntax and Usage</b>
<b>area-virtual-link</b> <1-3> <b>transit-delay</b> <1-3600> Configures the delay in transit, in seconds. The default value is 1. <b>Command mode:</b> Router OSPF
<b>no area-virtual-link</b> <1-3> Deletes OSPF virtual link. <b>Command mode:</b> Router OSPF
<b>show ip ospf area-virtual-link</b> <1-3> Displays the current OSPF virtual link settings. <b>Command mode:</b> All

## OSPF Host Entry Configuration

The following table describes the OSPF Host Entry commands.

**Table 283.** *OSPF Host Entry Configuration Commands*

<b>Command Syntax and Usage</b>
<b>host</b> <1-128> <b>address</b> <IP address> Configures the base IP address for the host entry. <b>Command mode:</b> Router OSPF
<b>host</b> <1-128> <b>area</b> <0-2> Configures the area index of the host. <b>Command mode:</b> Router OSPF
<b>host</b> <1-128> <b>cost</b> <1-65535> Configures the cost value of the host. <b>Command mode:</b> Router OSPF
<b>[no] host</b> <1-128> <b>enable</b> Enables or disables OSPF host entry. <b>Command mode:</b> Router OSPF
<b>no host</b> <1-128> Deletes OSPF host entry. <b>Command mode:</b> Router OSPF
<b>show ip ospf host</b> <1-128> Displays the current OSPF host entries. <b>Command mode:</b> All

## OSPF Route Redistribution Configuration

The following table describes the OSPF Route Redistribution commands.

**Table 284.** *OSPF Route Redistribution Configuration Commands*

Command Syntax and Usage
<p><b>[no] redistribute {fixed static rip ebgp ibgp} &lt;rmap ID (1-32)&gt;</b></p> <p>Adds or removes selected routing map to the rmap list.</p> <p>This option adds or removes a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>[no] redistribute {fixed static rip ebgp ibgp} export metric &lt;1-16777214&gt; metric-type {type1 type2}</b></p> <p>Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter <b>none</b>.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>show ip ospf redistribute</b></p> <p>Displays the current route map settings.</p> <p><b>Command mode:</b> All</p>

## OSPF MD5 Key Configuration

The following table describes the OSPF MD5 Key commands.

**Table 285.** *OSPF MD5 Key Commands*

Command Syntax and Usage
<p><b>message-digest-key &lt;1-255&gt; md5-key &lt;1-16 characters&gt;</b></p> <p>Sets the authentication key for this OSPF packet.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>no message-digest-key &lt;1-255&gt;</b></p> <p>Deletes the authentication key for this OSPF packet.</p> <p><b>Command mode:</b> Router OSPF</p>
<p><b>show ip ospf message-digest-key &lt;1-255&gt;</b></p> <p>Displays the current MD5 key configuration.</p> <p><b>Command mode:</b> All</p>

## Open Shortest Path First Version 3 Configuration

The following table describes the OSPFv3 commands.

**Table 286.** *OSPFv3 Configuration Commands*

Command Syntax and Usage
<p><b>[no] ipv6 router ospf</b>            Enter OSPFv3 configuration mode. Enables or disables OSPFv3 routing protocol.  <b>Command mode:</b> Global configuration</p>
<p><b>abr-type [standard cisco ibm]</b>            Configures the Area Border Router (ABR) type, as follows:</p> <ul style="list-style-type: none"> <li>o Standard</li> <li>o Cisco</li> <li>o IBM</li> </ul> <p>The default setting is <code>standard</code>.  <b>Command mode:</b> Router OSPF3</p>
<p><b>as-external lsdb-limit</b> &lt;LSDB limit (0-2147483647, -1 for no limit)&gt;            Sets the link state database limit.  <b>Command mode:</b> Router OSPF3</p>
<p><b>[no] enable</b>            Enables or disables OSPFv3 on the switch.  <b>Command mode:</b> Router OSPF3</p>
<p><b>exit-overflow-interval</b> &lt;0-4294967295&gt;            Configures the number of seconds that a router takes to exit Overflow State.            The default value is 0.  <b>Command mode:</b> Router OSPF3</p>
<p><b>[no] nssaAsbrDfRtTrans</b>            Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR.            The default setting is <code>disabled</code>.  <b>Command mode:</b> Router OSPF3</p>

**Table 286.** OSPFv3 Configuration Commands (continued)

Command Syntax and Usage
<p><b>neighbor</b> &lt;1-256&gt; {<b>address</b> &lt;IPv6 address&gt; <b>enable</b> <b>interface</b> &lt;1-126&gt; <b>priority</b> &lt;0-255&gt;}</p> <p>Configures directly reachable routers over non-broadcast networks. This is required for non-broadcast multiple access (NBMA) networks and optional for Point-to-Multipoint networks.</p> <ul style="list-style-type: none"> <li>o <b>address</b> configures the neighbor's IPv6 address.</li> <li>o <b>enable</b> activates a previously disabled neighbor.</li> <li>o <b>interface</b> configures the OSPFv3 interface used for the neighbor entry.</li> <li>o <b>priority</b> configures the priority value used for the neighbor entry. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the neighbor cannot be used as Designated Router.</li> </ul> <p>The default value is 1.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>no neighbor</b> &lt;1-256&gt; [<b>enable</b>]</p> <p>Deletes the neighbor entry.</p> <p>Using the <b>enable</b> option only disables the neighbor, while preserving its settings.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>reference-bandwidth</b> &lt;0-4294967295&gt;</p> <p>Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric.</p> <p>The default value is 100,000.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>router-id</b> &lt;IPv4 address&gt;</p> <p>Defines the router ID.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>timers spf</b> {&lt;SPF delay (0-65535)&gt;} {&lt;SPF hold time (0-65535)&gt;}</p> <p>Configures the number of seconds that SPF calculation is delayed after a topology change message is received.</p> <p>The default value is 5.</p> <p>Configures the number of seconds between SPF calculations.</p> <p>The default value is 10.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>show ipv6 ospf</b></p> <p>Displays the current OSPF configuration settings.</p> <p><b>Command mode:</b> All</p>

## OSPFv3 Area Index Configuration

The following table describes the OSPFv3 Area Index commands.

**Table 287.** *OSPFv3 Area Index Configuration Options*

Command Syntax and Usage
<p><b>area</b> &lt;area index&gt; <b>area-id</b> &lt;IP address&gt;</p> <p>Defines the IP address of the OSPFv3 area number.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area</b> &lt;area index&gt; <b>default-metric</b> &lt;metric value (1-16777215)&gt;</p> <p>Configures the cost for the default summary route in a stub area or NSSA.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area</b> &lt;area index&gt; <b>default-metric type</b> &lt;1-3&gt;</p> <p>Configures the default metric type applied to the route.</p> <p><b>Note:</b> This command applies only to area type of Stub/NSSA.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>[no] area</b> &lt;area index&gt; <b>enable</b></p> <p>Enables or disables the OSPF area.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area</b> &lt;area index&gt; <b>stability-interval</b> &lt;1-255&gt;</p> <p>Configures the stability interval for an NSSA, in seconds. When the interval expires, an elected translator determines that its services are no longer required.</p> <p>The default value is 40.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area</b> &lt;area index&gt; <b>translation-role</b> {always candidate}</p> <p>Configures the translation role for an NSSA area, as follows:</p> <ul style="list-style-type: none"> <li>o <b>always:</b> Type 7 LSAs are always translated into Type 5 LSAs.</li> <li>o <b>candidate:</b> An NSSA border router participates in the translator election process.</li> </ul> <p>The default setting is candidate.</p> <p><b>Command mode:</b> Router OSPF3</p>



**Table 287.** OSPFv3 Area Index Configuration Options (continued)

Command Syntax and Usage
<p><b>area</b> <i>&lt;area index&gt;</i> <b>type {transit stub nssa} {no-summary}</b></p> <p>Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.</p> <p><b>Transit area:</b> allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.</p> <p><b>Stub area:</b> is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.</p> <p><b>NSSA:</b> Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.</p> <p>Enables or disables the no-summary option. When enabled, the area-border router neither originates nor propagates Inter-Area-Prefix LSAs into stub/NSSA areas. Instead it generates a default Inter-Area-Prefix LSA.</p> <p>The default setting is <b>disabled</b>.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>no area</b> <i>&lt;area index&gt;</i></p> <p>Deletes the OSPF area.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>show ipv6 ospf areas</b></p> <p>Displays the current OSPFv3 area configuration.</p> <p><b>Command mode:</b> All</p>

## OSPFv3 Summary Range Configuration

The following table describes the OSPFv3 Summary Range commands.

**Table 288.** *OSPFv3 Summary Range Configuration Options*

Command Syntax and Usage
<b>area-range</b> <1-16> <b>address</b> <IPv6 address> <prefix length (1-128)> Configures the base IPv6 address and subnet prefix length for the range. <b>Command mode:</b> Router OSPF3
<b>area-range</b> <1-16> <b>area</b> <area index (0-2)> Configures the area index used by the switch. <b>Command mode:</b> Router OSPF3
<b>[no] area-range</b> <1-16> <b>enable</b> Enables or disables the OSPFv3 summary range. <b>Command mode:</b> Router OSPF3
<b>[no] area-range</b> <1-16> <b>hide</b> Hides or shows the OSPFv3 summary range. <b>Command mode:</b> Router OSPF3
<b>area-range</b> <1-16> <b>lsa-type</b> {summary Type7} Configures the LSA type, as follows: <ul style="list-style-type: none"><li>o Summary LSA</li><li>o Type7 LSA</li></ul> <b>Command mode:</b> Router OSPF3
<b>area-range</b> <1-16> <b>tag</b> <0-4294967295> Configures the route tag. <b>Command mode:</b> Router OSPF3
<b>no area-range</b> <1-16> Deletes the OSPFv3 summary range. <b>Command mode:</b> Router OSPF3
<b>show ipv6 ospf area-range</b> Displays the current OSPFv3 summary range. <b>Command mode:</b> All

## OSPFv3 AS-External Range Configuration

The following table describes the OSPFv3 AS-External Range commands.

**Table 289.** OSPFv3 AS-External Range Configuration Options

Command Syntax and Usage
<p><b>summary-prefix</b> &lt;1-16&gt; <b>address</b> &lt;IPv6 address&gt; &lt;IPv6 prefix length (1-128)&gt;</p> <p>Configures the base IPv6 address and the subnet prefix length for the range.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>summary-prefix</b> &lt;1-16&gt; <b>aggregation-effect</b> {allowAll denyAll advertise not-advertise}</p> <p>Configures the aggregation effect, as follows:</p> <ul style="list-style-type: none"> <li>– <b>allowAll:</b> If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. Aggregated Type-7 LSAs are generated in all the attached NSSAs for the range.</li> <li>– <b>denyAll:</b> Type-5 and Type-7 LSAs are not generated.</li> <li>– <b>advertise:</b> If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. For other area IDs, aggregated Type-7 LSAs are generated in the NSSA area.</li> <li>– <b>not-advertise:</b> If the area ID is 0.0.0.0, Type-5 LSAs are not generated, while all NSSA LSAs within the range are cleared and aggregated Type-7 LSAs are generated for all NSSAs. For other area IDs, aggregated Type-7 LSAs are not generated in the NSSA area.</li> </ul> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>summary-prefix</b> &lt;1-16&gt; <b>area</b> &lt;area index (0-2)&gt;</p> <p>Configures the area index used by the switch.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>[no] summary-prefix</b> &lt;1-16&gt; <b>enable</b></p> <p>Enables or disables the OSPFv3 AS-external range.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>[no] summary-prefix</b> &lt;1-16&gt; <b>translation</b></p> <p>When enabled, the P-bit is set in the generated Type-7 LSA. When disabled, the P-bit is cleared.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>no summary-prefix</b> &lt;1-16&gt;</p> <p>Deletes the OSPFv3 AS-external range.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>show ipv6 ospf summary-prefix</b> &lt;1-16&gt;</p> <p>Displays the current OSPFv3 AS-external range.</p> <p><b>Command mode:</b> All</p>

## OSPFv3 Interface Configuration

The following table describes the OSPFv3 Interface commands.

**Table 290.** *OSPFv3 Interface Configuration Options*

Command Syntax and Usage
<b>interface ip</b> <interface number> Enter Interface IP mode, from Global Configuration mode. <b>Command mode:</b> Global configuration
<b>[no] ipsec dynamic-policy</b> <1-10> Adds or removes an IP security dynamic policy to the OSPFv3 interface. <b>Command mode:</b> Interface IP
<b>[no] ipsec manual-policy</b> <1-10> Adds or removes an IP security manual policy to the OSPFv3 interface. <b>Command mode:</b> Interface IP
<b>ipv6 ospf area</b> <area index (0-2)> Configures the OSPFv3 area index. <b>Command mode:</b> Interface IP
<b>ipv6 ospf area</b> <area index (0-2)> <b>instance</b> <0-255> Configures the instance ID for the interface. <b>Command mode:</b> Interface IP
<b>[no] ipv6 ospf cost</b> <1-65535> Configures the metric value for sending a packet on the interface. <b>Command mode:</b> Interface IP
<b>[no] ipv6 ospf dead-interval</b> <1-65535> Configures the health parameters of a hello packet, in seconds, before declaring a silent router to be down. <b>Command mode:</b> Interface IP
<b>[no] ipv6 ospf enable</b> Enables or disables OSPFv3 on the interface. <b>Command mode:</b> Interface IP
<b>[no] ipv6 ospf hello-interval</b> <1-65535> Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface. <b>Command mode:</b> Interface IP

**Table 290.** OSPFv3 Interface Configuration Options (continued)

<p><b>Command Syntax and Usage</b></p>
<p><b>[no] ipv6 ospf linklsasuppress</b></p> <p>Enables or disables Link LSA suppression. When suppressed, no Link LSAs are originated.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 ospf network {broadcast non-broadcast   pint-to-multipoint point-to-point}</b></p> <p>Configures the network type for the OSPFv3 interface:</p> <ul style="list-style-type: none"> <li>o broadcast: network where all routers use the broadcast capability</li> <li>o non-broadcast: non-broadcast multiple access (NBMA) network supporting pseudo-broadcast (multicast and broadcast traffic is configured manually)</li> <li>o point-to-multipoint: network where multiple point-to-point links are set up on the same interface</li> <li>o point-to-point: network that joins a single pair of routers</li> </ul> <p>The default value is broadcast.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 ospf passive-interface</b></p> <p>Enables or disables the <b>passive</b> setting on the interface. On a <b>passive</b> interface, OSPFv3 protocol packets are suppressed.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 ospf poll-interval &lt;0-4294967295&gt;</b></p> <p>Configures the poll interval in seconds for neighbors in NBMA networks.</p> <p>The default value is 120.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>no ipv6 ospf poll-interval</b></p> <p>Configures the poll interval in seconds for neighbors in NBMA and point-to-multipoint networks to its default 120 seconds value.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 ospf priority &lt;priority value (0-255)&gt;</b></p> <p>Configures the priority value for the switch's OSPFv3 interface.</p> <p>A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR).</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ipv6 ospf retransmit-interval &lt;1-1800&gt;</b></p> <p>Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface.</p> <p><b>Command mode:</b> Interface IP</p>

**Table 290.** *OSPFv3 Interface Configuration Options (continued)*

Command Syntax and Usage
<b>[no] ipv6 ospf transmit-delay</b> <1-1800> Configures the estimated time, in seconds, taken to transmit LS update packet over this interface. <b>Command mode:</b> Interface IP
<b>no ipv6 ospf</b> Deletes OSPFv3 from interface. <b>Command mode:</b> Interface IP
<b>show ipv6 ospf interface</b> Displays the current settings for OSPFv3 interface. <b>Command mode:</b> Interface IP

## OSPFv3 over IPsec Configuration

The following table describes the OSPFv3 over IPsec Configuration commands.

**Table 291.** *Layer 3 IPsec Configuration Options*

Command Syntax and Usage
<b>ipv6 ospf authentication ipsec enable</b> Enables IPsec authentication. <b>Command mode:</b> Interface IP
<b>ipv6 ospf authentication ipsec spi</b> <256-4294967295> {md5 sha1} <authentication key (hexadecimal)> Configures the Security Parameters Index (SPI), algorithm, and authentication key for the Authentication Header (AH). The algorithms supported are: <ul style="list-style-type: none"><li>o MD5 (hexadecimal key length is 32)</li><li>o SHA1 (hexadecimal key length is 40)</li></ul> <b>Command mode:</b> Interface IP
<b>ipv6 ospf authentication ipsec default</b> Resets the Authentication Header (AH) configuration to default values. <b>Command mode:</b> Interface IP
<b>no ipv6 ospf authentication ipsec spi</b> <256-4294967295> Disables the specified Authentication Header (AH) SPI. <b>Command mode:</b> Interface IP

**Table 291.** Layer 3 IPsec Configuration Options (continued)

Command Syntax and Usage
<p><b>ipv6 ospf encryption ipsec enable</b></p> <p>Enables OSPFv3 encryption for this interface.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 ospf encryption ipsec spi</b> &lt;256-4294967295&gt;  <b>esp</b> {3des aes-cbc des null} &lt;encryption key (hexadecimal)&gt; <b>null</b>  <b>{md5 sha1 none}</b> &lt;authentication key (hexadecimal)&gt;</p> <p>Configures the Security Parameters Index (SPI), encryption algorithm, authentication algorithm, and authentication key for the Encapsulating Security Payload (ESP). The ESP algorithms supported are:</p> <ul style="list-style-type: none"> <li>o 3DES (hexadecimal key length is 48)</li> <li>o AES-CBC (hexadecimal key length is 32)</li> <li>o DES (hexadecimal key length is 16)</li> </ul> <p>The authentication algorithms supported are:</p> <ul style="list-style-type: none"> <li>o MD5 (hexadecimal key length is 32)</li> <li>o SHA1 (hexadecimal key length is 40)</li> <li>o none</li> </ul> <p><b>Note:</b> If the encryption algorithm is null, the authentication algorithm must be either MD5 or SHA1. (hexadecimal key length is 40). If an encryption algorithm is specified (3DES, AES-CBC, or DES), the authentication algorithm can be none.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 ospf encryption ipsec default</b></p> <p>Resets the Encapsulating Security Payload (ESP) configuration to default values.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>no ipv6 ospf encryption ipsec spi</b> &lt;256-4294967295&gt;</p> <p>Disables the specified Encapsulating Security Payload (ESP) SPI.</p> <p><b>Command mode:</b> Interface IP</p>

## OSPFv3 Virtual Link Configuration

The following table describes the OSPFv3 Virtual Link commands.

**Table 292.** *OSPFv3 Virtual Link Configuration Options*

Command Syntax and Usage
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>area</b> &lt;area index (0-2)&gt;</p> <p>Configures the OSPF area index.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>dead-interval</b> &lt;1-65535&gt;</p> <p>Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>[no] area-virtual-link</b> &lt;1-3&gt; <b>enable</b></p> <p>Enables or disables OSPF virtual link.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>hello-interval</b> &lt;1-65535&gt;</p> <p>Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>neighbor-router</b> &lt;NBR router ID (IP address)&gt;</p> <p>Configures the router ID of the virtual neighbor. The default setting is 0.0.0.0.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>retransmit-interval</b> &lt;1-1800&gt;</p> <p>Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is five seconds.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>transmit-delay</b> &lt;1-1800&gt;</p> <p>Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>no area-virtual-link</b> &lt;1-3&gt;</p> <p>Deletes OSPF virtual link.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>show ipv6 ospf area-virtual-link</b></p> <p>Displays the current OSPFv3 virtual link settings.</p> <p><b>Command mode:</b> All</p>



## OSPFv3 over IPsec for Virtual Link Configuration

The following table describes the OSPFv3 over IPsec for Virtual Link Configuration commands.

**Table 293.** *Layer 3 IPsec Configuration Options*

Command Syntax and Usage
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>authentication ipsec</b> {default enable spi &lt;256-4294967295&gt;}</p> <p>Sets OSPFv3 authentication mode.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>authentication ipsec spi</b> &lt;256-4294967295&gt; {md5 &lt;md5 key&gt; sha1 &lt;sha1 key&gt;}</p> <p>Configures the OSPFv3 security parameter index authentication.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>encryption ipsec</b> {default enable spi &lt;256-4294967295&gt;}</p> <p>Sets OSPFv3 encryption.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>area-virtual-link</b> &lt;1-3&gt; <b>encryption ipsec spi</b> &lt;256-4294967295&gt; <b>esp</b> {3des &lt;3des key&gt; aes-cbc &lt;aes-cbc key&gt; null} {md5 none sha1}</p> <p>Configures the OSPFv3 security parameter index encryption.</p> <p><b>Command mode:</b> Router OSPF3</p>
<p><b>show ipv6 ospf area-virtual-link</b></p> <p>Displays the current OSPFv3 virtual link settings.</p> <p><b>Command mode:</b> All</p>

## OSPFv3 Host Entry Configuration

The following table describes the OSPFv3 Host Entry commands.

**Table 294.** *OSPFv3 Host Entry Configuration Options*

Command Syntax and Usage
<b>host</b> <1-128> <b>address</b> <IPv6 address> <prefix length (1-128)> Configures the base IPv6 address and the subnet prefix length for the host entry. <b>Command mode:</b> Router OSPF3
<b>host</b> <1-128> <b>area</b> <area index (0-2)> Configures the area index of the host. <b>Command mode:</b> Router OSPF3
<b>host</b> <1-128> <b>cost</b> <1-65535> Configures the cost value of the host. <b>Command mode:</b> Router OSPF3
<b>[no] host</b> <1-128> <b>enable</b> Enables or disables the host entry. <b>Command mode:</b> Router OSPF3
<b>no host</b> <1-128> Deletes the host entry. <b>Command mode:</b> Router OSPF3
<b>show ipv6 ospf host</b> [<1-128>] Displays the current OSPFv3 host entries. <b>Command mode:</b> All

## OSPFv3 Redistribute Entry Configuration

The following table describes the OSPFv3 Redistribute Entry commands.

**Table 295.** *OSPFv3 Redist Entry Configuration Options*

Command Syntax and Usage
<b>redist-config</b> <1-128> <b>address</b> <IPv6 address> <IPv6 prefix length (1-128)> Configures the base IPv6 address and the subnet prefix length for the redistribution entry. <b>Command mode:</b> Router OSPF3
<b>[no] redist-config</b> <1-128> <b>enable</b> Enables or disables the OSPFv3 redistribution entry. <b>Command mode:</b> Router OSPF3

**Table 295.** OSPFv3 Redist Entry Configuration Options

Command Syntax and Usage
<b>redist-config</b> <1-128> <b>metric-type</b> asExtttype1 asExtttype2 Configures the metric type applied to the route before it is advertised into the OSPFv3 domain. <b>Command mode:</b> Router OSPF3
<b>redist-config</b> <1-128> <b>metric-value</b> <1-16777215> Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain. <b>Command mode:</b> Router OSPF3
<b>[no] redist-config</b> <1-128> <b>tag</b> <0-4294967295> Configures the route tag. <b>Command mode:</b> Router OSPF3
<b>no redist-config</b> <1-128> Deletes the OSPFv3 redistribution entry. <b>Command mode:</b> Router OSPF3
<b>show ipv6 ospf redist-config</b> Displays the current OSPFv3 redistribution configuration entries. <b>Command mode:</b> Router OSPF3

## OSPFv3 Redistribute Configuration

The following table describes the OSPFv3 Redistribute commands.

**Table 296.** OSPFv3 Redistribute Configuration Options

Command Syntax and Usage
<b>[no] redistribute {connected static} export</b> <metric value (1-16777215)> <metric type (1-2)> <tag (0-4294967295)> Exports the routes of this protocol as external OSPFv3 AS-external LSAs in which the metric, metric type, and route tag are specified. To remove a previous configuration and stop exporting the routes of the protocol, use the no form of the command. <b>Command mode:</b> Router OSPF3
<b>show ipv6 ospf</b> Displays the current OSPFv3 route redistribution settings. <b>Command mode:</b> All

## Border Gateway Protocol Configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it's called internal BGP (iBGP). When run between different autonomous systems, it's called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current Enterprise NOS implementation, the EN4093R 10Gb Ethernet Scalable Switch does not advertise BGP routes that are learned from one iBGP *speaker* to another iBGP *speaker*.

BGP is turned off by default.

**Note:** Fixed routes are subnet routes. There is one fixed route per IP interface.

**Table 297.** *Border Gateway Protocol Commands*

<b>Command Syntax and Usage</b>
<b>router bgp</b> Enter Router BGP configuration mode. <b>Command mode:</b> Global configuration
<b>as</b> <0-65535> Set Autonomous System number. <b>Command mode:</b> Router BGP
<b>[no] asn4comp</b> Enables or disables ASN4 to ASN2 compatibility. <b>Command mode:</b> Router BGP
<b>[no] enable</b> Globally enables or disables BGP. <b>Command mode:</b> Router BGP
<b>local-preference</b> <0-4294967294> Sets the local preference. The path with the higher value is preferred. When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP. <b>Command mode:</b> Router BGP

**Table 297.** *Border Gateway Protocol Commands (continued)*

Command Syntax and Usage
<b>neighbor</b> <1-12> Configures each BGP <i>peer</i> . Each border router, within an autonomous system, exchanges routing information with routers on other external networks. To view command options, see <a href="#">page 509</a> . <b>Command mode:</b> Router BGP
<b>show ip bgp</b> Displays the current BGP configuration. <b>Command mode:</b> All

## BGP Peer Configuration

These commands are used to configure BGP peers, which are border routers that exchange routing information with routers on internal and external networks. The peer option is disabled by default.

**Table 298.** *BGP Peer Configuration Commands*

Command Syntax and Usage
<b>neighbor</b> <1-12> <b>advertisement-interval</b> <1-65535> Sets time, in seconds, between advertisements. The default value is 60. <b>Command mode:</b> Router BGP
<b>[no] neighbor</b> <1-12> <b>passive</b> Enables or disables BGP passive mode, which prevents the switch from initiating BGP connections with peers. Instead, the switch waits for the peer to send an open message first. <b>Command mode:</b> Router BGP
<b>[no] neighbor</b> <1-12> <b>password</b> <1-16 characters> Configures the BGP peer password. <b>Command mode:</b> Router BGP
<b>neighbor</b> <peer numer (1-12)> <b>redistribute</b> Configures BGP neighbor redistribution. To view command options, see <a href="#">page 513</a> . <b>Command mode:</b> Router BGP
<b>neighbor</b> <1-12> <b>remote-address</b> <IP address> Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0 . 0 . 0 . 0. <b>Command mode:</b> Router BGP

**Table 298.** BGP Peer Configuration Commands (continued)

Command Syntax and Usage
<p><b>neighbor</b> &lt;1-12&gt; <b>remote-as</b> &lt;1-65535&gt;</p> <p>Sets the remote autonomous system number for the specified peer.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>neighbor</b> &lt;1-12&gt; <b>retry-interval</b> &lt;1-65535&gt;</p> <p>Sets connection retry interval, in seconds.</p> <p>The default value is 120.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] neighbor</b> &lt;1-12&gt; <b>route-map in</b> &lt;1-32&gt;</p> <p>Adds or removes route map into in-route map list.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] neighbor</b> &lt;1-12&gt; <b>route-map out</b> &lt;1-32&gt;</p> <p>Adds or removes route map into out-route map list.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>neighbor</b> &lt;1-12&gt; <b>route-origination-interval</b> &lt;1-65535&gt;</p> <p>Sets the minimum time between route originations, in seconds.</p> <p>The default value is 15.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>neighbor</b> &lt;1-12&gt; <b>shutdown</b></p> <p>Disables this peer configuration.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>no neighbor</b> &lt;1-12&gt; <b>shutdown</b></p> <p>Enables this peer configuration.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>neighbor</b> &lt;1-12&gt; <b>time-to-live</b> &lt;1-255&gt;</p> <p>Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded.</p> <p>This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of “hops” the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network.</p> <p>The default number is set at 1.</p> <p><b>Note:</b> The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value).</p> <p><b>Command mode:</b> Router BGP</p>

**Table 298.** BGP Peer Configuration Commands (continued)

Command Syntax and Usage
<p><b>neighbor</b> &lt;1-12&gt; <b>timers hold-time</b> &lt;0, 3-65535&gt;</p> <p>Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer.</p> <p>The default value is 180.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>neighbor</b> &lt;1-12&gt; <b>timers keep-alive</b> &lt;0, 1-21845&gt;</p> <p>Sets the keep-alive time for the specified peer, in seconds.</p> <p>The default value is 60.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>neighbor</b> &lt;1-12&gt; <b>update-source</b> {&lt;interface number&gt; <b>loopback</b> &lt;1-5&gt;}</p> <p>Sets the source interface number for this peer.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>no neighbor</b> &lt;1-12&gt;</p> <p>Deletes this peer configuration.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>show ip bgp neighbor</b> [&lt;1-12&gt;]</p> <p>Displays the current BGP peer configuration.</p> <p><b>Command mode:</b> All</p>

## BGP Aggregation Configuration

These commands enable you to configure BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

**Table 299.** BGP Aggregation Configuration Commands

Command Syntax and Usage
<p><b>aggregate-address</b> &lt;1-16&gt; &lt;IP address&gt; &lt;IP netmask&gt;</p> <p>Defines the starting subnet IP address for this aggregation, using dotted decimal notation.</p> <p>The default address is 0 . 0 . 0 . 0.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] aggregate-address</b> &lt;1-16&gt; <b>enable</b></p> <p>Enables or disables this BGP aggregation.</p> <p><b>Command mode:</b> Router BGP</p>

**Table 299.** *BGP Aggregation Configuration Commands*

<b>Command Syntax and Usage</b>
<b>no aggregate-address</b> <1-16> Deletes this BGP aggregation. <b>Command mode:</b> Router BGP
<b>show ip bgp aggregate-address</b> [<1-16>] Displays the current BGP aggregation configuration. <b>Command mode:</b> All



## BGP Neighbor Redistribution Configuration

This menu enables you to redistribute routes learned from various routing information sources into BGP.

**Table 300.** BGP Redistribution Configuration Commands

Command Syntax and Usage
<p><b>[no] neighbor &lt;1-12&gt; redistribute default-action {import originate redistribute}</b></p> <p>Sets default route action. Defaults routes can be configured as import, originate, redistribute, or none.</p> <p><b>None:</b> No routes are configured.</p> <p><b>Import:</b> Import these routes.</p> <p><b>Originate:</b> The switch sends a default route to peers if it does not have any default routes in its routing table.</p> <p><b>Redistribute:</b> Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] neighbor &lt;1-12&gt; redistribute default-metric &lt;1-4294967294&gt;</b></p> <p>Sets default metric of advertised routes.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] neighbor &lt;1-12&gt; redistribute fixed</b></p> <p>Enables or disables advertising fixed routes.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] neighbor &lt;1-12&gt; redistribute ospf</b></p> <p>Enables or disables advertising OSPF routes.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] neighbor &lt;1-12&gt; redistribute rip</b></p> <p>Enables or disables advertising RIP routes.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>[no] neighbor &lt;1-12&gt; redistribute static</b></p> <p>Enables or disables advertising static routes.</p> <p><b>Command mode:</b> Router BGP</p>
<p><b>show ip bgp neighbor &lt;1-12&gt; redistribute</b></p> <p>Displays current redistribution configuration.</p> <p><b>Command mode:</b> All</p>

## Multicast Listener Discovery Protocol Configuration

Table 301 describes the commands used to configure MLD parameters.

**Table 301.** *MLD Protocol Configuration Commands*

Command Syntax and Usage
<b>ipv6 mld</b> Enter MLD global configuration mode. <b>Command mode:</b> Global configuration
<b>default</b> Resets MLD parameters to their default values. <b>Command mode:</b> MLD Configuration
<b>[no] enable</b> Globally enables or disables MLD. <b>Command mode:</b> MLD Configuration
<b>exit</b> Exit from MLD configuration mode. <b>Command mode:</b> MLD Configuration
<b>show ipv6 mld</b> Displays the current MLD configuration parameters. <b>Command mode:</b> All

### MLD Interface Configuration

Table 302 describes the commands used to configure MLD parameters for an interface.

**Table 302.** *MLD Interface Configuration Commands*

Command Syntax and Usage
<b>ipv6 mld default</b> Resets MLD parameters for the selected interface to their default values. <b>Command mode:</b> Interface IP
<b>ipv6 mld dmrtr {enable disable}</b> Enables or disables dynamic Mrouter learning on the interface. The default setting is disabled. <b>Command mode:</b> Interface IP
<b>[no] ipv6 mld enable</b> Enables or disables this MLD interface. <b>Command mode:</b> Interface IP

**Table 302.** MLD Interface Configuration Commands (continued)

Command Syntax and Usage
<p><b>ipv6 mld llistnr</b> &lt;1-32&gt;</p> <p>Configures the Last Listener query interval, in seconds. The default value is 1.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 mld qinterval</b> &lt;2-65535&gt;</p> <p>Configures the interval for MLD Query Reports, in seconds. The default value is 125.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 mld qri</b> &lt;1000-65535&gt;</p> <p>Configures the interval for MLD Query Response Reports, in milliseconds. The default value is 10,000.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 mld robust</b> &lt;2-10&gt;</p> <p>Configures the MLD Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 mld version</b> &lt;1-2&gt;</p> <p>Defines the MLD protocol version number.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>show ipv6 mld interface</b> &lt;interface number&gt;</p> <p>Displays the current MLD interface configuration.</p> <p><b>Command mode:</b> All</p>

## IGMP Configuration

[Table 303](#) describes the commands used to configure basic IGMP parameters.

**Table 303.** *IGMP Configuration Commands*

Command Syntax and Usage
<b>[no] ip igmp aggregate</b> Enables or disables IGMP Membership Report aggregation. <b>Command mode:</b> Global configuration
<b>[no] ip igmp enable</b> Globally enables or disables IGMP. <b>Command mode:</b> Global configuration
<b>show ip igmp</b> Displays the current IGMP configuration parameters. <b>Command mode:</b> All

The following sections describe the IGMP configuration options.

- [“IGMP Snooping Configuration” on page 517](#)
- [“IGMPv3 Configuration” on page 518](#)
- [“IGMP Relay Configuration” on page 519](#)
- [“IGMP Relay Multicast Router Configuration” on page 521](#)
- [“IGMP Static Multicast Router Configuration” on page 522](#)
- [“IGMP Filtering Configuration” on page 519](#)
- [“IGMP Advanced Configuration” on page 523](#)
- [“IGMP Querier Configuration” on page 524](#)

## IGMP Snooping Configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

[Table 304](#) describes the commands used to configure IGMP Snooping.

**Table 304.** *IGMP Snooping Configuration Commands*

Command Syntax and Usage
<b>[no] ip igmp snoop enable</b> Enables or disables IGMP Snooping. <b>Command mode:</b> Global configuration
<b>ip igmp snoop source-ip &lt;IP address&gt;</b> Configures the source IP address used as a proxy for IGMP Group Specific Queries. <b>Command mode:</b> Global configuration
<b>[no] ip igmp snoop vlan &lt;VLAN number&gt;</b> Adds or removes the selected VLAN(s) to IGMP Snooping. <b>Command mode:</b> Global configuration
<b>no ip igmp snoop vlan all</b> Removes all VLANs from IGMP Snooping. <b>Command mode:</b> Global configuration
<b>ip igmp snoop mrouter-timeout &lt;1-600&gt;</b> Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255. <b>Command mode:</b> Global configuration
<b>show ip igmp snoop</b> Displays the current IGMP Snooping parameters. <b>Command mode:</b> All

## IGMPv3 Configuration

Table 305 describes the commands used to configure IGMP version 3.

**Table 305.** IGMP version 3 Configuration Commands

Command Syntax and Usage
<p><b>[no] ip igmp snoop igmpv3 enable</b></p> <p>Enables or disables IGMP version 3. The default setting is disabled. <b>Command mode:</b> Global configuration</p>
<p><b>[no] ip igmp snoop igmpv3 exclude</b></p> <p>Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default setting is enabled. <b>Command mode:</b> Global configuration</p>
<p><b>ip igmp snoop igmpv3 sources &lt;1-64&gt;</b></p> <p>Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8. <b>Command mode:</b> Global configuration</p>
<p><b>[no] ip igmp snoop igmpv3 v1v2</b></p> <p>Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default setting is enabled. <b>Command mode:</b> Global configuration</p>
<p><b>show ip igmp snoop igmpv3</b></p> <p>Displays the current IGMP v3 Snooping configuration. <b>Command mode:</b> All</p>

## IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

[Table 306](#) describes the commands used to configure IGMP Relay.

**Table 306.** *IGMP Relay Configuration Commands*

Command Syntax and Usage
<b>[no] ip igmp relay enable</b> Enables or disables IGMP Relay. <b>Command mode:</b> Global configuration
<b>ip igmp relay report &lt;0-150&gt;</b> Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10. <b>Command mode:</b> Global configuration
<b>[no] ip igmp relay vlan &lt;VLAN number&gt;</b> Adds or removes the VLAN to the list of IGMP Relay VLANs. <b>Command mode:</b> Global configuration
<b>show ip igmp relay</b> Displays the current IGMP Relay configuration. <b>Command mode:</b> All

## IGMP Filtering Configuration

[Table 307](#) describes the commands used to configure an IGMP filter.

**Table 307.** *IGMP Filtering Configuration Commands*

Command Syntax and Usage
<b>ip igmp profile &lt;1-16&gt;</b> Configures the IGMP filter. To view command options, see <a href="#">page 520</a> . <b>Command mode:</b> Global configuration
<b>[no] ip igmp filtering</b> Enables or disables IGMP filtering globally. <b>Command mode:</b> Global configuration
<b>show ip igmp filtering</b> Displays the current IGMP Filtering parameters. <b>Command mode:</b> All

## IGMP Filter Definition

Table 308 describes the commands used to define an IGMP filter.

**Table 308.** IGMP Filter Definition Commands

Command Syntax and Usage
<b>ip igmp profile</b> <1-16> <b>action</b> {allow deny} Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny. <b>Command mode:</b> Global configuration
<b>[no] ip igmp profile</b> <1-16> <b>enable</b> Enables or disables this IGMP filter. <b>Command mode:</b> Global configuration
<b>ip igmp profile</b> <1-16> <b>range</b> <IP address 1> <IP address 2> Configures the range of IP multicast addresses for this filter. <b>Command mode:</b> Global configuration
<b>no ip igmp profile</b> <1-16> Deletes this filter's parameter definitions. <b>Command mode:</b> Global configuration
<b>show ip igmp profile</b> <1-16> Displays the current IGMP filter. <b>Command mode:</b> All

## IGMP Filtering Port Configuration

Table 309 describes the commands used to configure a port for IGMP filtering.

**Table 309.** IGMP Filter Port Configuration Commands

Command Syntax and Usage
<b>[no] ip igmp filtering</b> Enables or disables IGMP filtering on this port. <b>Command mode:</b> Interface port
<b>[no] ip igmp profile</b> <1-16> Adds or removes an IGMP filter to this port. <b>Command mode:</b> Interface port
<b>show interface port</b> <port alias or number> <b>igmp-filtering</b> Displays the current IGMP filter parameters for this port. <b>Command mode:</b> All



## IGMP Relay Multicast Router Configuration

Table 310 describes the commands used to configure multicast routers for IGMP Relay.

**Table 310.** IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage
<p><b>ip igmp relay mrouter</b> &lt;1-2&gt; <b>address</b> &lt;IP address&gt;</p> <p>Configures the IP address of the IGMP multicast router used for IGMP Relay.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp relay mrouter</b> &lt;1-2&gt; <b>attempt</b> &lt;1-128&gt;</p> <p>Configures the number of successful ping attempts required before the switch declares this Mrouter is up.</p> <p>The default value is 5.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip igmp relay mrouter</b> &lt;1-2&gt; <b>enable</b></p> <p>Enables or disables the multicast router.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp relay mrouter</b> &lt;1-2&gt; <b>interval</b> &lt;1-60&gt;</p> <p>Configures the time interval between ping attempts to the upstream Mrouters, in seconds.</p> <p>The default value is 2.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp relay mrouter</b> &lt;1-2&gt; <b>retry</b> &lt;1-120&gt;</p> <p>Configures the number of failed ping attempts required before the switch declares this Mrouter is down.</p> <p>The default value is 4.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp relay mrouter</b> &lt;1-2&gt; <b>version</b> &lt;1-2&gt;</p> <p>Configures the IGMP version (1 or 2) of the multicast router.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip igmp relay mrouter</b> &lt;1-2&gt;</p> <p>Deletes the multicast router from IGMP Relay.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip igmp relay</b></p> <p>Displays the current IGMP Relay configuration.</p> <p><b>Command mode:</b> All</p>

## IGMP Static Multicast Router Configuration

Table 311 describes the commands used to configure a static multicast router.

**Note:** When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

**Table 311.** IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage
<p><b>ip igmp mrouter port</b> &lt;port alias or number&gt; &lt;VLAN number&gt; &lt;version (1-3)&gt;</p> <p>Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2 or 3) of the multicast router.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip igmp mrouter port</b> &lt;port alias or number&gt; &lt;VLAN number&gt; &lt;version (1-3)&gt;</p> <p>Removes a static multicast router from the selected port/VLAN combination.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip igmp mrouter all</b></p> <p>Removes all static multicast routers.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>clear ip igmp mrouter</b></p> <p>Clears the Dynamic router port table.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip igmp mrouter</b></p> <p>Displays the current IGMP Static Multicast Router parameters.</p> <p><b>Command mode:</b> All</p>

## IGMP Advanced Configuration

Table 312 describes the commands used to configure advanced IGMP parameters.

**Table 312.** IGMP Advanced Configuration Commands

Command Syntax and Usage
<p><b>[no] ip igmp fastleave</b> &lt;VLAN number&gt;</p> <p>Enables or disables Fastleave processing. Fastleave lets the switch immediately remove a port from the IGMP port list if the host sends a Leave message and the proper conditions are met.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp query-interval</b> &lt;1-600&gt;</p> <p>Sets the IGMP router query interval, in seconds.</p> <p>The default value is 125.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp robust</b> &lt;1-10&gt;</p> <p>Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If you expect the subnet to have a high rate of packet loss, increase the value.</p> <p>The default value is 2.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip igmp rtralert</b></p> <p>Enables or disables the Router Alert option in IGMP messages.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp timeout</b> &lt;1-255&gt;</p> <p>Configures the Query Response Interval. This is a value used to determine the Group Membership Interval, together with the Robustness Variable and the Query Interval. The range is from 1 to 255 seconds.</p> <p>The default value is 10.</p> <p><b>Command mode:</b> Global configuration</p>

## IGMP Querier Configuration

Table 313. describes the commands used to configure IGMP Querier.

**Table 313.** IGMP Querier Configuration Options

Command Syntax and Usage
<p><b>[no] ip igmp querier enable</b> Globally enables or disables IGMP Querier. <b>Command mode:</b> Global configuration</p>
<p><b>[no] ip igmp querier vlan &lt;VLAN number&gt; enable</b> Enables or disables the IGMP Querier for the specified VLAN. <b>Command mode:</b> Global configuration</p>
<p><b>ip igmp querier vlan &lt;VLAN number&gt; election-type [ipv4 mac]</b> Sets the IGMP Querier election criteria as IP address or Mac address. The default setting is IPv4. <b>Command mode:</b> Global configuration</p>
<p><b>ip igmp querier vlan &lt;VLAN number&gt; max-response &lt;1-256&gt;</b> Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. By varying the Query Response Interval, an administrator may tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval. The default value is 100. <b>Command mode:</b> Global configuration</p>
<p><b>ip igmp querier vlan &lt;VLAN number&gt; query-interval &lt;1-608&gt;</b> Configures the interval between IGMP Query broadcasts, in seconds. The default value is 125. <b>Command mode:</b> Global configuration</p>
<p><b>ip igmp querier vlan &lt;VLAN number&gt; robustness &lt;1-10&gt;</b> Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is 2. <b>Command mode:</b> Global configuration</p>
<p><b>ip igmp querier vlan &lt;VLAN number&gt; source-ip &lt;IP address&gt;</b> Configures the IGMP source IP address for the selected VLAN. <b>Command mode:</b> Global configuration</p>

**Table 313.** IGMP Querier Configuration Options (continued)

Command Syntax and Usage
<p><b>ip igmp querier vlan</b> &lt;VLAN number&gt; <b>startup-count</b> &lt;1-10&gt;</p> <p>Configures the Startup Query Count, which is the number of IGMP Queries sent out at startup. Each Query is separated by the Startup Query Interval. The default value is 2.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp querier vlan</b> &lt;VLAN number&gt; <b>startup-interval</b> &lt;1-608&gt;</p> <p>Configures the Startup Query Interval, which is the interval between General Queries sent out at startup. The default value is 31 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip igmp querier vlan</b> &lt;VLAN number&gt; <b>version</b> [v1 v2 v3]</p> <p>Configures the IGMP version. The default version is v3.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip igmp querier</b></p> <p>Displays the current IGMP Querier parameters.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp querier vlan</b> &lt;VLAN number&gt;</p> <p>Displays IGMP Querier information for the selected VLAN.</p> <p><b>Command mode:</b> Global configuration</p>

## IKEv2 Configuration

Table 314 describes the commands used to configure IKEv2.

**Table 314.** *IKEv2 Options*

Command Syntax and Usage
<b>[no] ikev2 cookie</b> Enables or disables cookie notification. <b>Command mode:</b> Global configuration
<b>ikev2 retransmit-interval</b> <1-20> Sets the interval, in seconds, the timeout value in case a packet is not received by the peer and needs to be retransmitted. The default value is 20. <b>Command mode:</b> Global configuration
<b>show ikev2</b> Displays the current IKEv2 settings. <b>Command mode:</b> All

## IKEv2 Proposal Configuration

Table 315 describes the commands used to configure an IKEv2 proposal.

**Table 315.** *IKEv2 Proposal Options*

Command Syntax and Usage
<b>ikev2 proposal</b> Enter IKEv2 proposal mode. <b>Command mode:</b> Global configuration
<b>encryption {3des aes-cbc}</b> Configures IKEv2 encryption mode. The default value is 3des. <b>Command mode:</b> IKEv2 proposal
<b>group {24}</b> Configures the the DH group. The default group is 24. <b>Command mode:</b> IKEv2 proposal
<b>integrity {sha1}</b> Configures the IKEv2 authentication algorithm type. The default value is sha1. <b>Command mode:</b> IKEv2 proposal

## IKEv2 Preshare Key Configuration

Table 316 describes the commands used to configure IKEv2 preshare keys.

**Table 316.** *IKEv2 Preshare Key Options*

Command Syntax and Usage
<b>ikev2 preshare-key local</b> <1-32 characters> Configures the local preshare key. The default value is <code>ibm123</code> . <b>Command mode:</b> Global configuration
<b>ikev2 preshare-key remote</b> <1-32 characters> <IPv6 address> Configures the remote preshare key for the IPv6 address. <b>Command mode:</b> Global configuration
<b>show ikev2 preshare-key</b> Displays the current IKEv2 Preshare key settings. <b>Command mode:</b> Global configuration

## IKEv2 Identification Configuration

Table 317 describes the commands used to configure IKEv2 identification.

**Table 317.** *IKEv2 Identification Options*

Command Syntax and Usage
<b>ikev2 identity local address</b> Configures the switch to use the supplied IPv6 address as identification. <b>Command mode:</b> Global configuration
<b>ikev2 identity local email</b> <1-32 characters> Configures the switch to use the supplied email address (such as "xyz@example.com") as identification. <b>Command mode:</b> Global configuration
<b>ikev2 identity local fqdn</b> <1-32 characters> Configures the switch to use the fully-qualified domain name (such as "example.com") as identification. <b>Command mode:</b> Global configuration
<b>show ikev2 identity</b> Displays the current IKEv2 identification settings. <b>Command mode:</b> All

## IPsec Configuration

Table 318 describes the commands used to configure IPsec.

**Table 318.** *IPsec Options*

Command Syntax and Usage
<p><b>[no] ipsec enable</b>            Enables or disables IPsec.  <b>Command mode:</b> Global configuration</p>
<p><b>show ipsec</b>            Displays the current IPsec settings.  <b>Command mode:</b> All</p>

## IPsec Transform Set Configuration

Table 319 describes the commands used to configure IPsec transforms.

**Table 319.** *IPsec Transform Set Options*

Command Syntax and Usage
<p><b>ipsec transform-set &lt;1-10&gt; {ah-sha1 esp-3des              esp-aes-cbc esp-null}</b>            Sets the AH or ESP authentication, encryption, or integrity algorithm. The available algorithms are as follows:</p> <ul style="list-style-type: none"> <li>o ah-md5</li> <li>o ah-sha1</li> <li>o esp-3des</li> <li>o esp-aes-cbc</li> <li>o esp-des</li> <li>o esp-md5</li> <li>o esp-null</li> <li>o esp</li> <li>o sha1</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>ipsec transform-set &lt;1-10&gt; transport {ah-md5 ah-sha1              esp-3des esp-aes-cbc esp-md5 esp-null}</b>            Sets transport mode and the AH or ESP authentication, encryption, or integrity algorithm.  <b>Command mode:</b> Global configuration</p>
<p><b>ipsec transform-set &lt;1-10&gt; tunnel {ah-md5 ah-sha1 esp-3des              esp-aes-cbc esp-md5 esp-null}</b>            Sets tunnel mode and the AH or ESP authentication, encryption, or integrity algorithm.  <b>Command mode:</b> Global configuration</p>



**Table 319.** *IPsec Transform Set Options (continued)*

Command Syntax and Usage
<b>no ipsec transform</b> <1-10> Deletes the transform set. <b>Command mode:</b> Global configuration
<b>show ipsec transform-set</b> <1-10> Displays the current IPsec Transform Set settings. <b>Command mode:</b> All

## IPsec Traffic Selector Configuration

[Table 320](#) describes the commands used to configure an IPsec traffic selector.

**Table 320.** *IPsec Traffic Selector Options*

Command Syntax and Usage
<b>ipsec traffic-selector</b> <1-10> { <b>permit deny</b> } { <b>any icmp tcp</b> } {<IPv6 address>  <b>any</b> } Sets the traffic selector to permit or deny the specified type of traffic. <b>Command mode:</b> Global configuration
<b>no ipsec traffic-selector</b> <1-10> Resets the specified traffic selector to its default settings. <b>Command mode:</b> Global configuration

## IPsec Dynamic Policy Configuration

[Table 321](#) describes the commands used to configure an IPsec dynamic policy.

**Table 321.** *IPsec Dynamic Policy Options*

Command Syntax and Usage
<b>ipsec dynamic-policy</b> <1-10> Enter IPsec dynamic policy mode. <b>Command mode:</b> Global configuration
<b>peer</b> <IPv6 address> Sets the remote peer IP address. <b>Command mode:</b> IPsec dynamic policy
<b>pfs</b> { <b>enable disable</b> } Enables/disables perfect forward security. <b>Command mode:</b> IPsec dynamic policy

**Table 321.** *IPsec Dynamic Policy Options (continued)*

<b>Command Syntax and Usage</b>
<b>sa-lifetime</b> <120-86400> Sets the IPsec SA lifetime in seconds. The default value is 86400. <b>Command mode:</b> IPsec dynamic policy
<b>traffic-selector</b> <1-10> Sets the traffic selector for the IPsec policy. <b>Command mode:</b> IPsec dynamic policy
<b>transform-set</b> <1-10> Sets the transform set for the IPsec policy. <b>Command mode:</b> IPsec dynamic policy
<b>show ipsec dynamic-policy</b> <1-10> Displays the current IPsec dynamic policy settings. <b>Command mode:</b> All

## *IPsec Manual Policy Configuration*

[Table 322](#) describes the commands used to configure an IPsec manual policy.

**Table 322.** *IPsec Manual Policy Options*

<b>Command Syntax and Usage</b>
<b>ipsec manual-policy</b> <1-10> Enter IPsec manual policy mode. <b>Command mode:</b> Global configuration
<b>in-ah auth-key</b> <key code (hexadecimal)> Sets inbound Authentication Header (AH) authenticator key. <b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. <b>Command mode:</b> IPsec manual policy
<b>in-ah spi</b> <256-4294967295> Sets the inbound Authentication Header (AH) Security Parameter Index (SPI). <b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. <b>Command mode:</b> IPsec manual policy

**Table 322.** *IPsec Manual Policy Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>in-esp auth-key</b> &lt;key code (hexadecimal)&gt;</p> <p>Sets the inbound Encapsulating Security Payload (ESP) authenticator key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>in-esp cipher-key</b> &lt;key code (hexadecimal)&gt;</p> <p>Sets the inbound Encapsulating Security Payload (ESP) cipher key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>in-esp spi</b> &lt;256-4294967295&gt;</p> <p>Sets the inbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI).</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>out-ah auth-key</b> &lt;key code (hexadecimal)&gt;</p> <p>Sets the outbound Authentication Header (AH) authenticator key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>out-ah spi</b> &lt;256-4294967295&gt;</p> <p>Sets the outbound Authentication Header (AH) Security Parameter Index (SPI).</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>out-esp auth-key</b> &lt;key code (hexadecimal)&gt;</p> <p>Sets the outbound Encapsulating Security Payload (ESP) authenticator key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>

**Table 322.** *IPsec Manual Policy Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>out-esp cipher-key</b> &lt;<i>key code (hexadecimal)</i>&gt;</p> <p>Sets the outbound Encapsulating Security Payload (ESP) cipher key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>out-esp spi</b> &lt;<i>256-4294967295</i>&gt;</p> <p>Sets the outbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI).</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>peer</b> &lt;<i>IPv6 address</i>&gt;</p> <p>Sets the remote peer IP address.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>traffic-selector</b> &lt;<i>1-10</i>&gt;</p> <p>Sets the traffic selector for the IPsec policy.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>transform-set</b> &lt;<i>1-10</i>&gt;</p> <p>Sets the transform set for the IPsec policy.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<p><b>show ipsec manual-policy</b> &lt;<i>1-10</i>&gt;</p> <p>Displays the current IPsec manual policy settings.</p> <p><b>Command mode:</b> All</p>

## Domain Name System Configuration

The Domain Name System (DNS) commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `tracert`, and `tftp` commands.

**Table 323.** *Domain Name Service Commands*

Command Syntax and Usage
<p><b>[no] ip dns domain-name</b> &lt;string&gt;</p> <p>Sets the default domain name used by the switch.</p> <p>For example: <code>mycompany.com</code></p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip dns primary-server</b> &lt;IP address&gt;</p> <p>You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip dns secondary-server</b> &lt;IP address&gt;</p> <p>You are prompted to set the IPv4 address for your secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip dns ipv6 primary-server</b> &lt;IP address&gt;</p> <p>You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ip dns ipv6 secondary-server</b> &lt;IP address&gt;</p> <p>You are prompted to set the IPv6 address for your secondary DNS server, using hexadecimal format with colons. If the primary DNS server fails, the configured secondary will be used instead.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip dns ipv6 request-version</b> {ipv4 ipv6}</p> <p>Sets the protocol used for the first request to the DNS server, as follows:</p> <ul style="list-style-type: none"> <li>o IPv4</li> <li>o IPv6</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip dns</b></p> <p>Displays the current Domain Name System settings.</p> <p><b>Command mode:</b> All</p>

## Bootstrap Protocol Relay Configuration

The Bootstrap Protocol (BOOTP) Relay commands are used to let hosts get their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the EN4093R.

BOOTP relay is turned off by default.

**Table 324.** *Global BOOTP Relay Configuration Options*

Command Syntax and Usage
<b>[no] ip bootp-relay server &lt;1-4&gt; address &lt;IP address&gt;</b> Sets the IP address of the selected global BOOTP server. <b>Command mode:</b> Global configuration
<b>[no] ip bootp-relay enable</b> Globally enables or disables BOOTP relay. <b>Command mode:</b> Global configuration

## BOOTP Relay Broadcast Domain Configuration

These commands allow you to configure a BOOTP server for a specific broadcast domain, based on its associated VLAN.

**Table 325.** *BOOTP Relay Broadcast Domain Configuration Options*

Command Syntax and Usage
<b>[no] ip bootp-relay bcst-domain &lt;1-10&gt; enable</b> Enables or disables BOOTP Relay for the broadcast domain. When disabled, BOOTP Relay is performed by one of the global BOOTP servers. <b>Command mode:</b> Global configuration
<b>ip bootp-relay bcst-domain &lt;1-10&gt; server &lt;1-4&gt; address &lt;IPv4 address&gt;</b> Sets the IP address of the BOOTP server. <b>Command mode:</b> Global configuration
<b>ip bootp-relay bcst-domain &lt;1-10&gt; vlan &lt;VLAN number&gt;</b> Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN. <b>Command mode:</b> Global configuration
<b>no ip bootp-relay bcst-domain &lt;1-10&gt;</b> Deletes the selected broadcast domain configuration. <b>Command mode:</b> Global configuration
<b>show ip bootp-relay</b> Displays the current parameters for the BOOTP Relay broadcast domain. <b>Command mode:</b> All

## VRRP Configuration

Virtual Router Redundancy Protocol (VRRP) support on the EN4093R provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. Enterprise NOS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the “High Availability” chapter in the *Enterprise NOS 8.4 Application Guide*.

**Table 326.** *Virtual Router Redundancy Protocol Commands*

<b>Command Syntax and Usage</b>
<b>router vrrp</b> Enter Router VRRP configuration mode. <b>Command mode:</b> Global configuration
<b>[no] enable</b> Globally enables or disables VRRP on this switch. <b>Command mode:</b> Router VRRP
<b>group</b> Configures VRRP virtual routers groups. To view command options, see <a href="#">page 540</a> . <b>Command mode:</b> Router VRRP
<b>holdoff &lt;0-255&gt;</b> Globally sets the time, in seconds, VRRP waits from when the master switch goes down until elevating a new switch to be the master switch. <b>Command mode:</b> Router VRRP
<b>[no] hot-standby</b> Enables or disables hot standby processing, in which two or more switches provide redundancy for each other. By default, this option is disabled. <b>Command mode:</b> Router VRRP
<b>interface &lt;interface number&gt;</b> Configures VRRP authentication parameters for the IP interfaces used with the virtual routers. To view command options, see <a href="#">page 543</a> . <b>Command mode:</b> Router VRRP

**Table 326.** *Virtual Router Redundancy Protocol Commands*

<b>Command Syntax and Usage</b>
<p><b>tracking-priority-increment</b></p> <p>Configures weights for the various criteria used to modify priority levels during the master router election process. To view command options, see <a href="#">page 544</a>.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>virtual-router</b> &lt;1-128&gt;</p> <p>Configures virtual routers for the switch. To view command options, see <a href="#">page 537</a>.</p> <p>Command mode: Router VRRP</p>
<p><b>show ip vrrp</b></p> <p>Displays the current VRRP parameters.</p> <p><b>Command mode:</b> All</p>



## Virtual Router Configuration

These commands are used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

**Table 327.** VRRP Virtual Router Configuration Commands

Command Syntax and Usage
<p><b>[no] virtual-router &lt;1-128&gt; address &lt;IP address&gt;</b></p> <p>Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the VRID (above) to configure the same virtual router on each participating VRRP device.</p> <p>The default address is 0 . 0 . 0 . 0.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>[no] virtual-router &lt;1-128&gt; enable</b></p> <p>Enables or disables this virtual router.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>virtual-router &lt;1-128&gt; interface &lt;interface number&gt;</b></p> <p>Selects a switch IP interface. If the IP interface has the same IP address as the <b>addr</b> option above, this switch is considered the “owner” of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the <b>preem</b> option below is disabled.</p> <p>The default value is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>[no] virtual-router &lt;1-128&gt; preemption</b></p> <p>Enables or disables master preemption. When <b>enabled</b>, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when <b>preemption</b> is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router <b>addr</b> are the same).</p> <p>The default setting is enabled.</p> <p><b>Command mode:</b> Router VRRP</p>

**Table 327.** VRRP Virtual Router Configuration Commands (continued)

Command Syntax and Usage
<p><b>virtual-router</b> &lt;1-128&gt; <b>priority</b> &lt;1-254&gt;</p> <p>Defines the election priority bias for this virtual server. The priority value can be any integer between 1 and 254.</p> <p>During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).</p> <p>When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.</p> <p>The default value is 100.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>virtual-router</b> &lt;1-128&gt; <b>timers advertise</b> &lt;1-255&gt;</p> <p>Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds.</p> <p>The default value is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>virtual-router</b> &lt;1-128&gt; <b>track</b></p> <p>Enables the priority system used when electing the master router from a pool of virtual routers. To view command options, see <a href="#">page 539</a>.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>virtual-router</b> &lt;1-128&gt; <b>virtual-router-id</b> &lt;1-255&gt;</p> <p>Defines the virtual router ID (VRID). This is used in conjunction with the [no] <b>virtual-router</b> &lt;128&gt; <b>address</b> &lt;IP address&gt; command below to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router.</p> <p>The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255.</p> <p>The default value is 1.</p> <p><b>Note:</b> All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>no virtual-router</b> &lt;1-128&gt;</p> <p>Deletes this virtual router from the switch configuration.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>show ip vrrp virtual-router</b> &lt;1-128&gt;</p> <p>Displays the current configuration information for this virtual router.</p> <p><b>Command mode:</b> All</p>

## Virtual Router Priority Tracking Configuration

These commands are used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking commands.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria apply to standard virtual routers, otherwise called “virtual interface routers.” A virtual *server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

**Table 328.** VRRP Priority Tracking Configuration Commands

Command Syntax and Usage
<p><b>[no] virtual-router &lt;1-128&gt; track interfaces</b></p> <p>When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master.</p> <p>This command is disabled by default.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>[no] virtual-router &lt;1-128&gt; track ports</b></p> <p>When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master.</p> <p>This command is disabled by default.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>[no] virtual-router &lt;1-128&gt; track virtual-routers</b></p> <p>When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency.</p> <p>This command is disabled by default.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>show ip vrrp virtual-router &lt;1-128&gt; track</b></p> <p>Displays the current configuration for priority tracking for this virtual router.</p> <p><b>Command mode:</b> All</p>

## Virtual Router Group Configuration

Virtual Router Group commands are used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the EN4093R to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

**Note:** This option is required to be configured only when using at least two EN4093Rs in a hot-standby failover configuration, where only one switch is active at any time.

**Table 329.** VRRP Virtual Router Group Configuration Commands

Command Syntax and Usage
<p><b>group advertisement</b> &lt;1-255&gt;</p> <p>Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds.</p> <p>The default value is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>[no] group enable</b></p> <p>Enables or disables the virtual router group.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>group interface</b> &lt;interface number&gt;</p> <p>Selects a switch IP interface.</p> <p>The default switch IP interface number is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>group preempt-delay-time</b> &lt;0-255&gt;</p> <p>Configures the preempt delay interval (in seconds). This timer is configured on the virtual router group and prevents the switch from transitioning back to Master state until the preempt delay interval has expired. Ensure that the interval is long enough for OSPF or other routing protocols to converge.</p> <p>The default is 0 seconds.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>[no] group preemption</b></p> <p>Enables or disables master pre-emption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will pre-empt the lower priority master and assume control. Note that even when <code>preemption</code> is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router address are the same).</p> <p>The default setting is <code>enabled</code>.</p> <p><b>Command mode:</b> Router VRRP</p>

**Table 329.** VRRP Virtual Router Group Configuration Commands (continued)

<b>Command Syntax and Usage</b>	
<b>group priority</b> <1-254>	<p>Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254.</p> <p>During the master router election process, the routing device with the highest virtual router priority number wins.</p> <p>Each virtual router group is treated as one entity regardless of how many virtual routers are in the group. When the switch tracks the virtual router group, it measures the resources contained in the group (such as interfaces, VLAN ports, real servers). The priority is updated as a group. Every virtual router in the group has the same priority.</p> <p>The <i>owner</i> parameter does not apply to the virtual router group. The group itself cannot be an owner and therefore the priority is 1-254.</p> <p>The default value is 100.</p> <p><b>Command mode:</b> Router VRRP</p>
<b>group track</b>	<p>Enables the priority system used when electing the master router from a pool of virtual router groups. To view command options, see <a href="#">page 542</a>.</p> <p><b>Command mode:</b> Router VRRP</p>
<b>group virtual-router-id</b> <1-255>	<p>Defines the virtual router ID (VRID).</p> <p>The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All VRID values must be unique within the VLAN to which the virtual router's IP interface (see <a href="#">interface</a> below) belongs.</p> <p>The default virtual router ID is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
<b>no group</b>	<p>Deletes the virtual router group from the switch configuration.</p> <p><b>Command mode:</b> Router VRRP</p>
<b>show ip vrrp group</b>	<p>Displays the current configuration information for the virtual router group.</p> <p><b>Command mode:</b> All</p>

## Virtual Router Group Priority Tracking Configuration

**Note:** If *Virtual Router Group Tracking* is enabled, the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

**Table 330.** *Virtual Router Group Priority Tracking Configuration Commands*

Command Syntax and Usage
<p><b>[no] group track interfaces</b></p> <p>When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>[no] group track ports</b></p> <p>When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Router VRRP</p>
<p><b>show ip vrrp group track</b></p> <p>Displays the current configuration for priority tracking for this virtual router.</p> <p><b>Command mode:</b> All</p>

## VRRP Interface Configuration

**Note:** The *interface* represents the IP interface on which authentication parameters must be configured.

These commands are used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

**Table 331.** VRRP Interface Commands

Command Syntax and Usage
<b>interface</b> <interface number> <b>authentication</b> {password none} Defines the type of authentication that will be used: none (no authentication) or password (password authentication). <b>Command mode:</b> Router VRRP
<b>[no] interface</b> <interface number> <b>password</b> <password> Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see <b>interface authentication</b> above). <b>Command mode:</b> Router VRRP
<b>no interface</b> <interface number> Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted. <b>Command mode:</b> Router VRRP
<b>show ip vrrp interface</b> <interface number> Displays the current configuration for this IP interface's authentication parameters. <b>Command mode:</b> All

## VRRP Tracking Configuration

These commands are used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met (see “VRRP Virtual Router Priority Tracking Commands” on [page 539](#)), the priority level for the virtual router is increased by a defined amount.

**Table 332.** VRRP Tracking Configuration Commands

Command Syntax and Usage
<b>tracking-priority-increment interfaces</b> <0-254> Defines the priority increment value for active IP interfaces detected on this switch. The default value is 2. <b>Command mode:</b> Router VRRP
<b>tracking-priority-increment ports</b> <0-254> Defines the priority increment value for active ports on the virtual router’s VLAN. The default value is 2. <b>Command mode:</b> Router VRRP
<b>tracking-priority-increment virtual-routers</b> <0-254> Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2. <b>Command mode:</b> Router VRRP
<b>show ip vrrp tracking-priority-increment</b> Displays the current configuration of priority tracking increment values. <b>Command mode:</b> All

**Note:** These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Commands (see [page 539](#)) are enabled.



## Protocol Independent Multicast Configuration

The following table displays Protocol Independent Multicast configuration commands:

**Table 333.** *PIM Configuration Options*

Command Syntax and Usage
<b>ip pim component</b> <1-2> Enter PIM component mode. See <a href="#">page 546</a> to view options. <b>Command mode:</b> Global configuration
<b>[no] ip pim enable</b> Globally enables or disables PIM. <b>Command mode:</b> Global configuration
<b>[no] ip pim pmbr enable</b> Enables or disables PIM border router. The default setting is disabled. <b>Command mode:</b> Global configuration
<b>ip pim regstop-ratelimit-period</b> <0-2147483647> Configures the register stop rate limit, in seconds. The default value is 5. <b>Command mode:</b> Global configuration
<b>[no] ip pim static-rp enable</b> Enables or disables static RP configuration. The default setting is disabled. <b>Command mode:</b> Global configuration
<b>clear ip pim mroute</b> Clears PIM multicast router entries. <b>Command mode:</b> Global configuration

## PIM Component Configuration

Use these commands to configure a PIM Component:

**Table 334.** PIM Component Configuration Options

Command Syntax and Usage
<b>ip pim component</b> <1-2> Enter PIM component mode. <b>Command mode:</b> Global configuration
<b>mode {dense sparse}</b> Configures the operational mode of the PIM router (dense or sparse). <b>Command mode:</b> PIM Component
<b>show ip pim component</b> [<1-2>] Displays the current PIM component configuration settings. <b>Command mode:</b> All

## RP Candidate Configuration

Use these commands to configure a PIM router Rendezvous Point (RP) candidate.

**Table 335.** RP Candidate Configuration Options

Command Syntax and Usage
<b>rp-candidate holdtime</b> <0-255> Configures the hold time of the RP candidate, in seconds. <b>Command mode:</b> PIM Component
<b>[no] rp-candidate rp-address</b> <group multicast address> <group subnet mask> <IP address> Adds or removes an RP candidate. <b>Command mode:</b> PIM Component

## RP Static Configuration

Use these commands to configure a static PIM router Rendezvous Point (RP).

**Table 336.** RP Static Configuration Options

Command Syntax and Usage
<b>[no] rp-static rp-address</b> <group multicast address> <group subnet mask> <IP address> Adds or removes a static RP. <b>Command mode:</b> PIM Component

## PIM Interface Configuration

The following table displays PIM Interface configuration commands:

**Table 337.** PIM Interface Configuration Options

Command Syntax and Usage
<p><b>interface ip</b> &lt;interface number&gt; Enter Interface IP mode. <b>Command mode:</b> Global Configuration</p>
<p><b>[no] ip pim border-bit</b> Enables or disables the interface as a border router. The default setting is disabled. <b>Command mode:</b> Interface IP</p>
<p><b>[no] ip pim cbsr-preference</b> &lt;0-255&gt; Configures the candidate bootstrap router preference. <b>Command mode:</b> Interface IP</p>
<p><b>ip pim component-id</b> &lt;1-2&gt; Defines the component ID for the interface. <b>Command mode:</b> Interface IP</p>
<p><b>ip pim dr-priority</b> &lt;0-4294967294&gt; Configures the designated router priority. The default value is 1. <b>Command mode:</b> Interface IP</p>
<p><b>[no] ip pim enable</b> Enables or disables PIM on the interface. <b>Command mode:</b> Interface IP</p>
<p><b>ip pim hello-interval</b> &lt;0-65535&gt; Configures the time interval, in seconds, between PIM Hello packets. The default value is 30. <b>Command mode:</b> Interface IP</p>
<p><b>ip pim hello-holdtime</b> &lt;1-65535&gt; Configures the time period for which a neighbor is to consider this switch to be operative (up). The default value is 105. <b>Command mode:</b> Interface IP</p>
<p><b>ip pim join-prune-interval</b> &lt;0-65535&gt; Configures the interval between Join Prune messages, in seconds. The default value is 60. <b>Command mode:</b> Interface IP</p>

**Table 337.** PIM Interface Configuration Options (continued)

<p><b>Command Syntax and Usage</b></p>
<p><b>ip pim lan-delay</b> &lt;0-32767&gt;</p> <p>Configures the LAN delay value for the router interface, in seconds.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip pim lan-prune-delay</b></p> <p>Enables or disables LAN delay advertisements on the interface.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip pim neighbor-addr</b> &lt;IP address&gt; {allow deny}</p> <p>Allows or denies PIM access to the specified neighbor. You can configure a list of up to 72 neighbors that bypass the neighbor filter. Once you configure the interface to allow a neighbor, you can configure the interface to deny the neighbor.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>[no] ip pim neighbor-filter</b></p> <p>Enables or disables the PIM neighbor filter on the interface. When enabled, this interface does not accept any PIM neighbors, unless specifically permitted using the following command:</p> <p>ip pim neighbor-addr &lt;IP address&gt;</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ip pim override-interval</b> &lt;0-65535&gt;</p> <p>Configures the override interval for the router interface, in seconds.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>show ip pim interface</b> [&lt;interface number&gt; detail]</p> <p>Displays the current PIM interface parameters.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip pim neighbor-filters</b></p> <p>Displays the configured PIM neighbor filters.</p> <p><b>Command mode:</b> All</p>

## IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateway 1 is used for data traffic.
- Gateways 3 and 4 are used for management traffic.

[Table 338](#) describes the IPv6 Default Gateway Configuration commands.

**Table 338.** *IPv6 Default Gateway Configuration Commands*

Command Syntax and Usage
<b>ip gateway6</b> <1,3-4> <b>address</b> <IPv6 address> [ <b>enable</b> ] Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:0:abcd:12). The <b>enable</b> option also enable the default gateway. <b>Command mode:</b> Global configuration
<b>[no] ip gateway6</b> <1,3-4> <b>enable</b> Enables or disables the default gateway. <b>Command mode:</b> Global configuration
<b>no ip gateway6</b> <1,3-4> Deletes the default gateway. <b>Command mode:</b> Global configuration
<b>show ipv6 gateway6</b> <1,3-4> Displays the current IPv6 default gateway configuration. <b>Command mode:</b> All

## IPv6 Static Route Configuration

Table 339 describes the IPv6 static route configuration commands.

**Table 339.** IPv6 Static Route Configuration Commands

Command Syntax and Usage
<p><b>ip route6</b> &lt;IPv6 address&gt; &lt;prefix length&gt; &lt;IPv6 gateway address&gt; [&lt;interface number&gt;] Adds an IPv6 static route. <b>Command mode:</b> Global configuration</p>
<p><b>no ip route6</b> &lt;IPv6 address&gt; &lt;prefix length&gt; Removes the selected route. <b>Command mode:</b> Global configuration</p>
<p><b>no ip route6</b> [<b>destination-address</b> &lt;IPv6 address&gt;  <b>gateway</b> &lt;default gateway address&gt; <b>interface</b> &lt;1-128&gt; <b>all</b>] Clears IPv6 static routes. You are prompted to select the routes to clear, based on the following criteria:</p> <ul style="list-style-type: none"><li>o <b>destination-address:</b> Destination IPv6 address of the route</li><li>o <b>gateway:</b> Default gateway address used by the route</li><li>o <b>interface:</b> Interface used by the route</li><li>o <b>all:</b> All IPv6 static routes</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ipv6 route static</b> Displays the current static route configuration. <b>Command mode:</b> All</p>

## IPv6 Neighbor Discovery Cache Configuration

Table 340 describes the IPv6 Neighbor Discovery cache configuration commands.

**Table 340.** IPv6 Neighbor Discovery Cache Configuration Commands

Command Syntax and Usage
<p><b>ip neighbors</b> &lt;IPv6 address&gt; &lt;MAC address&gt; <b>vlan</b> &lt;VLAN number&gt;  <b>port</b> &lt;port number or alias&gt;</p> <p>Adds a static entry to the Neighbor Discovery cache table.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip neighbors</b> {&lt;IPv6 address&gt;  <b>all</b>}</p> <p>Deletes the selected entry from the static Neighbor Discovery cache table.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip neighbors all</b> [<b>if</b> &lt;1-128&gt; <b>interface port</b>  &lt;port alias or number&gt; <b>vlan</b> &lt;VLAN number&gt;]</p> <p>Clears the selected static entries in the Neighbor Discovery cache table.</p> <p><b>Command mode:</b> Global configuration</p>

## IPv6 Neighbor Discovery Prefix Configuration

The following table describes the Neighbor Discovery prefix configuration options. These commands allow you to define a list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from an interface.

**Table 341.** IPv6 Neighbor Discovery Prefix Commands

Command Syntax and Usage
<p><b>interface ip</b> &lt;1-127&gt;</p> <p>Enters Interface IP mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ipv6 nd prefix</b> {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} [<b>no-advertise</b>]</p> <p>Adds a Neighbor Discovery prefix to the interface.</p> <p>The default setting is enabled.</p> <p>To disable the prefix and not advertise it in the Prefix Information options in Router Advertisement messages sent from the interface use the <b>no-advertise</b> option.</p> <p>Additional prefix options are listed in this table.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>no ipv6 nd prefix</b> {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} [<b>interface all</b>]</p> <p>Removes the selected Neighbor Discovery prefix(es). If you specify an interface number, all prefixes for the interface are removed.</p> <p><b>Command mode:</b> Interface IP</p>

**Table 341.** IPv6 Neighbor Discovery Prefix Commands (continued)

Command Syntax and Usage
<p><b>ipv6 nd prefix</b> {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} <b>no-autoconfig</b></p> <p>Disables the autonomous flag. When enabled, the autonomous flag indicates that the prefix can be used for stateless address configuration.</p> <p>The default setting is enabled.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 nd prefix</b> {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} <b>off-link</b> <b>[no-autoconfig]</b></p> <p>Disables the on-link flag. When enabled, the on-link flag indicates that this prefix can be used for on-link determination. When disabled, the advertisement makes no statement about on-link or off-link properties of the prefix.</p> <p>The default setting is enabled.</p> <p>To clear the off-link flag, omit the off-link parameter when you issue this command.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>ipv6 nd prefix</b> {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} <b>valid-lifetime</b> &lt;0-4294967295&gt; [<b>infinite variable</b>] <b>preferred-lifetime</b> &lt;0-4294967295&gt; [<b>infinite variable</b>]</p> <p>Configures the Valid Lifetime and (optionally) the Preferred Lifetime of the prefix, in seconds.</p> <p>The Valid Lifetime is the length of time (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination.</p> <p>The default value is 2592000.</p> <p>The Preferred Lifetime is the length of time (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred.</p> <p>The default value is 604800.</p> <p><b>Note:</b> The Preferred Lifetime value must not exceed the Valid Lifetime value.</p> <p><b>Command mode:</b> Interface IP</p>
<p><b>show ipv6 prefix</b> {&lt;interface number&gt;}</p> <p>Displays current Neighbor Discovery prefix parameters.</p> <p><b>Command mode:</b> All</p>



## IPv6 Prefix Policy Table Configuration

The following table describes the configuration options for the IPv6 Prefix Policy Table. The Prefix Policy Table allows you to override the default address selection criteria.

**Table 342.** *IPv6 Prefix Policy Table Options*

Command Syntax and Usage
<p><b>[no] ip prefix-policy</b> &lt;IPv6 prefix&gt; &lt;prefix length&gt; &lt;precedence (0-100)&gt; &lt;label (0-100)&gt;</p> <p>Adds or removes a Prefix Policy Table entry. Enter the following parameters:</p> <ul style="list-style-type: none"><li>o IPv6 address prefix</li><li>o Prefix length</li><li>o Precedence: The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence.</li><li>o Label: The label allows you to select prefixes based on matching labels. Source prefixes are coupled with destination prefixes if their labels match.</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>show ip prefix-policy</b></p> <p>Displays the current Prefix Policy Table configuration.</p> <p><b>Command mode:</b> All</p>

## IPv6 Path MTU Configuration

The following table describes the configuration options for Path MTU (Maximum Transmission Unit). The Path MTU cache can consume system memory and affect performance. These commands allow you to manage the Path MTU cache.

**Table 343.** *IPv6 Path MTU Commands*

Command Syntax and Usage
<p><b>ip pmtu6 timeout {0 &lt;10-100&gt;}</b></p> <p>Sets the timeout value for Path MTU cache entries, in minutes. Enter 0 (zero) to set the timeout to infinity (no timeout).</p> <p>The default value is 10.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>clear ipv6 pmtu</b></p> <p>Clears all entries in the Path MTU cache.</p> <p><b>Command mode:</b> All Except User EXEC</p>
<p><b>show ipv6 pmtu</b></p> <p>Displays the current Path MTU configuration.</p> <p><b>Command mode:</b> All</p>

## IP Loopback Interface Configuration

An IP loopback interface is not connected to any physical port. A loopback interface is always accessible over the network.

**Table 344.** *IP Loopback Interface Commands*

Command Syntax and Usage
<b>interface loopback</b> <1-5> Enter Interface Loopback mode. <b>Command mode:</b> Global configuration
<b>[no] enable</b> Enables or disables the loopback interface. <b>Command mode:</b> Interface loopback
<b>ip address</b> <IP address> Defines the loopback interface IP address. <b>Command mode:</b> Interface loopback
<b>ip netmask</b> <subnet mask> Defines the loopback interface subnet mask. <b>Command mode:</b> Interface loopback
<b>ip ospf area</b> <area number> Configures the OSPF area index used by the loopback interface. <b>Command mode:</b> Interface loopback
<b>[no] ip ospf enable</b> Enables or disables OSPF for the loopback interface. <b>Command mode:</b> Interface loopback
<b>no interface loopback</b> <1-5> Deletes the selected loopback interface. <b>Command mode:</b> Global configuration
<b>show interface loopback</b> <1-5> Displays the current IP loopback interface parameters. <b>Command mode:</b> All

## DHCP Snooping

DHCP Snooping provides security by filtering untrusted DHCP packets and by maintaining a binding table of trusted interfaces.

**Table 345.** *DHCP Snooping Options*

<b>Command Syntax and Usage</b>
<p><b>[no] ip dhcp snooping</b>          Enables or disables DHCP Snooping.  <b>Command mode:</b> Global configuration</p>
<p><b>ip dhcp snooping binding</b> &lt;MAC address&gt; <b>vlan</b> &lt;VLAN ID (1-4094)&gt;          &lt;IP address&gt; <b>port</b> &lt;port alias or number&gt; <b>expiry</b> &lt;1-4294967295&gt;          Adds a manual entry to the binding table.  <b>Command mode:</b> Global configuration</p>
<p><b>no ip dhcp snooping binding</b> {&lt;MAC address&gt; <b>all</b>  <b>[interface port</b> &lt;port alias or number&gt; <b>vlan</b> &lt;VLAN ID (1-4094)&gt;]}          Removes an entry from the binding table.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] ip dhcp snooping information option-insert</b>          Enables or disables option 82 support for DHCP Snooping.          When enabled, DHCP Snooping performs the following functions:</p> <ul style="list-style-type: none"> <li>o if a DHCP packet from a client contains option 82 information, the information is retained.</li> <li>o when DHCP Snooping forwards a DHCP packet from a client, option 82 information is added to the packet.</li> </ul> <p>owhen DHCP snooping forward a DHCP packet from a server, option 82 information is removed from the packet.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] ip dhcp snooping vlan</b> &lt;VLAN ID (1-4094)&gt;          Adds or removes the selected VLAN to DHCP Snooping. Member ports participate in DHCP Snooping.  <b>Command mode:</b> Global configuration</p>
<p><b>show ip dhcp snooping</b>          Displays the current DHCP Snooping parameters.  <b>Command mode:</b> All</p>

---

## Converged Enhanced Ethernet Configuration

Table 346 describes the Converged Enhanced Ethernet (CEE) configuration commands.

**Table 346.** *CEE Commands*

Command Syntax and Usage
<b>[no] cee enable</b> Globally enables or disables CEE. <b>Command mode:</b> Global configuration
<b>[no] cee iscsi enable</b> Enables or disables ISCSI TLV advertisements. <b>Command mode:</b> Global configuration
<b>show cee</b> Displays the current CEE parameters. <b>Command mode:</b> All
<b>show cee iscsi</b> Displays the current ISCSI TLV parameters. <b>Command mode:</b> All

## ETS Global Configuration

Enhanced Transmission Selection (ETS) allows you to allocate bandwidth to different traffic types, based on 802.1p priority.

**Note:** ETS configuration supersedes the QoS 802.1p menu. When ETS is enabled, you cannot configure the 802.1p menu options.

### ETS Global Priority Group Configuration

Table 347 describes the global ETS Priority Group configuration options.

**Table 347.** Global ETS Priority Group Commands

Command Syntax and Usage
<p><b>[no] cee global ets mcast-priority-group mcpgid &lt;0-3&gt;</b> <b>[bandwidth percentage &lt;0, 10-100&gt;] [priority &lt;0-7&gt;]</b></p> <p>Configures Multicast Priority Group parameters. You can enter the link bandwidth percentage allocated to the Multicast Priority Group, and assign one or more 802.1p values to the Multicast Priority Group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>cee global ets mcast-priority-group mcpgid &lt;0-3&gt;</b> <b>description &lt;1-31 characters&gt;</b></p> <p>Enter text that describes the multicast priority group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no cee global ets mcast-priority-group mcpgid &lt;0-3&gt;</b> <b>description</b></p> <p>Removes the description for the specified multicast priority group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>cee global ets priority-group pgid &lt;0-7, 15&gt;</b> <b>bandwidth &lt;802.1p priority (0-7)&gt; &lt;bandwidth percentage (0, 10-100)&gt;</b></p> <p>Allows you to configure Priority Group parameters. You can enter the link bandwidth percentage allocated to the Priority Group, and also assign one or more 802.1p values to the Priority Group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>cee global ets priority-group pgid &lt;0-7, 15&gt;</b> <b>description &lt;1-31 characters&gt;</b></p> <p>Enter text that describes this Priority Group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no cee global ets priority-group &lt;0-7, 15&gt; description</b></p> <p>Removes the description for the specified Priority Group.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 347.** *Global ETS Priority Group Commands*

<b>Command Syntax and Usage</b>
<b>cee global ets priority-group pgid &lt;0-7, 15&gt; priority &lt;0-7&gt;</b> Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end. <b>Command mode:</b> Global configuration
<b>show cee global ets</b> Displays the current global ETS Priority Group parameters. <b>Command mode:</b> All
<b>show cee global ets mcast-priority-group &lt;0-3&gt;</b> Displays the current global ETS Multicast Priority Group parameters. <b>Command mode:</b> All
<b>show cee global ets priority-group &lt;0-7, 15&gt;</b> Displays the current global ETS Priority Group parameters. <b>Command mode:</b> All

## Priority Flow Control Configuration

Priority-based Flow Control (PFC) enhances flow control by allowing the switch to pause traffic based on its 802.1p priority value, while allowing traffic at other priority levels to continue.

### Global Priority Flow Control Configuration

[Table 348](#) describes the global PFC Priority Group configuration options.

**Table 348.** *Global PFC Priority Group Commands*

<b>Command Syntax and Usage</b>
<b>[no] cee global pfc enable</b> Globally enables or disables Priority Flow Control on all ports. <b>Command mode:</b> Global configuration
<b>cee global pfc priority &lt;0-7&gt; description &lt;1-31 characters&gt;</b> Enter text that describes this Priority Group. <b>Command mode:</b> Global configuration
<b>no cee global pfc priority &lt;0-7&gt; description</b> Removes the description for the specified Priority Group. <b>Command mode:</b> Global configuration
<b>[no] cee global pfc priority &lt;0-7&gt; enable</b> Enables or disables Priority Flow Control for the specified priority level. <b>Command mode:</b> Global configuration
<b>show cee global pfc</b> Displays the current Priority Flow Control global configuration. <b>Command mode:</b> All



## Port-level 802.1p PFC Configuration

Table 349 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

**Table 349.** Port 802.1p PFC Options

Command Syntax and Usage
<p><b>[no] cee port</b> &lt;port alias or number&gt; <b>pfc enable</b></p> <p>Enables or disables Priority Flow Control on the selected port.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>cee port</b> &lt;port alias or number&gt; <b>pfc priority</b> &lt;0-7&gt; <b>description</b> &lt;1-31 characters&gt;</p> <p>Enter text to describe the priority value.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no cee port</b> &lt;port alias or number&gt; <b>pfc priority</b> &lt;0-7&gt; <b>description</b></p> <p>Deletes the description from the specified priority value.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cee port</b> &lt;port alias or number&gt; <b>pfc priority</b> &lt;0-7&gt; <b>enable</b></p> <p>Enables or disables Priority Flow Control on the selected 802.1p priority.</p> <p><b>Note:</b> PFC can be enabled on 802.1p priority 3 and one other priority only.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show cee port</b> &lt;port alias or number&gt; <b>pfc priority</b> &lt;0-7&gt;</p> <p>Displays the current 802.1p PFC parameters for the selected port.</p> <p><b>Command mode:</b> All</p>
<p><b>show cee port</b> &lt;port alias or number&gt; <b>pfc</b></p> <p>Displays the current PFC parameters for the selected port.</p> <p><b>Command mode:</b> All</p>

## DCBX Port Configuration

Table 350 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

**Table 350.** *Port DCBX Commands*

Command Syntax and Usage
<p><b>[no] cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx app_proto advertise</b></p> <p>Enables or disables DCBX Application Protocol advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx app_proto willing</b></p> <p>Enables or disables Application Protocol willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx enable</b></p> <p>Enables or disables DCBX on the port.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx ets advertise</b></p> <p>Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx ets willing</b></p> <p>Enables or disables ETS willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx pfc advertise</b></p> <p>Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx pfc willing</b></p> <p>Enables or disables PFC willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show cee port</b> <i>&lt;port alias or number&gt;</i> <b>dcbx</b></p> <p>Displays the current port DCBX parameters.</p> <p><b>Command mode:</b> All</p>

---

## Fibre Channel over Ethernet Configuration

Fibre Channel over Ethernet (FCoE) transports Fibre Channel frames over an Ethernet fabric. The CEE features and FCoE features allow you to create a lossless Ethernet transport mechanism.

**Note:** On EN4093 models, FCoE is not supported in stacking mode.

[Table 351](#) describes the FCoE configuration options.

**Table 351.** *FCoE Configuration Commands*

Command Syntax and Usage
<b>[no] fcoe fips automatic-vlan</b> Enables or disables automatic VLAN creation, based on response received from the connected device. <b>Command mode:</b> Global configuration
<b>[no] fcoe fips enable</b> Globally enables or disables FIP Snooping on. <b>Command mode:</b> Global configuration
<b>[no] fcoe fips timeout-acl</b> Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system. <b>Command mode:</b> Global configuration
<b>show fcoe information</b> Displays the current FCoE parameters. <b>Command mode:</b> All

## FIPS Port Configuration

FIP Snooping allows the switch to monitor FCoE Initialization Protocol (FIP) frames to gather discovery, initialization, and maintenance data. This data is used to automatically configure ACLs that provide FCoE connections and data security.

[Table 352](#) describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

**Table 352.** *Port FIP Snooping Commands*

Command Syntax and Usage
<p><b>fcoe fips port</b> <i>&lt;port alias or number&gt;</i> <b>fcf-mode</b> [<b>auto on off</b>]</p> <p>Configures FCoE Forwarding (FCF) on the port, as follows:</p> <ul style="list-style-type: none"><li>o <b>on</b>: Configures the port as a Fibre Channel Forwarding (FCF) port.</li><li>o <b>off</b>: Configures the port as an FCoE node (ENode).</li><li>o <b>auto</b>: Automatically detect the configuration of the connected device, and configure this port to match.</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] fcoe fips port</b> <i>&lt;port alias or number&gt;</i> <b>enable</b></p> <p>Enables or disables FIP Snooping on the port.</p> <p>The default setting is <b>enabled</b>.</p> <p><b>Note:</b> If IPv6 ACLs are assigned to the port, you cannot enable FCoE.</p> <p><b>Command mode:</b> Global configuration</p>

---

## Remote Monitoring Configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

The following sections describe the Remote Monitoring (RMON) configuration options.

- [“RMON History Configuration” on page 565](#)
- [“RMON Event Configuration” on page 566](#)
- [“RMON Alarm Configuration” on page 567](#)

### RMON History Configuration

[Table 353](#) describes the RMON History commands.

**Table 353.** *RMON History Commands*

Command Syntax and Usage
<p><b>rmon history</b> &lt;1-65535&gt; <b>interface-oid</b> &lt;1-127 characters&gt;</p> <p>Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows:</p> <p>1.3.6.1.2.1.2.2.1.1.x, where x is the ifIndex.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>rmon history</b> &lt;1-65535&gt; <b>owner</b> &lt;1-127 characters&gt;</p> <p>Enter a text string that identifies the person or entity that uses this History index.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>rmon history</b> &lt;1-65535&gt; <b>polling-interval</b> &lt;1-3600&gt;</p> <p>Configures the time interval over which the data is sampled for each bucket. The default value is 1800.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>rmon history</b> &lt;1-65535&gt; <b>requested-buckets</b> &lt;1-65535&gt;</p> <p>Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is 30.</p> <p><b>Note:</b> The maximum number of buckets that can be granted is 50.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 353.** *RMON History Commands (continued)*

Command Syntax and Usage
<b>no rmon history</b> <1-65535> Deletes the selected History index. <b>Command mode:</b> Global configuration
<b>show rmon history</b> Displays the current RMON History parameters. <b>Command mode:</b> All

## RMON Event Configuration

[Table 354](#) describes the RMON Event commands.

**Table 354.** *RMON Event Commands*

Command Syntax and Usage
<b>rmon event</b> <1-65535> <b>description</b> <1-127 characters> Enter a text string to describe the event. <b>Command mode:</b> Global configuration
<b>rmon event</b> <1-65535> <b>owner</b> <1-127 characters> Enter a text string that identifies the person or entity that uses this event index. <b>Command mode:</b> Global configuration
<b>[no] rmon event</b> <1-65535> <b>type</b> {log trap both} Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station. <b>Command mode:</b> Global configuration
<b>no rmon event</b> <1-65535> Deletes the selected RMON Event index. <b>Command mode:</b> Global configuration
<b>show rmon event</b> Displays the current RMON Event parameters. <b>Command mode:</b> All

## RMON Alarm Configuration

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

[Table 355](#) describes the RMON Alarm commands.

**Table 355.** *RMON Alarm Commands*

Command Syntax and Usage
<b>rmon alarm</b> <1-65535> <b>alarm-type</b> { <b>rising</b>   <b>falling</b>   <b>either</b> } Configures the alarm type as rising, falling, or either (rising or falling). <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>falling-crossing-index</b> <1-65535> Configures the falling alarm event index that is triggered when a falling threshold is crossed. <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>falling-limit</b> <-2147483647 - 214748364> Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>interval</b> <1-65535> Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is <b>1800</b> . <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>oid</b> <1-127 characters> Configures an alarm MIB Object Identifier. <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>owner</b> <1-127 characters> Enter a text string that identifies the person or entity that uses this alarm index. <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>rising-crossing-index</b> <1-65535> Configures the rising alarm event index that is triggered when a rising threshold is crossed. <b>Command mode:</b> Global configuration

**Table 355.** *RMON Alarm Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>rmon alarm</b> &lt;1-65535&gt; <b>rising-limit</b> &lt;-2147483647 - 2147483647&gt;</p> <p>Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>rmon alarm</b> &lt;1-65535&gt; <b>sample</b> {abs delta}</p> <p>Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:</p> <ul style="list-style-type: none"><li>o <b>abs</b>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li><li>o <b>delta</b>—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</li></ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no rmon alarm</b> &lt;1-65535&gt;</p> <p>Deletes the selected RMON Alarm index.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show rmon alarm</b></p> <p>Displays the current RMON Alarm parameters.</p> <p><b>Command mode:</b> All</p>



---

## VMReady

[Table 356](#) describes the VMReady configuration options.

**Table 356.** *VMReady Configuration Options*

Command Syntax and Usage
<b>[no] virt enable</b> Enables or disables VMReady. <b>Note:</b> The no form of this command deletes all configured VM groups. <b>Command mode:</b> Global configuration
<b>virt vmcheck</b> Configures VM Check validation settings. For command options, see <a href="#">page 574</a> . <b>Command mode:</b> Global configuration
<b>virt vmgroup</b> Configures VM Group settings. For command options, see <a href="#">page 571</a> . <b>Command mode:</b> Global configuration
<b>virt vmpolicy vmbwidth</b> Configures VM Bandwidth management settings. For command options, see <a href="#">page 570</a> . <b>Command mode:</b> Global configuration
<b>virt vmprofile</b> Configures VM Profile settings. For command options, see <a href="#">page 575</a> . <b>Command mode:</b> Global configuration
<b>virt vmrmisc</b> Configures Miscellaneous VMready settings. For command options, see <a href="#">page 577</a> . <b>Command mode:</b> Global configuration
<b>virt vmware</b> Configures VMware settings. For command options, see <a href="#">page 576</a> . <b>Command mode:</b> Global configuration
<b>show virt</b> Displays the current virtualization parameters. <b>Command mode:</b> All

## VM Policy Bandwidth Management

Table 357 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

**Table 357.** VM Bandwidth Management Options

Command Syntax and Usage
<p><b>[no] virt vmpolicy vmbwidth</b> [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt; &lt;IP address&gt; &lt;index number&gt;] <b>bwctrl</b></p> <p>Enables or disables bandwidth control on the VM policy.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmpolicy vmbwidth</b> [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt; &lt;IP address&gt; &lt;index number&gt;] <b>rxrate</b> &lt;0-4000000&gt; &lt;max. burst (0-4096)&gt;</p> <p>The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64.</p> <p>The second values configures the maximum burst size, in kilobits. Enter one of the following values: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmpolicy vmbwidth</b> [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt; &lt;IP address&gt; &lt;index number&gt;] <b>txrate</b> &lt;0-4000000&gt; &lt;max. burst (0-4096)&gt; [&lt;ACL number (1-640)&gt;]</p> <p>The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64.</p> <p>The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p>The third value represents the ACL assigned to the transmission rate. The ACL is automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no virt vmpolicy vmbwidth</b> [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt; &lt;IP address&gt; &lt;index number&gt;]</p> <p>Deletes the bandwidth management settings from this VM policy.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show virt vmpolicy vmbwidth</b> [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt; &lt;IP address&gt; &lt;index number&gt;]</p> <p>Displays the current VM bandwidth management parameters.</p> <p><b>Command mode:</b> All</p>

## VM Group Configuration

Table 358 describes the VM group configuration options. A VM group is a collection of members, such as VMs, ports, or LAGs. Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

**Table 358.** VM Group Commands

Command Syntax and Usage
<p><b>virt vmgroup</b> &lt;1-4096&gt; <b>cpu</b></p> <p>Enables or disables sending unregistered IPMC traffic to CPU.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmgroup</b> &lt;1-4096&gt; <b>flood</b></p> <p>Enables or disables flooding unregistered IPMC traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmgroup</b> &lt;1-4096&gt; <b>key</b> &lt;1-65535&gt;</p> <p>Adds or removes an LACP <i>admin key</i> to the VM group. LACP LAGs formed with this <i>admin key</i> will be included in the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmgroup</b> &lt;1-4096&gt; <b>optflood</b></p> <p>Enables or disables optimized flooding.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmgroup</b> &lt;1-4096&gt; <b>port</b> &lt;port number or alias&gt;</p> <p>Adds or removes the selected port to the VM group.</p> <p><b>Note:</b> A port can be added to a VM group only if no VMs on that port are members of the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmgroup</b> &lt;1-4096&gt; <b>portchannel</b> &lt;LAG number&gt;</p> <p>Adds or removes the selected LAG to the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmgroup</b> &lt;1-4096&gt; <b>profile</b> &lt;profile name (1-39 characters)&gt;</p> <p>Adds the selected VM profile to the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no virt vmgroup</b> &lt;1-4096&gt; <b>profile</b></p> <p>Removes the VM profile assigned to the VM group.</p> <p><b>Note:</b> This command can only be used if the VM group is empty (only has the profile assigned).</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmgroup</b> &lt;1-4096&gt; <b>stg</b> &lt;STG number&gt;</p> <p>Assigns the VM group VLAN to a Spanning Tree Group (STG).</p> <p><b>Command mode:</b> Global configuration</p>

**Table 358.** VM Group Commands (continued)

Command Syntax and Usage
<p><b>[no] virt vmgroup &lt;1-4096&gt; tag</b></p> <p>Enables or disables VLAN tagging on ports in this VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmgroup &lt;1-4096&gt; validate [basic advanced]</b></p> <p>Enables MAC address spoof prevention for the specified VM group. Default setting is disabled.</p> <ul style="list-style-type: none"> <li>o <b>basic</b> validation ensures lightweight port-based protection by cross-checking the VM MAC address, switch port and switch ID between the switch and the hypervisor. Applicable for “trusted” hypervisors, which are not susceptible to duplicating or reusing MAC addresses on virtual machines.</li> <li>o <b>advanced</b> validation ensures heavyweight VM-based protection by cross-checking the VM MAC address, VM UUID, switch port and switch ID between the switch and the hypervisor. Applicable for “untrusted” hypervisors, which are susceptible to duplicating or reusing MAC addresses on virtual machines.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no virt vmgroup &lt;1-4096&gt; validate</b></p> <p>Disables MAC address spoof prevention for the specified VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmgroup &lt;1-4096&gt; vm [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt; &lt;IP address&gt; &lt;index number&gt;]</b></p> <p>Adds or removes a VM to the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (<b>virt vmware vcspec</b>). The VM index number is found in the VM information dump (<b>show virt vm</b>).</p> <p><b>Note:</b> If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmgroup &lt;1-4096&gt; vmap &lt;VMAP number&gt; {intports extports}</b></p> <p>Assigns the selected VLAN Map to this group. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VM Group.</p> <p>For more information about configuring VLAN Maps, see <a href="#">“VMAP Configuration” on page 402</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmgroup &lt;1-4096&gt; vport &lt;virtual port alias or number&gt;</b></p> <p>Adds or removes the selected virtual port to the VM group.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 358.** *VM Group Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>virt vmgroup</b> &lt;1-4096&gt; <b>vlan</b> &lt;VLAN number&gt;</p> <p>Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns an unused VLAN when adding a port or a VM to the VM Group.</p> <p><b>Note:</b> If you add a VM profile to this group, the group will use the VLAN assigned to the profile.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no virt vmgroup</b> &lt;1-4096&gt;</p> <p>Deletes the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show virt vmgroup</b> &lt;1-4096&gt;</p> <p>Displays the current VM group parameters.</p> <p><b>Command mode:</b> All</p>

## VM Check Configuration

Table 359 describes the VM Check validation options used for MAC address spoof prevention.

**Table 359.** *VM Check Configuration Options*

<b>Command Syntax and Usage</b>
<b>virt vmcheck acls max</b> <1-640> Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. The default value is 50. <b>Command mode:</b> Global configuration
<b>no virt vmcheck acls</b> Disables ACL-based MAC address spoofing prevention in advanced validation mode. <b>Command mode:</b> Global configuration
<b>virt vmcheck action advanced {acl link log}</b> Sets up action taken when detecting MAC address spoofing in advanced validation mode: <ul style="list-style-type: none"><li>o <b>acl</b> registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address</li><li>o <b>link</b> registers a syslog entry and disables the corresponding switch port</li><li>o <b>log</b> registers a syslog entry</li></ul> The default setting is <b>acl</b> . <b>Command mode:</b> Global configuration
<b>virt vmcheck action basic {link log}</b> Sets up action taken when detecting MAC address spoofing in basic validation mode: <ul style="list-style-type: none"><li>o <b>link</b> registers a syslog entry and disables the corresponding switch port</li><li>o <b>log</b> registers a syslog entry</li></ul> The default setting is <b>link</b> . <b>Command mode:</b> Global configuration
<b>[no] virt vmcheck trust</b> <ports> Enables or disables trusted ports for VM communication. By default, all ports are disabled. <b>Command mode:</b> Global configuration
<b>show virt vmcheck</b> Displays the current VM Check settings. See <a href="#">page 167</a> for sample output. <b>Command mode:</b> Global configuration

## VM Profile Configuration

Table 360 describes the VM Profiles configuration options.

**Table 360.** VM Profiles Commands

Command Syntax and Usage
<p><b>virt vmprofile</b> &lt;profile name (1-39 characters)&gt;            Defines a name for the VM profile.  <b>Command mode:</b> Global configuration</p>
<p><b>no virt vmprofile</b> &lt;profile name (1-39 characters)&gt;            Deletes the selected VM profile.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmprofile edit</b> &lt;profile name (1-39 characters)&gt; <b>eshaping</b> [<b>&lt;average (1-1000000000)&gt;</b> <b>&lt;burst (1-1000000000)&gt;</b> <b>&lt;peak (1-1000000000)&gt;</b>]            Configures traffic egress shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> <li>o Average traffic, in Kilobits per second</li> <li>o Maximum burst size, in Kilobytes</li> <li>o Peak traffic, in Kilobits per second</li> <li>o Delete traffic shaping parameters.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmprofile edit</b> &lt;profile name (1-39 characters)&gt; <b>shaping</b> [<b>&lt;average (1-1000000000)&gt;</b> <b>&lt;burst (1-1000000000)&gt;</b> <b>&lt;peak (1-1000000000)&gt;</b>]            Configures traffic shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> <li>o Average traffic, in Kilobits per second</li> <li>o Maximum burst size, in Kilobytes</li> <li>o Peak traffic, in Kilobits per second</li> <li>o Delete traffic shaping parameters.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmprofile edit</b> &lt;profile name (1-39 characters)&gt; <b>vlan</b> &lt;VLAN number&gt;            Assigns a VLAN to the VM profile.  <b>Command mode:</b> Global configuration</p>
<p><b>show virt vmprofile</b> [<b>&lt;profile name&gt;</b>]            Displays the current VM Profile parameters.  <b>Command mode:</b> All</p>

## VMWare Configuration

Table 361 describes the VMware configuration options. When the user configures the VMware Virtual Center, the VM Agent module in the switch can perform advanced functionality by communicating with the VMware management console. The Virtual Center provides VM and Host names, IP addresses, Virtual Switch and port group information. The VM Agent on the switch communicates with the Virtual Center to synchronize VM profiles between the switch and the VMware virtual switch.

**Note:** VM Profiles and Hello cannot be configured or enabled unless the Virtual Center is configured.

**Table 361.** *VM Ware Commands*

Command Syntax and Usage
<p><b>virt vmware hbport</b> &lt;1-65535&gt;</p> <p>Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center.</p> <p>The default value is port 902.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>virt vmware hello</b> [enable haddr &lt;IP_address&gt; hport &lt;port_no&gt; htimer &lt;1-60&gt;]</p> <p>Configures CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors facilitates MAC address spoof prevention.</p> <p>Default setting is disabled.</p> <ul style="list-style-type: none"> <li>o enable enables CDP advertisements transmission.</li> <li>o haddr advertises a specific IP address instead of the default management IP.</li> <li>o hport enables ports on which CDP advertisements are sent.</li> <li>o htimer sets the number of seconds between successive CDP advertisements. Default value is 30.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>no virt vmware hello</b> [enable hport &lt;port_no&gt;]</p> <p>Disables CDP advertisement transmissions completely or only on specific ports.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] virt vmware vcspec</b> &lt;IP address&gt; &lt;username&gt; [noauth]</p> <p>Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system. You are prompted for the following information:</p> <ul style="list-style-type: none"> <li>– IP address of the Virtual Center</li> <li>– User name and password for the Virtual Center</li> <li>– Whether to authenticate the SSL security certificate (yes or no)</li> </ul> <p><b>Command mode:</b> Global configuration</p>



**Table 361.** *VM Ware Commands*

<b>Command Syntax and Usage</b>
<b>show virt vmware</b> Displays the current VMware parameters. <b>Command mode:</b> All

## Miscellaneous VMready Configuration

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the Enterprise NOS CLI, ISCLI and the Miscellaneous VMready Configuration Menu. [Table 361](#) describes the VMready configuration options.

**Table 362.** *VMware Miscellaneous Options*

<b>Command Syntax and Usage</b>
<b>[no] virt vmrmisc lmac</b> Enables or disables the switch to treat locally administered MAC addresses as VMs. <b>Command mode:</b> Global configuration
<b>[no] virt vmrmisc oui &lt;3 byte VM MAC OUI&gt; &lt;Vendor Name&gt;</b> Adds or removes a MAC OUI. <b>Command mode:</b> Global configuration
<b>show virt oui</b> Displays all the configured MAC OUIs. <b>Command mode:</b> All

---

## Virtual NIC Configuration

Table 363 describes the Virtual NIC (vNIC) configuration options.

**Table 363.** *Virtual NIC options*

<b>Command Syntax and Usage</b>
<b>[no] vnic egress-bw-meter</b> Enables or disables vNIC bandwidth metering. When enabled, any bandwidth which is not used by the vNIC to which it is allocated is shared with other vNICs. In all cases, the configured values for minimum bandwidth are honored. Only the excess bandwidth is shared. <b>Command mode:</b> Global configuration
<b>[no] vnic enable</b> Globally enables or disables vNIC. <b>Command mode:</b> Global configuration
<b>[no] vnic uplink-share</b> Enable or disable vNIC shared mode. When enabled, multiple vNIC groups can be assigned to the same uplink port. <b>Command mode:</b> Global configuration
<b>show vnic</b> Displays the current vNIC parameters. <b>Command mode:</b> All

## Virtual NIC Group Configuration

Table 364 describes the Virtual NIC (vNIC) Group configuration options.

**Table 364.** *vNIC Group Commands*

<b>Command Syntax and Usage</b>
<b>vnic vnicgroup &lt;1-32&gt;</b> Enters vNIC Group Configuration mode. <b>Command mode:</b> Global Configuration
<b>[no] enable</b> Enables or disables the vNIC Group. <b>Command mode:</b> vNIC Group configuration
<b>[no] failover</b> Enables or disables uplink failover for the vNIC Group. Uplink Failover for the vNIC Group will disable all vNIC and non-vNIC ports in the group. Other port functions continue to operate normally. The default setting is <b>disabled</b> . <b>Command mode:</b> vNIC Group configuration

**Table 364.** *vNIC Group Commands (continued)*

<b>Command Syntax and Usage</b>	
<b>[no] key</b> <LAG number>	Adds or removes the uplink LACP LAG to the vNIC Group. <b>Command mode:</b> vNIC Group configuration
<b>[no] member</b> <vNIC number>	Adds or removes a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: 1 . 1 . <b>Command mode:</b> vNIC Group configuration
<b>[no] port</b> <port number or alias>	Adds or removes the non-vNIC port or uplink port to the vNIC Group. <b>Command mode:</b> vNIC Group configuration
<b>[no] trunk</b> <LAG number>	Adds or removes the uplink LAG to the vNIC Group. <b>Command mode:</b> vNIC Group configuration
<b>vlan</b> <VLAN number>	Assigns a VLAN to the vNIC Group. <b>Command mode:</b> vNIC Group configuration
<b>no vnic vnicgroup</b> <1-32>	Deletes the selected vNIC Group. <b>Command mode:</b> Global configuration
<b>show vnicgroup</b>	Displays the current vNIC Group parameters. <b>Command mode:</b> All

## vNIC Port Configuration

Table 365 describes the Virtual NIC (vNIC) port configuration options.

**Table 365.** *vNIC Port Commands*

Command Syntax and Usage
<p><b>vnic port</b> &lt;port alias or number&gt; <b>index</b> &lt;1-4&gt;</p> <p>Enters vNIC Configuration mode.</p> <p><b>Note:</b> This command is valid for internal server ports only.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>bandwidth</b> &lt;1-100&gt;</p> <p>Configures the maximum bandwidth allocated to this vNIC, in increments of 100 Mbps. For example:</p> <ul style="list-style-type: none"><li>- 1 = 100 Mbps</li><li>- 10 = 1000 Mbps</li></ul> <p><b>Command mode:</b> vNIC configuration</p>
<p><b>[no] enable</b></p> <p>Enables or disables the vNIC.</p> <p><b>Command mode:</b> vNIC configuration</p>

## UFP Configuration

Table 366 describes the Unified Fabric Port (UFP) configuration options. UFP allows defining up to 8 virtual ports per physical port. Each virtual port can be set up to operate in a specific mode (access, trunk, tunnel, FCoE, auto) and within predefined bandwidth limits.

**Note:** vNIC and UFP are mutually exclusive. Only one of them can be globally enabled at any point in time.

**Table 366.** *UFP Commands*

Command Syntax and Usage
<p><b>[no] ufp enable</b>            Globally enables or disables UFP.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] ufp port &lt;port_no.&gt; enable</b>            Enables or disables UFP on the specified physical ports.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] ufp port &lt;port_no.&gt; qos-mode [bw ets]</b>            Sets the UFP QoS mode: bandwidth or ETS.  <b>Command mode:</b> Global configuration</p>
<p><b>ufp port &lt;port_no.&gt; vport &lt;1-8&gt;</b>            Enters UFP Virtual Port Configuration mode.  <b>Command mode:</b> Global configuration</p>
<p><b>no ufp port &lt;port_no.&gt; [vport &lt;1-8&gt;]</b>            Disables UFP settings on the specified physical or virtual port.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] enable</b>            Enables or disables the virtual port.  <b>Command mode:</b> UFP Virtual Port Configuration</p>
<p><b>evb profile &lt;1-16&gt;</b>            Applies the specified EVB profile for the virtual port.  <b>Command mode:</b> UFP Virtual Port Configuration</p>
<p><b>no evb profile</b>            Disables the specified EVB profile for the virtual port.  <b>Command mode:</b> UFP Virtual Port Configuration</p>

**Table 366.** UFP Commands (continued)

<p><b>Command Syntax and Usage</b></p>
<p><b>network {default-tag default-vlan &lt;2-4094&gt;}</b></p> <p>Configures the virtual port network configuration settings:</p> <ul style="list-style-type: none"><li>o <b>default-tag</b> enables tagging egress frames with the default VLAN ID when the virtual port is in access or trunk mode and <b>default-vlan</b> is defined. Default setting is disabled.</li><li>o <b>default-vlan</b> configures the default VLAN ID for the virtual port.</li></ul> <p><b>Note:</b> VLANs 4002-4009 cannot be used as customer VLANs.</p> <p><b>Note:</b> A customer VLAN cannot be configured on multiple virtual ports of the same physical port.</p> <p><b>Command mode:</b> UFP Virtual Port Configuration</p>
<p><b>no network default-tag</b></p> <p>Disables default VLAN ID tagging on the virtual port.</p> <p><b>Command mode:</b> UFP Virtual Port Configuration</p>
<p><b>network mode {access auto fcoe trunk tunnel}</b></p> <p>Configures the virtual port's operating mode:</p> <ul style="list-style-type: none"><li>o <b>access</b> allows the virtual port to associate only with the default customer VLAN, as defined by the <b>network default-vlan</b> command.</li><li>o <b>auto</b> integrates UFP with VMReady/802.1qbg. This mode allows dynamic vlan creation for the vport.</li><li>o <b>fcoe</b> configures the virtual port to carry Fibre Channel over Ethernet traffic when linked to a Fibre Channel virtual Host Bus Adapter. Setting a virtual port in fcoe mode enables Priority Flow Control on the physical port.</li><li>o <b>trunk</b> allows the virtual port to associate with up to 1024 customer VLANs.</li><li>o <b>tunnel</b> makes the virtual port VLAN agnostic. This is the default setting.</li></ul> <p><b>Command mode:</b> UFP Virtual Port Configuration</p>
<p><b>network private-vlan {host trunk promiscuous}</b></p> <p>Configures the virtual port's private VLAN mode:</p> <ul style="list-style-type: none"><li>o <b>host</b> allows only ONE secondary VLAN. In case of network trunk mode, the other VLANs will be in different Private VLAN domain.</li><li>o <b>trunk</b> allows both primary and secondary VLAN as well as non-Private VLAN domains. The Isolate-VLAN is also allowed to pass through this port type.</li><li>o <b>promiscuous</b> allows private VLAN promiscuous mode</li></ul> <p><b>Command mode:</b> UFP Virtual Port Configuration</p>
<p><b>no network private-vlan</b></p> <p>Disables private-VLAN mode on the virtual port.</p> <p><b>Command mode:</b> UFP Virtual Port Configuration</p>

**Table 366.** UFP Commands (continued)

Command Syntax and Usage
<p><b>qos bandwidth {max &lt;10-100&gt; min &lt;10-100&gt;}</b></p> <p>Configures bandwidth allocation for the virtual port:</p> <ul style="list-style-type: none"><li>o Configures the minimum bandwidth guaranteed for the virtual port as a percentage of the physical port's bandwidth. The default value is 25.</li><li>o Configures the maximum bandwidth allowed for this virtual port as a percentage of the physical port's bandwidth. The default value is 100.</li></ul> <p><b>Note:</b> The aggregated minimum bandwidth guaranteed for all the virtual ports within a physical port cannot exceed 100.</p> <p><b>Command mode:</b> UFP Virtual Port Configuration</p>
<p><b>qos ets [host-control priority &lt;0-7&gt;]</b></p> <p>Configures ETS bandwidth allocation for the virtual port:</p> <ul style="list-style-type: none"><li>o Enables or disables host COS control.</li><li>o Configures 802.1p priority value for the specific vPort.</li></ul> <p><b>Note:</b> The aggregated minimum bandwidth guaranteed for all the virtual ports within a physical port cannot exceed 100.</p> <p><b>Command mode:</b> UFP Virtual Port Configuration</p>

## Edge Virtual Bridge Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). [Table 367](#) describes the EVB configuration options.

**Table 367.** *Edge Virtual Bridge Configuration Options*

Command Syntax and Usage
<b>virt evb vsidb</b> <VSIDB_number> Enter Virtual Station Interface Database configuration mode. <b>Command mode:</b> Global configuration
<b>virt evb update vsidb</b> <VSIDB_number> Update VSI types from the VSI database. <b>Command mode:</b> All
<b>filename</b> <file name> Sets the Virtual Station Interface Type database document name. <b>Command mode:</b> VSI Database
<b>no filename</b> Removes the Virtual Station Interface Type database document name. <b>Command mode:</b> VSI Database
<b>filepath</b> <file path> Sets the Virtual Station Interface Type database document path. <b>Command mode:</b> VSI Database
<b>no filepath</b> Removes the Virtual Station Interface Type database document path. <b>Command mode:</b> VSI Database
<b>host</b> <IP address> [ <b>mgt-port</b>   <b>extm-port</b>   <b>data-port</b> ] Sets the Virtual Station Interface Type database manager IPv4/IPv6 address and the port used for the connection. By default, the management port is used. <b>Command mode:</b> VSI Database
<b>port</b> <1-65534> Sets the Virtual Station Interface Type database manager port. <b>Command mode:</b> VSI Database
<b>protocol</b> {http https} Sets the Virtual Station Interface Type database transport protocol. The default setting is HTTP. <b>Command mode:</b> VSI Database



**Table 367.** Edge Virtual Bridge Configuration Options

Command Syntax and Usage
<p><b>update-interval</b> &lt;5-300&gt;</p> <p>Sets the Virtual Station Interface Type database update interval in seconds.</p> <p><b>Command mode:</b> VSI Database</p>
<p><b>no update-interval</b> &lt;5-300&gt;</p> <p>Disables periodic updates.</p> <p><b>Command mode:</b> VSI Database</p>
<p><b>no virt evb vsidb</b> &lt;VSIDB_number&gt;</p> <p>Resets the Virtual Station Interface Type database information to the default values.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>clear virt evb vsi</b> [<b>mac-address</b> <b>port</b> &lt;port alias or number&gt;  <b>type-id</b> &lt;1-16777215&gt; <b>vlan</b> &lt;1-4094&gt;]</p> <p>Clears VSI database associations.</p> <p><b>Command mode:</b> All</p>
<p><b>clear virt evb vsidb</b> [<b>manager-id</b> &lt;0-255&gt; <b>type-id</b> &lt;1-16777215&gt;  <b>version</b> &lt;0-255&gt;]</p> <p>Clears local VSI types cache.</p> <p><b>Command mode:</b> All</p>
<p><b>show virt evb vsitypes</b> [<b>mgrid</b> &lt;0-255&gt; <b>typeid</b> &lt;1-16777215&gt;  <b>version</b> &lt;0-255&gt;]</p> <p>Displays the current Virtual Station Interface Type database parameters.</p> <p><b>Command mode:</b> All</p>
<p><b>show virt evb vsidb</b> &lt;VSIDB_number&gt;</p> <p>Displays the current Virtual Station Interface database information.</p> <p><b>Command mode:</b> All</p>

## Edge Virtual Bridge Profile Configuration

Table 368 describes the Edge Virtual Bridge profile configuration options.

**Table 368.** *Edge Virtual Bridge VSI Type Profile Configuration Options*

<b>Command Syntax and Usage</b>
<p><b>virt evb profile</b> &lt;profile_number&gt;  Enter Virtual Station Interface type profile configuration mode.  <b>Command mode:</b> Global configuration</p>
<p><b>[no] reflective-relay</b>  Enables or disables VEPA mode (Reflective Relay capability).  <b>Command mode:</b> EVB Profile</p>
<p><b>[no] vsi-discovery</b>  Enables or disables VSI Discovery (ECP and VDP).  <b>Command mode:</b> EVB Profile</p>
<p><b>no virt evb profile</b> &lt;profile_number&gt;  Deletes the specified EVB profile.  <b>Command mode:</b> Global configuration</p>
<p><b>evb profile</b> &lt;1-16&gt;  Applies the specified EVB profile for the port. Automatically enables LLDP EVB TLV on the corresponding port.  <b>Command mode:</b> Interface port/UFP Virtual port</p>
<p><b>no evb profile</b>  Resets EVB profile for the port. Automatically disables LLDP, EVB, and TLV on the corresponding port.  <b>Command mode:</b> Interface port/UFP Virtual port</p>
<p><b>show virt evb profile</b> [&lt;1-16&gt;]  Displays the current EVB profile parameters.  <b>Command mode:</b> All</p>

---

## OpenFlow Configuration

OpenFlow is an open interface used to control the forwarding plane in compatible switches and routers remotely, from an external controller. The EN4093R 10Gb Ethernet Scalable Switch can function as either a Hybrid or OpenFlow-only switch:

- In Hybrid mode (default), an OpenFlow pipeline can be set up to run in parallel to the normal Ethernet switching pipeline. The two pipelines are completely separate, each with its own dedicated ports and confined packet flows.
- In OpenFlow-only mode, the normal Ethernet switching capabilities are disabled, and the EN4093R 10Gb Ethernet Scalable Switch behaves as a pure OpenFlow switch.

Table 369 describes the OpenFlow configuration options.

**Table 369.** *OpenFlow Configuration Options*

<b>Command Syntax and Usage</b>
<b>boot openflow {v1 v13}</b> Switches between OpenFlow version 1.0 and OpenFlow version 1.3 on reboot. The default setting is v1. <b>Command mode:</b> Global configuration
<b>boot profile default</b> Starts the switch in Hybrid mode on reboot. This is the default setting. <b>Command mode:</b> Global configuration
<b>boot profile openflow</b> Starts the switch in OpenFlow-only mode on reboot. <b>Command mode:</b> Global configuration
<b>[no] openflow enable</b> Enables or disables OpenFlow. <b>Note:</b> Features involving TCAM resources are not supported on all ports. <b>Command mode:</b> Global configuration
<b>openflow fdb-priority &lt;1-65535&gt;</b> Configures a priority value to map flows with matching priority to FDB entries, if the flow uses destination MAC address and VLAN as the matching qualifier and single port as the action. The default value is 1000. <b>Note:</b> When you issue this command, all registered flow entries are cleared. <b>Command mode:</b> Global configuration
<b>no openflow fdb-priority</b> Resets priority value required for FDB flows to the default value of 1000. <b>Command mode:</b> Global configuration

**Table 369.** *OpenFlow Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>openflow fdb-timeout</b> &lt;1-300&gt;</p> <p>Configures a time interval in seconds for periodically clearing dynamically learned FDB entries on edge ports.</p> <p>The default value is <code>disabled</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no openflow fdb-timeout</b></p> <p>Disables periodical clearing of dynamically learned FDB entries on edge ports.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] openflow mgmtport</b> &lt;port alias or number&gt;</p> <p>Enables or disables OpenFlow management for the selected port. Use OpenFlow management ports to communicate with an OpenFlow Controller. In Hybrid mode, controllers can also connect to the switch using legacy ports.</p> <p>The default setting is <code>disabled</code>.</p> <p><b>Note:</b> Available only in OpenFlow-only mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>openflow mpls-priority</b> &lt;1-65535&gt;</p> <p>Configures a priority value to map flows with matching priority to MPLS entries.</p> <p>The default value is <code>65535</code>.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Note:</b> When you issue this command, all the existing MPLS flows are cleared automatically.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no openflow mpls-priority</b></p> <p>Resets the priority value required for MPLS flows to the default value of <code>65535</code>.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>openflow instance</b> &lt;1-2&gt;</p> <p>Enters OpenFlow Instance command mode for the specified instance ID.</p> <p><b>Command mode:</b> Global configuration, OpenFlow Instance</p>
<p><b>no openflow instance</b> &lt;1-2&gt;</p> <p>Deletes the instance and clears flow table and statistics for the specified instance ID.</p> <p><b>Command mode:</b> Global configuration, OpenFlow Instance</p>

**Table 369.** *OpenFlow Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>[no] buffer</b></p> <p>Enables or disables buffering support for OpenFlow packets. The default setting is disabled.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>connect-retry</b> &lt;1-8&gt;</p> <p>Configures the maximum number of attempts to establish connection to a controller, before assuming the controller is down. The default value is 4.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no connect-retry</b></p> <p>Resets the connect-retry value to 4.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>controller</b> &lt;1-4&gt; <b>address</b> &lt;ip_address&gt; [<b>data-port</b>   <b>mgt-port</b>   <b>extm-port</b>]</p> <p>Configures the IP address of the OpenFlow Controller. You may specify the port to use for data transfer: data port (<b>data-port</b>), management port (<b>mgt-port</b>) or external management port (<b>extm-port</b>). By default, the system uses the management port.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>controller</b> &lt;1-4&gt; <b>port</b> &lt;TCP port number (1-65535)&gt;</p> <p>Configures the TCP port used for communication with the Controller. The default port is 6633.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no controller</b> &lt;1-4&gt;</p> <p>Deletes the selected controller from the specified instance ID.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>dpid</b> &lt;hex string&gt;</p> <p>Applies an 8 byte Datapath ID to the instance, which enables equal cost multi-path routing in an OpenFlow environment. The default value is the instance ID followed by the switch MAC.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no dpid</b></p> <p>Resets the instance's Datapath ID to the default value (instance ID followed by the switch MAC).</p> <p><b>Command mode:</b> OpenFlow Instance</p>

**Table 369.** *OpenFlow Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>echo-reply-timeout</b> &lt;2-65535&gt;</p> <p>Configures the duration in seconds the switch will wait to receive an echo reply from the controller, before assuming failure.</p> <p>The default value is 15.</p> <p><b>Note:</b> The <code>echo-reply-timeout</code> value must be lower than the <code>echo-request-interval</code> value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no echo-reply-timeout</b></p> <p>Resets the <code>echo-reply-timeout</code> to the default value of 15.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>echo-request-interval</b> &lt;5-65535&gt;</p> <p>Configures the maximum duration in seconds the switch will keep sending echo requests to a non-responsive controller.</p> <p>The default value is 30.</p> <p><b>Note:</b> The <code>echo-request-interval</code> value must be higher than the <code>echo-reply-timeout</code> value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no echo-request-interval</b></p> <p>Resets the <code>echo-request-interval</code> value to the default value of 30.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>[no] edgeport</b> {&lt;port numbers&gt; <b>portchannel</b> &lt;trunk identifier&gt;}</p> <p>Enables or disables the selected port/portchannel as an OpenFlow edge port/portchannel (outside port/portchannel). Edge ports/portchannels are usually connected to servers.</p> <p>The default settings is disabled.</p> <p><b>Note:</b> Learning is turned on and flood blocking is turned on in OpenFlow edge ports.</p> <p><b>Command mode:</b> OpenFlow instance</p>
<p><b>emergency</b> [<b>timeout</b> &lt;0-3600&gt;]</p> <p>Forces the instance in emergency mode.</p> <p>The <code>timeout</code> parameter configures the duration in seconds after which the emergency mode expires.</p> <p>The default value is 30.</p> <p><b>Note:</b> Supported only in OpenFlow 1.0.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

**Table 369.** *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
<p><b>no emergency [timeout]</b></p> <p>Brings the instance out of emergency mode.</p> <p>The <code>timeout</code> parameter resets the emergency mode duration to the default value of 30.</p> <p><b>Note:</b> Supported only in OpenFlow 1.0.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>[no] enable</b></p> <p>Enables or disables the instance. When disabling an instance, its flow tables and statistics are cleared.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>max-flow-acl &lt;0-750/1000&gt;</b></p> <p>Enables or disables the maximum flow ACL option, which ensures a dedicated maximum number of ACL flows are available for the instance. The maximum number of entries is 750 in Hybrid mode and 1000 in OpenFlow Only mode. The total number of 750/1000 entries is shared between instances. By default, <code>max-flow-acl</code> is set to 0, allowing instances to dynamically access the available ACL flow slots until depletion. Setting <code>max-flow-acl</code> manually limits the number of ACL flow slots available for other instances by the corresponding value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>max-flow-mcast-fdb &lt;0-4096&gt;</b></p> <p>Enables or disables the maximum flow multicast FDB option, which ensures a dedicated maximum number of FDB multicast flows are available for the instance. The total number of 4096 entries is shared between instances. By default, <code>max-flow-mcast-fdb</code> is set to 0, allowing instances to dynamically access the available FDB multicast flow slots until depletion. Setting <code>max-flow-mcast-fdb</code> manually limits the number of FDB multicast flow slots available for other instances by the corresponding value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>max-flow-mpls-pop &lt;0-1000&gt;</b></p> <p>Enables or disables the maximum flow MPLS pop option, which ensures a dedicated maximum number of MPLS label pop flows are available for the instance. The total number of 1000 entries is shared between instances. By default, <code>max-flow-mpls-pop</code> is set to 0, allowing instances to dynamically access the available MPLS label pop flow slots until depletion. Setting <code>max-flow-mpls-pop</code> manually limits the number of MPLS label pop flow slots available for other instances by the corresponding value.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

**Table 369.** *OpenFlow Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>max-flow-mpls-push</b> &lt;0-2000&gt;</p> <p>Enables or disables the maximum flow MPLS push option, which ensures a dedicated maximum number of MPLS label push flows are available for the instance. The total number of 2000 entries is shared between instances. By default, <code>max-flow-mpls-push</code> is set to 0, allowing instances to dynamically access the available MPLS label push flow slots until depletion. Setting <code>max-flow-mpls-push</code> manually limits the number of MPLS label push flow slots available for other instances by the corresponding value.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>max-flow-ucast-fdb</b> &lt;0-123904&gt;</p> <p>Enables or disables the maximum flow unicast FDB option, which ensures a dedicated maximum number of FDB unicast flows available for the instance. The total number of 123904 entries is shared between instances. By default, <code>max-flow-ucast-fdb</code> is set to 0, allowing instances to dynamically access the available FDB unicast flow slots until depletion. Setting <code>max-flow-ucast-fdb</code> manually limits the number of FDB unicast flow slots available for other instances by the corresponding value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no max-flow-acl</b></p> <p>Sets the instance's maximum number of ACL based flows to the default value of 0 (dynamic allocation).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no max-flow-mcast-fdb</b></p> <p>Sets the instance's maximum number of FDB based multicast flows to the default value of 0 (dynamic allocation).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no max-flow-ucast-fdb</b></p> <p>Sets the instance's maximum number of FDB based unicast flows to the default value of 0 (dynamic allocation).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no max-flow-mpls-pop</b></p> <p>Sets the instance's maximum number of MPLS label pop flows to the default value of 0 (dynamic allocation).</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>



**Table 369.** *OpenFlow Configuration Options (continued)*

<b>Command Syntax and Usage</b>	
<b>no max-flow-mps-push</b>	<p>Sets the instance's maximum number of MPLS label push flows to the default value of 0 (dynamic allocation).</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<b>[no] member {&lt;ports&gt; portchannel &lt;1-64&gt;}</b>	<p>Enables or disables port or static portchannel usage by the OpenFlow instance for data traffic.</p> <p><b>Note:</b> Static portchannels are supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<b>min-flow-timeout &lt;0-300&gt;</b>	<p>Sets the minimum number of seconds after which a flow can be cleared from the instance's tables.</p> <p>The default value is 0, meaning controller provided values are used instead.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<b>no min-flow-timeout</b>	<p>Sets the number of seconds after which a flow can be cleared from the instance's tables to the default value of 0 (controller provided values).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<b>[no] table-miss controller</b>	<p>Sets or disables the <code>table-miss</code> flow entry to send packets unmatched by any flow entries to the controller.</p> <p>The default value is <code>disabled</code>, meaning packets unmatched by flow entries are dropped.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<b>table-miss cookie &lt;0x0-0xffffffff&gt;</b>	<p>Sets the flow cookie for packets sent to controller as a result of a <code>table-miss</code> setting (send input packets that don't match any flow entries to controller).</p> <p>The default value is <code>0xffffffff</code>.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<b>no table-miss cookie</b>	<p>Resets the <code>table-miss</code> flow cookie to the default value of <code>0xffffffff</code>.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

**Table 369.** *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
<p><b>mirror-to-controller cookie</b> &lt;0x0-0xffffffff&gt;</p> <p>Sets the flow cookie for packets sent to controller as a result of a mirror-to-controller setting (flow is set to output the packet to a controller in addition to another destination).</p> <p>The default value is 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no mirror-to-controller cookie</b></p> <p>Resets the mirror-to-controller flow cookie to the default value of 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>send-to-controller cookie</b> &lt;0x0-0xffffffff&gt;</p> <p>Sets the flow cookie for packets sent to controller as a result of a send-to-controller setting (flow is set to output the packet only to a controller).</p> <p>The default value is 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>no send-to-controller cookie</b></p> <p>Resets the send-to-controller flow cookie to the default value of 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>[no] openflow fdb-aging</b></p> <p>Enables or disables periodical clearing of dynamically learned FDB entries on a specific port.</p> <p>On OpenFlow edge ports, the default value is <code>disabled</code>.</p> <p><b>Command mode:</b> Interface port</p>
<p><b>[no] openflow static-station-move</b></p> <p>Enables or disables forwarding frames that have source MAC addresses conflicting with entries in the static FDB table. This enables equal cost multi-path routing and use cases where IPS and Firewall devices forward packets without changing the source MAC address.</p> <p>The default value is <code>disabled</code>.</p> <p><b>Command mode:</b> Interface port</p>

**Table 369.** *OpenFlow Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>show openflow [flow-allocation group information table]</b></p> <p>Displays the current OpenFlow configuration. For more information, see <a href="#">page 145</a>.</p> <ul style="list-style-type: none"><li>o <b>flow-allocation</b> displays the current and maximum number of flows for each OpenFlow instance. For more information, see <a href="#">page 147</a>.</li><li>o <b>group</b> displays group information for all OpenFlow 1.3 instances. For more information, see <a href="#">page 149</a>.</li><li>o <b>information</b> displays the configuration for each OpenFlow instance. For more information, see <a href="#">page 145</a>.</li><li>o <b>table</b> displays the basic, emergency and static flow tables for each OpenFlow instance in OpenFlow 1.0. In OpenFlow 1.3, displays the dynamic and static flow tables. For more information, see <a href="#">page 152</a>.</li></ul> <p><b>Command mode:</b> All</p>
<p><b>show openflow instance &lt;1-2&gt; [group information table]</b></p> <p>Displays OpenFlow information for the specified instance ID:</p> <ul style="list-style-type: none"><li>o <b>group</b> displays group information per instance.</li><li>o <b>information</b> displays the instance configuration</li><li>o <b>table</b> displays the basic, emergency and static flow tables in OpenFlow 1.0. In OpenFlow 1.3, displays the dynamic and static flow tables.</li></ul> <p><b>Command mode:</b> All</p>

**Table 369.** *OpenFlow Configuration Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>clear openflow {group table [basic dynamic emergency static]}</b></p> <p>Clears OpenFlow data for all instances:</p> <ul style="list-style-type: none"><li>o The <b>group</b> option clears the OpenFlow 1.3 group table.</li><li>o The <b>table</b> option clears all basic, emergency and static flow tables in OpenFlow 1.0. In OpenFlow 1.3, clears the dynamic and static flow tables.<ul style="list-style-type: none"><li>• The <b>basic</b> option clears only the basic OpenFlow tables.</li><li>• The <b>emergency</b> option clears only the emergency OpenFlow tables.</li><li>• The <b>static</b> option clears only the static OpenFlow tables.</li><li>• The <b>dynamic</b> option clears only the dynamic OpenFlow tables.</li></ul></li></ul> <p><b>Command mode:</b> Privileged EXEC</p>
<p><b>clear openflow instance &lt;1-2&gt; {group table [basic dynamic emergency static]}</b></p> <p>Clears OpenFlow data for the specified instance ID:</p> <ul style="list-style-type: none"><li>o The <b>group</b> option clears the OpenFlow 1.3 group table.</li><li>o The <b>table</b> option clears all basic, emergency and static flow tables in OpenFlow 1.0. In OpenFlow 1.3, clears the dynamic and static flow tables.<ul style="list-style-type: none"><li>• The <b>basic</b> option clears only the basic OpenFlow table.</li><li>• The <b>emergency</b> option clears only the emergency OpenFlow table.</li><li>• The <b>static</b> option clears only the static OpenFlow table.</li><li>• The <b>dynamic</b> option clears only the dynamic OpenFlow table.</li></ul></li></ul> <p><b>Command mode:</b> Privileged EXEC</p>

## Static Flows Configuration

Static flows are OpenFlow entries set up manually from the CLI by the administrator. Static flows cannot be deleted/modified by OpenFlow controllers and will continue to function when the switch goes into emergency mode. Even if they qualify as FDB entries based on their settings, in version 1.0 of the OpenFlow standard, static flows are always stored as ACL entries. A total of maximum 750 static flows pool is shared between all OpenFlow instances.

Table 370 describes the static flow configuration options.

**Table 370.** *Static Flows Configuration Options*

Command Syntax and Usage
<p><b>static-table add index</b> &lt;1-750&gt; <b>match</b> &lt;matching qualifier&gt; <b>actions</b> &lt;matching qualifier&gt; [<b>options</b> &lt;matching qualifier&gt;] <b>priority</b> &lt;0-65535&gt;</p> <p>Adds a static flow entry to the instance.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>static-table modify index</b> &lt;1-750&gt; <b>match</b> &lt;matching qualifier&gt; <b>actions</b> &lt;matching qualifier&gt; [<b>options</b> &lt;matching qualifier&gt;] <b>priority</b> &lt;0-65535&gt;</p> <p>Overwrites a static flow entry.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>static-table remove index</b> &lt;1-750&gt;</p> <p>Deletes a static flow entry.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<p><b>clear openflow table static</b></p> <p>Deletes all static flow entries.</p> <p><b>Command mode:</b> Global configuration</p>

The following table describes the available matching qualifiers.

**Table 371.** *Static Flow Matching Qualifiers in OpenFlow 1.0*

Qualifier	Value
ingress-port	Port of instance
src-mac	Source MAC address
dst-mac	Destination MAC address
vlan-id	VLAN identifier (0-4095 + 65535 (untagged))
vlan-priority	802.1p Priority Code Point (0-7)
src-ip	Source IP address
dst-ip	Destination IP address
src-port	L4 source port (0-65536)
dst-port	L4 destination port (0-65535)

**Table 371.** *Static Flow Matching Qualifiers in OpenFlow 1.0 (continued)*

Qualifier	Value
ether-type	"arp"/"0806" or "ip"/"0800" or (hex-value <= 65535)
protocol	"tcp" or "udp" or 0-255
tos	IP Type of Service (0-255)
type	"request" or "reply" (can be set only if ether type is ARP)
all	Applicable to all traffic

**Table 372.** *Static Flow Matching Qualifiers in OpenFlow 1.3*

Qualifier	Value
in-port	switch input port
in-phy-port	switch physical input port, valid only when in-port is specified
eth-src	source MAC address and mask
eth-dst	destination MAC address and mask
vlan-vid	VLAN identifier ("untagged", "tagged", or <0-4094>)
vlan-pcp	802.1p(0-7)
ipv4-src	source IPv4 address and mask
ipv4-dst	destination IPv4 address and mask
tcp-src	TCP source port (0-65535)
tcp-dst	TCP destination port (0-65535)
udp-src	UDP source port (0-65535)
udp-dst	UDP destination port (0-65535)
icmpv4-type	ICMPv4 type
icmpv4-code	ICMPv4 code
eth-type	"arp"/"0806" or "ip"/"0800" or (hex-value <=65535)
ip-proto	"tcp" or "udp" or 0-255
ip-dscp	IP DSCP (6 bits in ToS field)
arp-op	"request" or "reply" (can be set only if eth-type is ARP)
mpls-label	MPLS label
all	all qualifiers or any qualifier

The following table describes the available actions,

**Table 373.** *Static Flow Actions in OpenFlow 1.0*

Action	Value
out-put	"all","in-port","flood","controller" or a valid port
set-src-mac	Change source MAC address
set-dst-mac	Change destination MAC address
strip-vlan-id	Remove VLAN identifier
set-vlan-priority	Set 802.1p priority code point value (0-7)
set-nw-tos	Set IP Type of Service (0-255)
drop	Drop packet
max-len	Maximum length to send to controller
set-vlan-id	Set VLAN ID

**Table 374.** *Static Flow Actions in OpenFlow 1.3*

Action	Value
out-put	"all","in-port","flood","controller" or a valid port
set-src-mac	change source MAC address
set-dst-mac	change destination MAC address
push-vlan	push a new VLAN tag
pop-vlan	pop the outer VLAN tag
push-mpls-label	push a new MPLS tag
set-vlan-id	set VLAN ID
set-vlan-priority	set 802.1p priority (0-7)
set-nw-tos	set IP TOS (0-255)
ttl-set	set MPLS TTL
copy-ttl-out	copy TTL outward - from next-to-outermost to outermost
copy-ttl-in	copy TTL inward - from outermost to next-to-outermost
drop	drop the packet

---

## Switch Partition (SPAR) Configuration

Switch partitions (SPARs) divide the data plane inside a physical switch into independent switching domains. Switch partitions do not communicate with each other, forcing hosts on different SPARs to bridge traffic over an upstream link, even if they belong to the same VLAN.

Up to 8 SPARs can be defined on a switch. Each SPAR supports up to 32 local VLANs, for further partitioning flexibility.

**Table 375.** *SPAR Configuration Options*

<b>Command Syntax and Usage</b>
<b>spar</b> <1-8> Enters SPAR Configuration mode. <b>Command mode:</b> Global configuration
<b>no spar</b> <1-8> Deletes the specified SPAR. <b>Command mode:</b> Global configuration
<b>[no] enable</b> Enables or disables the SPAR. <b>Command mode:</b> SPAR Configuration
<b>name</b> Configures the SPAR name. <b>Command mode:</b> SPAR Configuration
<b>domain default {vlan &lt;2-4094&gt; member &lt;port no.&gt;}</b> Configures the SPAR's default domain settings: <ul style="list-style-type: none"><li>o <b>vlan</b> configures the default SPAR VLAN ID. A unique factory default VLAN ID is assigned to each SPAR as "408x", where x is the SPAR ID &lt;1-8&gt;. This option provides an override if conflicts arise with a customer VLAN ID on the upstream network.</li><li>o <b>member</b> adds server ports to the SPAR.</li></ul> <b>Command mode:</b> SPAR Configuration
<b>no domain default member</b> <port no.> Removes server ports from the SPAR. <b>Command mode:</b> SPAR Configuration



**Table 375.** SPAR Configuration Options (continued)

Command Syntax and Usage
<p><b>domain local</b> &lt;1-32&gt; {<b>enable</b> <b>member</b> &lt;port no.&gt; <b>name</b> &lt;text&gt; <b>vlan</b> &lt;2-4094&gt;}</p> <p>Configures the SPAR's local domains:</p> <ul style="list-style-type: none"> <li>o <b>enable</b> enables the SPAR local domains</li> <li>o <b>member</b> adds server ports to the SPAR local domains</li> <li>o <b>name</b> configures the SPAR local domains names</li> <li>o <b>vlan</b> applies a VLAN ID to the SPAR local domains. The default value is 0.</li> </ul> <p><b>Command mode:</b> SPAR Configuration</p>
<p><b>no domain local</b> &lt;1-32&gt; [<b>enable</b> <b>member</b> &lt;port no.&gt; <b>vlan</b>]</p> <p>Deletes the SPAR local VLAN domains:</p> <ul style="list-style-type: none"> <li>o <b>enable</b> disables the SPAR local domains</li> <li>o <b>member</b> deletes SPAR local domains server ports</li> <li>o <b>vlan</b> deletes SPAR local domains vlan.</li> </ul> <p><b>Command mode:</b> SPAR Configuration</p>
<p><b>domain mode</b> {<b>passthrough</b> <b>local</b>}</p> <p>Configures the SPAR domain mode:</p> <ul style="list-style-type: none"> <li>o <b>passthrough</b> references member ports only by the SPAR default VLAN. This provides VLAN-unaware uplink connectivity via pass-through tunnel domain switching for SPAR member ports. The default value is passthrough.</li> <li>o <b>local</b> references member ports by both SPAR default VLAN and SPAR local domain VLANs. This provides VLAN-aware uplink connectivity via local domain switching for SPAR member ports</li> </ul> <p><b>Command mode:</b> SPAR Configuration</p>
<p><b>[no] uplink</b> {<b>port</b> &lt;port no.&gt; <b>portchannel</b> &lt;1-64&gt; <b>adminkey</b> &lt;1-65535&gt;}</p> <p>Enables or disables uplink connectivity for the SPAR. A single external port, portchannel, or LACP channel can be used for uplink. All uplinks within a SPAR are automatically assigned to the SPAR domain's default VLAN and to any SPAR local VLANs.</p> <p><b>Command mode:</b> SPAR Configuration</p>
<p><b>show spar</b> &lt;1-8&gt; [<b>domain</b> [<b>default</b> <b>local</b> &lt;1-32&gt;] <b>uplink</b>]</p> <p>Displays the SPAR settings:</p> <ul style="list-style-type: none"> <li>o <b>domain</b> filters only the SPAR domain related settings <ul style="list-style-type: none"> <li>• <b>default</b> filters only SPAR default domain settings</li> <li>• <b>local</b> &lt;1-32&gt; filters only SPAR local domains settings</li> </ul> </li> <li>o <b>uplink</b> filters only SPAR uplink settings</li> </ul> <p><b>Command mode:</b> All</p>

---

## Precision Time Protocol Configuration

Precision Time Protocol (PTP) allows high accuracy clock synchronization between a networked master clock and compliant network hosts. The Lenovo Flex System EN4093R 10Gb Ethernet Scalable Switch supports two PTP modes:

- Ordinary slave clock - Synchronizes the Real Time Clock (RTC) with PTP master clocks detected on the network.
- End-to-End transparent clock - Allows PTP traffic to pass through without affecting the RTC, while updating the correction fields for event packets.

**Table 376.** Precision Time Protocol Configuration Options

Command Syntax and Usage
<p><b>[no] ptp ordinary enable</b></p> <p>Enables or disables PTP ordinary slave clock mode. In this mode, if a PTP master clock is detected on the network, the RTC is synchronized with it. If no master clock is detected, the RTC is not affected. Default setting is disabled.</p> <p><b>Note:</b> Enabling PTP ordinary slave clock mode disables NTP settings and system time clock manual settings.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] ptp transparent enable</b></p> <p>Enables or disables PTP End-to-End transparent clock mode. In this mode, incoming PTP packets are forwarded based on routing rules currently in place for the PTP domain's multicast address (within the 224.0.1.129 - 224.0.1.132 range). On egress, PTP packet timestamps are updated based on the time spent between ingress and egress.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ptp</b></p> <p>Disables both PTP ordinary slave clock mode and PTP End-to-End transparent clock mode.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>ip ptp source-interface loopback &lt;1-5&gt;</b></p> <p>Loopback interface used as source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode. By default, the interface with the lowest index from the master clock's VLAN is used.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no ip ptp source-interface loopback</b></p> <p>Sets the source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode to the interface with the lowest index from the master clock's VLAN.</p> <p><b>Command mode:</b> Global configuration</p>

**Table 376.** Precision Time Protocol Configuration Options (continued)

<b>Command Syntax and Usage</b>
<b>[no] ptp</b> Enables or disables PTP on the current port. Disabled ports will not support PTP even if PTP is globally enabled. The default setting is enabled. <b>Note:</b> PTP is not supported on management ports. <b>Command mode:</b> Interface port
<b>clear ptp counters</b> Resets PTP packet counters. <b>Command mode:</b> Privileged EXEC
<b>show ptp [counters]</b> Displays current PTP settings. The counters option displays PTP packet counters. See <a href="#">page 316</a> for details. <b>Command mode:</b> All
<b>show interface port &lt;port alias or number&gt; ptp-counters</b> Displays Precision Time Protocol statistics for the port. See <a href="#">page 316</a> for details. <b>Command mode:</b> All

---

## Service Location Protocol Configuration

Service Location Protocol (SLP) enables networked devices to request/announce services over a local area network without prior configuration. In an SLP environment, devices may have the following roles:

- User Agents (UA) are devices requesting services.
- Service Agents (SA) are devices providing services.
- Directory Agents (DA) are devices caching services provided by SAs. When present in an SLA setup, DAs mediate all communication between UAs and SAs.

When SLP is enabled, the EN4093R 10Gb Ethernet Scalable Switch behaves as a Service Agent providing systems management services.

**Table 377.** *Service Location Protocol Options*

<b>Command Syntax and Usage</b>
<b>[no] ip slp enable</b> Enables or disables SLP. The default value is <code>disabled</code> . <b>Command mode:</b> Global configuration
<b>[no] ip slp active-da-discovery enable</b> Enables or disables active directory agent discovery. The default value is <code>disabled</code> . <b>Command mode:</b> Global configuration
<b>ip slp active-da-discovery-start-wait-time</b> <1-10> Number of seconds to wait after enabling SLP before attempting active DA discovery, if active DA discovery is enabled. The default value is 3. <b>Command mode:</b> Global configuration
<b>clear ip slp directory-agents</b> Clears directory agents discovered. <b>Command mode:</b> Privileged EXEC
<b>clear ip slp counters</b> Clears Service Location Protocol counters. <b>Command mode:</b> Privileged EXEC

---

## Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
EN 4093(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP, as described on [page 607](#).

---

## Saving the Active Switch Configuration

When the **copy running-config {ftp|tftp|sftp}** command is used, the switch's active configuration commands (as displayed using **show running-config**) will be uploaded to the specified script configuration file on the FTP/TFTP/SFTP server. To start the switch configuration upload, at the prompt, enter:

```
EN 4093(config)# copy running-config ftp [data-port|extm-port|mgt-port]
```

or:

```
EN 4093(config)# copy running-config tftp [data-port|extm-port|mgt-port]
```

or:

```
EN 4093(config)# copy running-config sftp [data-port|extm-port|mgt-port]
```

Select a port, or press **Enter** to use the default (management port). The switch prompts you for the server address and filename.

### Notes:

- The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).
- If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified configuration file must exist prior to executing the **copy running-config** command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

---

## Restoring the Active Switch Configuration

When the **copy {ftp|tftp|sftp} running-config** command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration.

To start the switch configuration download, at the prompt, enter:

```
EN 4093(config)# copy ftp running-config [data-port|extm-port|mgt-port]
```

or:

```
EN 4093(config)# copy tftp running-config [data-port|extm-port|mgt-port]
```

or:

```
EN 4093(config)# copy sftp running-config [data-port|extm-port|mgt-port]
```

Select a port, or press **Enter** to use the default (management port). The switch prompts you for the server address and filename.





---

## Chapter 5. Operations Commands

Operations commands generally affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use Operations commands to immediately disable a port (without the need to apply or save the change), with the understanding that when the switch is reset, the port returns to its normally configured operation.

These commands enable you to alter switch operational characteristics without affecting switch configuration.

**Table 378.** *General Operations Commands*

<b>Command Syntax and Usage</b>
<p><b>password</b> &lt;1-128 characters&gt;</p> <p>Allows the user to change the password. You must enter the current password in use for validation. The switch prompts for a new password between 1-128 characters.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<p><b>clear logging</b></p> <p>Clears all Syslog messages.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<p><b>ntp send</b></p> <p>Allows the user to send requests to the NTP server.</p> <p><b>Command Mode:</b> Privileged EXEC</p>

---

## Operations-Level Port Commands

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

**Table 379.** *Port Operations Commands*

Command Syntax and Usage
<p><b>no interface port</b> &lt;port number or alias&gt; <b>shutdown</b></p> <p>Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<p><b>interface port</b> &lt;port number or alias&gt; <b>shutdown</b></p> <p>Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<p><b>[no] interface portchannel</b> &lt;1-128&gt; <b>shutdown</b></p> <p>Temporarily enables or disables the specified port channel. The port channel will be returned to its configured operation mode when the switch is reset.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<p><b>[no] interface portchannel lacp</b> &lt;1-65535&gt; <b>shutdown</b></p> <p>Temporarily enables or disables specified LACP trunk groups.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<p><b>show interface port</b> &lt;port number or alias&gt; <b>operation</b></p> <p>Displays the port interface operational state.</p> <p><b>Command Mode:</b> Privileged EXEC</p>

---

## Operations-Level Port 802.1X Commands

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

**Table 380.** *802.1X Operations Commands*

Command Syntax and Usage
<p><b>interface port</b> <i>&lt;port number or alias&gt;</i> <b>dot1x init</b></p> <p>Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration:</p> <ul style="list-style-type: none"><li>o <b>force unauth</b>: the port is placed in unauthorized state, and traffic is blocked.</li><li>o <b>auto</b>: the port is placed in unauthorized state, then authentication is initiated.</li><li>o <b>force auth</b>: the port is placed in authorized state, and authentication is not required.</li></ul> <p><b>Command Mode:</b> Privileged EXEC</p>
<p><b>interface port</b> <i>&lt;port number or alias&gt;</i> <b>dot1x re-authenticate</b></p> <p>Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as <b>auto</b>.</p> <p><b>Command Mode:</b> Privileged EXEC</p>

---

## Operations-Level VRRP Commands

The following table displays Virtual Router Redundancy operations commands.

**Table 381.** *Virtual Router Redundancy Operations Commands*

Command Syntax and Usage
<p><b>router vrrp backup</b> &lt;virtual router number (1-255)&gt;</p> <p>Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:</p> <ul style="list-style-type: none"><li>o This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)</li><li>o This switch's virtual router has a higher priority and preemption is enabled.</li><li>o There are no other virtual routers available to take master control.</li></ul> <p><b>Command Mode:</b> Privileged EXEC</p>

---

## Operations-Level BGP Commands

The following table displays IP BGP operations commands.

**Table 382.** *IP BGP Operations Commands*

Command Syntax and Usage
<b>router bgp start</b> <1-12> Starts the peer session. <b>Command Mode:</b> Privileged EXEC
<b>router bgp stop</b> <1-12> Stops the peer session. <b>Command Mode:</b> Privileged EXEC
<b>show ip bgp state</b> Displays the current BGP operational state. <b>Command Mode:</b> Privileged EXEC

---

## Protected Mode Options

Protected Mode is used to secure certain switch management options, so they cannot be changed by the management module.

**Table 383.** *Protected Mode Options*

Command Syntax and Usage
<p><b>[no] protected-mode enable</b></p> <p>Enables or disables Protected Mode. When Protected Mode is <b>enabled</b>, the switch takes exclusive local control of all enabled options. When Protected Mode is <b>disabled</b>, the switch relinquishes exclusive local control of all enabled options.</p> <p><b>Command Mode:</b> Global Configuration</p>
<p><b>[no] protected-mode external-management</b></p> <p>Enables exclusive local control of switch management. When Protected Mode is set to <b>on</b>, the management module cannot be used to disable external management on the switch.</p> <p>The default value is <b>enabled</b>.</p> <p><b>Note:</b> Due to current management module implementation, this setting cannot be disabled.</p> <p><b>Command Mode:</b> Global Configuration</p>
<p><b>[no] protected-mode external-ports</b></p> <p>Enables exclusive local control of external ports. When Protected Mode is set to <b>on</b>, the management module cannot be used to disable external ports on the switch.</p> <p>The default value is <b>enabled</b>.</p> <p><b>Note:</b> Due to current management module implementation, this setting cannot be disabled.</p> <p><b>Command Mode:</b> Global Configuration</p>
<p><b>[no] protected-mode factory-default</b></p> <p>Enables exclusive local control of factory default resets. When Protected Mode is set to <b>on</b>, the management module cannot be used to reset the switch software to factory default values.</p> <p>The default value is <b>enabled</b>.</p> <p><b>Note:</b> Due to current management module implementation, this setting cannot be disabled.</p> <p><b>Command Mode:</b> Global Configuration</p>

**Table 383.** *Protected Mode Options (continued)*

<b>Command Syntax and Usage</b>
<p><b>[no] protected-mode management-vlan-interface</b></p> <p>Enables exclusive local control of the management interface. When Protected Mode is set to on, the management module cannot be used to configure parameters for the management interface.</p> <p>The default value is enabled.</p> <p><b>Note:</b> Due to current management module implementation, this setting cannot be disabled.</p> <p><b>Command Mode:</b> Global Configuration</p>
<p><b>show protected-mode</b></p> <p>Displays the current Protected Mode configuration.</p> <p><b>Command Mode:</b> Global Configuration</p>

---

## VMware Operations

Use these commands to perform minor adjustments to the VMware operation. Use these commands to perform Virtual Switch operations directly from the switch. Note that these commands require the configuration of Virtual Center access information (**virt vmware vcspec**).

**Table 384.** *VMware Operations Commands*

Command Syntax and Usage
<p><b>virt vmware pg</b> [<i>&lt;Port Group name&gt; &lt;host ID&gt; &lt;VSwitch name&gt; &lt;VLAN number&gt; &lt;shaping-enabled&gt; &lt;average-Kbps&gt; &lt;burst-KB&gt; &lt;peak-Kbps&gt;</i>]</p> <p>Adds a Port Group to a VMware host. You are prompted for the following information:</p> <ul style="list-style-type: none"><li>o Port Group name</li><li>o VMware host ID (Use host UUID, host IP address, or host name.)</li><li>o Virtual Switch name</li><li>o VLAN ID of the Port Group</li><li>o Whether to enable the traffic-shaping profile (1 or 0). If you choose 1 (yes), you are prompted to enter the traffic shaping parameters.</li></ul> <p><b>Command Mode:</b> All</p>
<p><b>no virt vmware pg</b> <i>&lt;Port Group name&gt; &lt;host ID&gt;</i></p> <p>Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"><li>o UUID</li><li>o IP address</li><li>o Host name</li></ul> <p><b>Command Mode:</b> All</p>
<p><b>[no] virt vmware vsw</b> <i>&lt;host ID&gt; &lt;Virtual Switch name&gt;</i></p> <p>Adds or removes a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"><li>o UUID</li><li>o IP address</li><li>o Host name</li></ul> <p><b>Command Mode:</b> All</p>



**Table 384.** *VMware Operations Commands (continued)*

<b>Command Syntax and Usage</b>
<p><b>virt vmware export</b> <i>&lt;VM profile name&gt;</i> <i>&lt;VMware host ID&gt;</i> <i>&lt;Virtual Switch name&gt;</i></p> <p>Exports a VM Profile to a VMware host.</p> <p>Use one of the following identifiers to specify each host:</p> <ul style="list-style-type: none"><li>o UUID</li><li>o IP address</li><li>o Host name</li></ul> <p>You may enter a Virtual Switch name, or enter a new name to create a new Virtual Switch.</p> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware scan</b></p> <p>Performs a scan of the VM Agent, and updates VM information.</p> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware vmacpg</b> <i>&lt;MAC address&gt;</i> <i>&lt;Port Group name&gt;</i></p> <p>Changes a VM NIC's configured Port Group.</p> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware updp</b> <i>&lt;Port Group name&gt;</i> <i>&lt;host ID&gt;</i> <i>&lt;VLAN number&gt;</i> <i>[&lt;shaping enabled&gt; &lt;average Kbps&gt; &lt;burst KB&gt; &lt;peak Kbps&gt;]</i></p> <p>Updates a VMware host's Port Group parameters.</p> <p><b>Command Mode:</b> All</p>

## VMware Distributed Virtual Switch Operations

Use these commands to administer a VMware Distributed Virtual Switch (dvSwitch).

**Table 385.** *VMware dvSwitch Operations (loper/virt/vmware/dvswitch)*

Command Syntax and Usage
<p><b>virt vmware dvswitch add</b> &lt;datacenter name&gt; &lt;dvSwitch name&gt; &lt;dvSwitch version&gt;</p> <p>Adds the specified dvSwitch to the specified DataCenter.</p> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dvswitch del</b> &lt;datacenter name&gt; &lt;dvSwitch name&gt;</p> <p>Removes the specified dvSwitch from the specified DataCenter.</p> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dvswitch addhost</b> &lt;dvSwitch name&gt; {&lt;host UUID    IP address  host name&gt;}</p> <p>Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> <li>o UUID</li> <li>o IP address</li> <li>o Host name</li> </ul> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dvswitch remhost</b> &lt;dvSwitch name&gt; {&lt;host UUID    IP address  host name&gt;}</p> <p>Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> <li>o UUID</li> <li>o IP address</li> <li>o Host name</li> </ul> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dvswitch addUplink</b> &lt;dvSwitch name&gt; &lt;host ID&gt; &lt;uplink name&gt;</p> <p>Adds the specified physical NIC to the specified dvSwitch uplink ports.</p> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dvswitch remUplink</b> &lt;dvSwitch name&gt; &lt;host ID&gt; &lt;uplink name&gt;</p> <p>Removes the specified physical NIC from the specified dvSwitch uplink ports.</p> <p><b>Command Mode:</b> All</p>

## VMware Distributed Port Group Operations

Use these commands to administer a VMware distributed port group.

**Table 386.** VMware Distributed Port Group Operations (*/oper/virt/vmware/dpg*)

Command Syntax and Usage
<p><b>virt vmware dpg add</b> &lt;port group name&gt; &lt;dvSwitch name&gt; &lt;VLAN ID&gt;  <b>[ishaping</b> &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;]  <b>[eshaping</b> &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;]</p> <p>Adds the specified port group to the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none"> <li>o <b>ishaping</b>: Enables ingress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> <li>o <b>eshaping</b>: Enables egress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> </ul> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dpg vmac</b> &lt;VNIC MAC&gt; &lt;port group name&gt;</p> <p>Adds the specified VM NIC to the specified port group.</p> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dpg update</b> &lt;port group name&gt; &lt;dvSwitch name&gt; &lt;VLAN ID&gt;  <b>[ishaping</b> &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;]  <b>[eshaping</b> &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;]</p> <p>Updates the specified port group on the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none"> <li>o <b>ishaping</b>: Enables ingress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> <li>o <b>eshaping</b>: Enables egress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> </ul> <p><b>Command Mode:</b> All</p>
<p><b>virt vmware dpg del</b> &lt;port group name&gt; &lt;dvSwitch name&gt;</p> <p>Removes the specified port group from the specified dvSwitch.</p> <p><b>Command Mode:</b> All</p>

---

## Edge Virtual Bridge Operations

Edge Virtual Bridge operations commands are listed in the following table:

**Table 387.** *Edge Virtual Bridge Operations Commands*

Command Syntax and Usage
<b>virt evb update vsidb</b> <VSIDB_number> Update VSI types from the VSI database. <b>Command mode:</b> All
<b>clear virt evb vsidb</b> [ <b>mgrid</b> <0-255>  <b>typeid</b> <1-16777215>  <b>version</b> <0-255>] Clears local VSI types cache. <b>Command mode:</b> Privileged EXEC
<b>clear virt evb vsi</b> [ <b>mac-address</b>   <b>port</b> <port alias or number>  <b>type-id</b> <1-16777215>  <b>vlan</b> <1-4094>] Clears VSI database associations. <b>Command mode:</b> Privileged EXEC

---

## Feature on Demand Key Options

Use the license key to upgrade the port mode. Base port mode is the default. To upgrade the port mode, you must obtain a software license key.

After selecting a port mode, you must reset the switch for the change to take affect. Use the following command to verify the port configuration:

**show interface information**

**Table 388.** *Feature on Demand Key Options*

Command Syntax and Usage
<p><b>software-key</b></p> <p>Enter FOD Key mode.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<p><b>enakey address</b> <i>&lt;hostname or IP address&gt;</i> <b>keyfile</b> <i>&lt;file name&gt;</i> <b>protocol {tftp sftp} mgt</b></p> <p>Unlocks the software port expansion feature. You are prompted to enter the host name or IP address of the server where the license key is stored, and the license key file name, as follows:</p> <ul style="list-style-type: none"><li>o 46Port</li><li>o 64Port</li></ul> <p><b>Note:</b> You must upgrade to 46Port port mode before you can upgrade to 64Port port mode.</p> <p><b>Command mode:</b> FOD Key mode</p> <p>Use the following command to perform the same action, regardless the command mode:</p> <p><b>copy tftp software-key address</b> <i>&lt;hostname or IP address&gt;</i> <b>keyfile</b> <i>&lt;file name&gt;</i> <b>mgt</b></p>
<p><b>ptkey address</b> <i>&lt;hostname or IP address&gt;</i> <b>key</b> <i>&lt;feature name&gt;</i> <b>protocol {tftp sftp} file</b> <i>&lt;file name&gt;</i> <b>mgt</b></p> <p>Loads the specified key file to a server.</p> <p><b>Command mode:</b> FOD Key mode</p> <p>Use the following command to perform the same action, regardless the command mode:</p> <p><b>copy software-key address</b> <i>&lt;hostname or IP address&gt;</i> <b>key</b> <i>&lt;file name&gt;</i> <b>protocol {tftp sftp} file</b> <i>&lt;file name&gt;</i> <b>mgt</b></p>

**Table 388.** *Feature on Demand Key Options*

Command Syntax and Usage
<p><b>invkeys</b> <b>address</b> <i>&lt;hostname or IP address&gt;</i> <b>invfile</b> <i>&lt;file name&gt;</i> <b>protocol {tftp sftp} mgt</b></p> <p>Loads key code inventory information to a server.</p> <p><b>Command mode:</b> FOD Key mode</p> <p>Use the following command to perform the same action, regardless the command mode:</p> <p><b>copy invkeys</b> <b>address</b> <i>&lt;hostname or IP address&gt;</i> <b>invfile</b> <i>&lt;file name&gt;</i> <b>protocol {tftp sftp} mgt</b></p>
<p><b>rmkey</b> <b>key</b> <i>&lt;feature name&gt;</i></p> <p>Removes the specified software feature.</p> <p><b>Command mode:</b> FOD Key mode</p>
<p><b>exit</b></p> <p>Exit from Feature on Demand Key mode.</p> <p><b>Command mode:</b> FOD Key mode</p>
<p><b>show software-key</b></p> <p>Shows software licensing keys.</p> <p><b>Command mode:</b> All</p>

---

## Chapter 6. Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands provide options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Working with Switch Images and Configuration Files” in the *Command Reference*.

The boot options are discussed in the following sections.

## Stacking Boot Options

The Stacking Boot options are used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

You must enable Stacking and reset the switch to enter Stacking mode. When the switch enters Stacking mode, the Stacking configuration menu appears. For more information, see [“Stacking Configuration” on page 381](#).

[Table 389](#) lists the Boot Stacking command options.

**Table 389.** *Boot Stacking Options*

Command Syntax and Usage
<p><b>boot stack mode [master member] [&lt;1-16&gt; all backup master]</b></p> <p>Configures the Stacking mode for the selected switch. This can be applied for:</p> <ul style="list-style-type: none"> <li>o a specific switch &lt;1-16&gt;</li> <li>o all switches</li> <li>o backup switch</li> <li>o master switch</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<p><b>boot stack higr-trunk &lt;list of ports&gt;</b></p> <p>Configures the ports used to connect the switch to the stack.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>boot stack vlan &lt;VLAN number&gt;</b></p> <p>Configures the VLAN used for Stacking control communication.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>default boot stack [master backup &lt;asnum (1-16)&gt; all]</b></p> <p>Resets the Stacking boot parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>boot stack push-image {image1 image2 boot} &lt;asnum (1-16)&gt;</b></p> <p>Pushes the selected software file from the master to the selected switch.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>boot stack enable</b></p> <p>Enables the switch stack.</p> <p><b>Command mode:</b> Global configuration</p>



**Table 389.** *Boot Stacking Options (continued)*

<b>Command Syntax and Usage</b>
<b>no boot stack enable</b> Disables the switch stack. <b>Command mode:</b> Global configuration
<b>show boot stack [master backup &lt;asnum (1-16)&gt; all]</b> Displays current Stacking boot parameters. <b>Command mode:</b> All

When in stacking mode, the following stand-alone features are not supported:

- Border Gateway Protocol (BGP)
- Equal-Cost Multi-Path (ECMP)
- Ethernet Operation, Administration and Maintenance (OAM)
- Explicit Congestion Notification (ECN)
- Internet Group Management Protocol version 3 (IGMPv3)
- Internet Group Management Protocol (IGMP) Querier
- Internet Group Management Protocol (IGMP) Relay
- Internet Group Management Protocol (IGMP) Snooping version 3
- Internet Key Exchange version 2 (IKEv2)
- IP Security (IPsec)
- Internet Protocol version 6 (IPv6)
- Loopback Interfaces
- MAC address notification
- Multicast Listener Discovery (MLD)
- Network Configuration (NETCONF) Protocol
- OpenFlow
- Open Shortest Path First (OSPF)
- Open Shortest Path First version 3 (OSPFv3)
- Port flood blocking
- Precision Time Protocol (PTP)
- EasyConnect (EZC)
- Protocol-based VLANs
- Protocol Independent Multicast (PIM)
- Router IDs
- Route maps
- Routing Information Protocol (RIP)
- sFlow port monitoring

- Spanning Tree Protocol (STP) Root Guard and Loop Guard
- Static MAC address adding
- Static Multicast Routes
- Storm control
- Switch Partition (SPAR)
- Uni-Directional Link Detection (UDLD)
- Virtual Link Aggregation Groups (VLAG)
- Virtual Router Redundancy Protocol (VRRP)

Switch menus and commands for unsupported features may be unavailable, or may have no effect on switch operation.

---

## Scheduled Reboot

This feature allows you to schedule a reboot to occur at a particular time in the future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the currently set reboot schedule.

**Table 390.** *Boot Scheduling Options*

<b>Command Syntax and Usage</b>
<b>boot schedule</b> <i>&lt;day of week&gt;</i> <i>&lt;time of day&gt;</i> Defines the reboot schedule. Enter the day of the week, followed by the time of day (in hh:mm format). For example: <code>boot schedule monday 11:30</code> <b>Command mode:</b> Global configuration
<b>no boot schedule</b> Cancels the next pending scheduled reboot. <b>Command mode:</b> Global configuration
<b>show boot</b> Displays the current reboot scheduling parameters. <b>Command mode:</b> All

---

## Netboot Configuration

Netboot allows the switch to automatically download its configuration file over the network during switch reboot, and apply the new configuration. Upon reboot, the switch includes the following options in its DHCP requests:

- Option 66 (TFTP server address)
- Option 67 (file path)

If the DHCP server returns the information, the switch initiates a TFTP file transfer, and loads the configuration file into the active configuration block. As the switch boots up, it applies the new configuration file. Note that the option 66 TFTP server address must be specified in IP-address format (host name is not supported).

If DHCP is not enabled, or the DHCP server does not return the required information, the switch uses the manually-configured TFTP server address and file path.

**Table 391.** *Netboot Options (/boot/netboot)*

Command Syntax and Usage
<p><b>[no] boot netboot enable</b></p> <p>Enables or disables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] boot netboot tftp</b> &lt;IP address&gt;</p> <p>Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is disabled, or if the DHCP server does not return the required information.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>[no] boot netboot cfgfile</b> &lt;1-31 characters&gt;</p> <p>Defines the file path for the configuration file on the TFTP server. For example: /directory/sub/config.cfg</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show boot</b></p> <p>Displays the current Netboot parameters.</p> <p><b>Command mode:</b> All</p>

---

## Flexible Port Mapping

Depending on the license keys installed on the switch, only a limited number of physical ports might be active. Flexible Port Mapping allows you to alter the default configuration set up by the license, by manually setting up which ports are active or inactive.

Active ports may not collectively exceed the bandwidth limit imposed by the current license level.

[Table 392](#) lists the Flexible Port Mapping command options.

**Table 392.** *Flexible Port Mapping Options*

<b>Command Syntax and Usage</b>
<b>[no] boot port-map</b> <i>&lt;port number or range&gt;</i> Enables or disables the specified ports. <b>Command mode:</b> Global configuration
<b>default boot port-map</b> Reverts the port mapping to the default licensed configuration. <b>Command mode:</b> Global configuration
<b>show boot port-map</b> Displays the total bandwidth available, current port mapping and configured port mapping. <b>Command mode:</b> All

---

## QSFP Port Configuration

Quad Small Form-factor Pluggable Plus (QSFP+) ports are designed to handle high-intensity traffic. Use the following commands to configure QSFP+ ports.

**Table 393.** *Netboot Options (/boot/qsfp-40Gports)*

Command Syntax and Usage
<p><b>[no] boot qsfp-40Gports</b> &lt;ports&gt;</p> <p>Enables or disables 40GbE mode on the selected QSFP+ ports. When enabled, each QSFP+ port is set as a single 40GbE port. When disabled, each QSFP+ port is configured to breakout into four 10GbE ports.</p> <p>You must reboot the switch for this change to take effect.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show boot qsfp-port-modes</b></p> <p>Displays the current QSFP port settings.</p> <p><b>Command mode:</b> All</p>

---

## SIOM Configuration

The Secure Input/Output Module (SIOM) enables you to determine which protocols can be enabled. The SIOM only allows secured traffic and secured authentication management. Use the following commands to configure QSFP+ ports.

**Table 394.** *SIOM Options*

Command Syntax and Usage
<p><b>[no] boot siom</b></p> <p>Enables or disables SIOM on the switch.</p> <p>You must reboot the switch for this change to take effect.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show boot siom</b></p> <p>Displays the current SIOM setting and the SIOM setting that will take effect after reboot.</p> <p><b>Command mode:</b> All</p>

---

## Configuring the Number of Spanning Tree Groups

The maximum number of Spanning Tree Groups (STGs) available on the switch can be configured to be either 128 or 256.

**Table 395.** *Configuring the Maximum Number of STGs Command Options*

Command Syntax and Usage
<p><b>boot spanning-tree max-instances {128 256}</b></p> <p>Configures the maximum number of Spanning Tree Groups (STGs) that can be used on the switch.</p> <p>The default value is 128.</p> <p><b>Note:</b> The switch needs to be reloaded for the configuration to take effect.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>no boot spanning-tree max-instances</b></p> <p>Reset the maximum number of STGs available on the switch to the default value of 128.</p> <p><b>Note:</b> The switch needs to be reloaded for the configuration to take effect.</p> <p><b>Command mode:</b> Global configuration</p>
<p><b>show boot spanning-tree</b></p> <p>Displays the maximum number of currently available STGs on the switch and the maximum number of available STGs after the switch reloads.</p> <p><b>Command mode:</b> All</p>

The following command displays the current maximum limit of STGs on the switch and the maximum limit configured after the switch reloads:

**show boot spanning-tree**

**Command mode:** All

```
Bootup Max PVRST Instances: 128
Saved Max PVRST Instances: 256
```

**NOTE:** A Reboot is required for the new settings to take effect. When switching from 256 to 128 STP instances, please remove any extra configuration for STP instance 128 and above, then save the configuration; otherwise, all STP instance configuration may be lost after reload.



---

## Updating the Switch Software Image

The switch software image is the executable code running on the EN4093R 10Gb Ethernet Scalable Switch. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch.

Use the following command to determine the current software version: **show boot**

Upgrading the software image on your switch requires the following:

- Loading the new image onto a FTP, SFTP or TFTP server on your network
- Transferring the new image from the FTP, SFTP or TFTP server to your switch
- Selecting the new software image to be loaded into switch memory the next time the switch is reset

## Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

**Note:** EN4093R models do not support image releases prior to 7.5.

To load a new software image to your switch, you need the following:

- The image or boot software loaded on an FTP/SFTP/TFTP server on your network
- The hostname or IP address of the FTP/SFTP/TFTP server
- The name of the new software image or boot file

**Note:** The DNS parameters must be configured if specifying hostnames.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. In Privileged EXEC mode, enter the following command:

```
EN 4093# copy {ftp|tftp|sftp} {image1|image2|boot-image} [extm-port |  
mgt-port |data-port]
```

Select a port, or press <Enter> to use the default (management port).

2. Enter the hostname or IP address of the FTP, SFTP or TFTP server.

```
Address or name of remote host: <IP address or hostname>
```

3. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP, SFTP, or TFTP directory (usually `tftpboot`).

4. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

5. The system prompts you to confirm your request.

Next, select a software image to run, as described in the following section.

## Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
EN 4093(config)# boot image {image1|image2}
```

2. Enter the name of the image you want the switch to use upon the next boot.

The system informs you of which image set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

## Uploading a Software Image from Your Switch

You can upload a software image from the switch to a FTP, SFTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
EN 4093# copy {image1|image2|boot-image} {ftp|tftp|sftp}
[extm-port|mgt-port|data-port|staggered-upgrade]
```

Select a port, or press `<Enter>` to use the default (management port).

2. Enter the name or the IP address of the FTP, SFTP or TFTP server:

```
Address or name of remote host: <IP address or hostname>
```

3. Enter the name of the file into which the image will be uploaded on the FTP, SFTP or TFTP server:

```
Destination file name: <filename>
```

4. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

5. The system then requests confirmation of what you have entered. To have the file uploaded, enter **Y**.

```
image2 currently contains Software Version 6.5.0  
that was downloaded at 0:23:39 Thu Jan 1, 2010  
Upload will transfer image2 (2788535 bytes) to file "image1"  
on FTP/TFTP server 1.90.90.95.  
Confirm upload operation (y/n) ? y
```

---

## Selecting a Configuration Block

When you make configuration changes to the EN4093R 10Gb Ethernet Scalable Switch, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform a save operation (`copy running-config startup-config`), your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your EN4093R 10Gb Ethernet Scalable Switch was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured EN4093R 10Gb Ethernet Scalable Switch is moved to a network environment where it will be re-configured for a different purpose.

In Global Configuration mode, use the following command to set which configuration block you want the switch to load the next time it is reset:

```
EN 4093(config)# boot configuration-block {active|backup|factory}
```

---

## Rebooting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

**Note:** Resetting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

Enter the following command to reset (reload) the switch:

```
EN 4093# reload
```

You are prompted to confirm your request.

```
Reset will use software "image2" and the active config block.  
>> Note that this will RESTART the Spanning Tree,  
>> which will likely cause an interruption in network service.  
Confirm reload (y/n) ?
```

In stacking mode, the following options are available:

- Reload master switch
- Reload without saving tech-dump
- Staggered reload
- Reload switch unit

---

## Changing the Switch Profile

The Enterprise NOS software for the EN4093R can be configured to operate in different modes for different deployment scenarios. The deployment profile changes some of the basic switch behavior, shifting switch resources to optimize capacity levels to meet the needs of different types of networks. For more information about deployment profiles, see the Enterprise NOS 8.4 *Application Guide*.

To change the deployment profile, select the new profile and reset the EN4093R. Use the following command to select a new profile:

```
EN 4093(config)#boot profile {default|openflow}
```

The following list describes the boot profile options:

- `default` - deployment profile with balanced resources
- `openflow` - OpenFlow Only deployment profile

---

## Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software upgrade.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift + B>**. The Boot Management menu appears.

```
Resetting the System ...
Memory Test .....

Boot Management Menu
  I - Change booting image
  C - Change configuration block
  R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
  Q - Reboot
  E - Exit
Please choose your menu option:
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press I and follow the screen prompts.
- To change the configuration block, press C and follow the screen prompts.
- To boot in recovery mode, press R. For more details, see [“Boot Recovery Mode” on page 640](#).
- To restart the boot process from the beginning, press Q.
- To exit the Boot Management menu, press E. The booting process continues.

## Boot Recovery Mode

The Boot Recovery Mode allows you to recover from a failed software or boot image upgrade using TFTP or XModem download.

To enter Boot Recovery Mode you must select “Boot in recovery mode” option from the Boot Management Menu.

```
Entering Rescue Mode.
Please select one of the following options:
    T) Configure networking and tftp download an image
    X) Use xmodem 1K to serial download an image
    P) Physical presence (low security mode)
    R) Reboot
    E) Exit

Option? :
```

The Boot Recovery Mode menu allows you to perform the following actions:

- To recover from a failed software or boot image upgrade using TFTP, press T and follow the screen prompts. For more details, see [“Recover from a Failed Image Upgrade using TFTP” on page 641](#).
- To recover from a failed software or boot image upgrade using XModem download, press X and follow the screen prompts. For more details, see [“Recovering from a Failed Image Upgrade using XModem Download” on page 643](#).
- To enable the loading of an unofficial image, press P and follow the screen prompts. For more details, see [“Physical Presence” on page 645](#).
- To restart the boot process from the beginning, press R.
- To exit Boot Recovery Mode menu, press E. The boot process continues.



## Recover from a Failed Image Upgrade using TFTP

Use the following procedure to recover from a failed image upgrade using TFTP:

1. Connect a PC to the console port of the switch.
2. Open a terminal emulator program that supports Telnet protocol (for example, HyperTerminal, CRT, PuTTY) and input the proper hostname (IP address) and port to connect to the console port of the switch.
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting R. The Recovery Mode menu will appear.
5. To start the recovery process using TFTP, select T. The following message will appear:

```
Performing TFTP rescue. Please answer the following questions (enter 'q' to quit):
```

6. Enter the type of management port to be used:

```
Which mgmt port to be used? Internal/External:
```

7. Enter the IP address of the management port:

```
IP addr :
```

8. Enter the network mask of the management port:

```
Netmask :
```

9. Enter the gateway of the management port:

```
Gateway :
```

10. Enter the IP address of the TFTP server:

```
Server addr :
```

11. Enter the filename of the image:

```
Image Filename:
```

12. If the file is a software image, enter an image number:

```
Install image as image 1 or 2 (hit return to just boot image):
```

After the procedure is complete, the Recovery Mode menu will be re-displayed.

Below is an example of a successful recovery procedure using TFTP:

```
Entering Rescue Mode.
Please select one of the following options:
    T) Configure networking and tftp download an image
    X) Use xmodem 1K to serial download an image
    P) Physical presence (low security mode)
    R) Reboot
    E) Exit

Option? : t
Performing TFTP rescue. Please answer the following questions (enter 'q'
to quit):
Which mgmt port to be used? Internal/External: internal
IP addr :10.241.6.4
Netmask :255.255.255.128
Gateway :10.241.6.66
Server addr:10.72.97.135
Image Filename: EN4093R-8.2.1.0_OS.img
    Netmask : 255.255.255.128
    Gateway : 10.241.6.66
Configuring management port.....
Installing image EN4093R-8.2.1.0_OS.img from TFTP server 10.72.97.135

Extracting images ... Do *NOT* power cycle the switch.
Installing Application: Image signature verified. Install image as image
1 or 2 (hit return to just boot image): 2
Installing image as image2: 100%

Image2 updated succeeded
Updating install log. File EN4093R-8.2.1.0_OS.img installed from
10.72.97.135 at 15:29:30 on 12-3-2015
Please select one of the following options:
    T) Configure networking and tftp download an image
    X) Use xmodem 1K to serial download an image
    P) Physical presence (low security mode)
    R) Reboot
    E) Exit

Option? :
```

## Recovering from a Failed Image Upgrade using XModem Download

Use the following procedure to recover from a failed image upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
  - Speed: 9600 bps
  - Data Bits: 8
  - Stop Bits: 1
  - Parity: None
  - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting R. The Recovery Mode menu will appear.
5. Select X for Xmodem download. You will see the following display:

```
Running xmodem rescue.....
```

6. When you see the following message, change the Serial Port speed to 115200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before  
initiating the download.
```

7. Press **<Enter>** to set the system into download accept mode. When the readiness meter displays (a series of "C" characters), start Xmodem on your terminal emulator. You will see a display similar to the following:

```
... Waiting for the <Enter> key to be hit before the download can start...  
CC
```

8. Select the image to download. Xmodem initiates the file transfer. When download is complete, you are asked to change the Serial Port speed back to 9600 bps:

```
Change the baud rate back to 9600 bps, hit the <ENTER> key
```

9. Press **<Enter>** to start installing the image. If the file is a software image, enter the image number:

```
Install image as image 1 or 2 (hit return to just boot image):
```

The image install will begin. After the procedure is complete, the Recovery Mode menu will be re-displayed.

```
Extracting images ... Do *NOT* power cycle the switch.
Installing Root Filesystem:
Image signature verified. 100%
Installing Kernel:
Image signature verified. 100%
Installing Device Tree:
Image signature verified. 100%
Installing Boot Loader: 100%
Updating install log. File image installed from xmodem at 18:06:02 on
13-3-2015
Please select one of the following options:
    T) Configure networking and tftp download an image
    X) Use xmodem 1K to serial download an image
    P) Physical presence (low security mode)
    R) Reboot
    E) Exit

Option? :
```

Boot image recovery is complete.

## Physical Presence

Use the following procedure to enable the installation of unofficial images on the switch:

1. Connect a PC to the console port of the switch.
2. Open a terminal emulator program that supports Telnet protocol (for example, HyperTerminal, CRT, PuTTY) and input the proper hostname (IP address) and port to connect to the console port of the switch.
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting R. The Recovery Mode menu will appear.
5. To begin the Physical Presence procedure, select P. The following warning message will appear:

```
WARNING: the following test is used to determine physical presence and if
completed will put the switch in low security mode.
```

6. You will be prompted for confirmation:

```
Do you wish to continue y/n?
```

7. A security test will be performed. The system location (blue) LED will blink a number of times between 1 and 12. Enter that number:

```
Hit a key to start the test. The blue location LED will blink a number of
times.
.....
How many times did the LED blink?
```

8. After entering the correct number, the Recovery Mode menu will re-appear. To install an unofficial image use one of the following procedures:
  - TFTP (for details, see [page 641](#))
  - XModem Download (for details, see [page 643](#))

### Notes:

- You have three attempts to successfully complete the security test. After three incorrect attempts, the switch will reboot.
- After the test is completed, the switch will be put in low security mode. This mode will allow you to install unofficial images on the switch. To revert to normal security mode, you must reboot the switch or press P again in the Recovery Mode menu.



---

## Chapter 7. Maintenance Commands

The maintenance commands are used to manage dump information and forward database information. They also include debugging commands to help with troubleshooting.

Dump information contains internal switch state data that is written to flash memory on the EN4093R 10Gb Ethernet Scalable Switch after any one of the following occurs:

- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

To use the maintenance commands, you must be logged in to the switch as the administrator.

**Table 396.** *General Maintenance Commands*

Command Syntax and Usage
<b>copy flash-dump ftp [data-port extm-port mgt-port]</b> Saves the system dump information via FTP. For details, see <a href="#">page 665</a> . <b>Command mode:</b> All except User EXEC
<b>copy flash-dump sftp [data-port extm-port mgt-port]</b> Saves the system dump information via SFTP. For details, see <a href="#">page 665</a> . <b>Command mode:</b> All except User EXEC
<b>copy flash-dump tftp [address data-port extm-port filename mgt-port]</b> Saves the system dump information via TFTP. For details, see <a href="#">page 665</a> . <b>Command mode:</b> All except User EXEC
<b>clear flash-dump</b> Clears dump information from flash memory. <b>Command mode:</b> All except User EXEC
<b>copy log sftp [data-port extm-port mgt-port]</b> Saves the system log file (SYSLOG) via SFTP. <b>Command mode:</b> All except User EXEC
<b>copy log tftp [address data-port filename mgt-port]</b> Saves the system log file (SYSLOG) via TFTP. <b>Command mode:</b> All except User EXEC
<b>copy sa1 sftp [data-port extm-port mgt-port]</b> Saves the security audit log file via SFTP. <b>Note:</b> Not available in Stacking mode. <b>Command mode:</b> All except User EXEC

**Table 396.** *General Maintenance Commands*

<b>Command Syntax and Usage</b>
<b>copy sal tftp [address data-port filename mgt-port]</b> Saves the security audit log file via TFTP. <b>Note:</b> Not available in Stacking mode. <b>Command mode:</b> All except User EXEC
<b>clear sal</b> Clears the security audit log file. <b>Note:</b> Not available in Stacking mode. <b>Command mode:</b> All except User EXEC
<b>copy tech-support ftp [data-port extm-port mgt-port]</b> Redirects the technical support dump (tsdmp) to an external FTP server. <b>Command mode:</b> All except User EXEC
<b>copy tech-support sftp [data-port extm-port mgt-port]</b> Redirects the technical support dump (tsdump) to an external SFTP server. <b>Commands mode:</b> All except User EXEC
<b>copy tech-support tftp [address data-port extm-port filename mgt-port]</b> Redirects the technical support dump (tsdmp) to an external TFTP server. <b>Command mode:</b> All except User EXEC
<b>show tech-support [12 13 link port]</b> Dumps all EN4093R information, statistics, and configuration. <b>Note:</b> Some of the features displayed may not be supported on your switch. You can log the output (tsdmp) into a file. To filter the information, use the following options: <ul style="list-style-type: none"><li>o 12 displays only Layer 2-related information</li><li>o 13 displays only Layer 3-related information</li><li>o link displays only link status-related information</li><li>o port displays only port-related information</li></ul> <b>Command mode:</b> All except User EXEC



## Forwarding Database Maintenance

The Forwarding Database commands can be used to view information and to delete a MAC address from the forwarding database or to clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

**Table 397.** *FDB Manipulation Commands*

Command Syntax and Usage
<p><b>show mac-address-table address</b> &lt;MAC address&gt;</p> <p>Displays a single database entry by its MAC address. If not specified, you are prompted for the MAC address of the device. Enter the MAC address using one of the following formats:</p> <ul style="list-style-type: none"> <li>o xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56)</li> <li>o xxxxxxxxxxxxxx (such as 080020123456)</li> </ul> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table configured-static</b></p> <p>Displays configured static entries in the FDB.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table interface port</b> &lt;port number or alias&gt;</p> <p>Displays all FDB entries for a particular port.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table multicast</b></p> <p>Displays all Multicast MAC entries in the FDB.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table portchannel</b> &lt;LAG number&gt;</p> <p>Displays all FDB entries for a particular LAG.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table private-vlan</b> &lt;VLAN number&gt;</p> <p>Displays all FDB entries on a single private VLAN.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table state {forward trunk unknown}</b></p> <p>Displays all FDB entries of a particular state.</p> <p><b>Command mode:</b> All</p>
<p><b>show mac-address-table static</b></p> <p>Displays static entries in the FDB.</p> <p><b>Command mode:</b> All</p>

**Table 397.** FDB Manipulation Commands (continued)

Command Syntax and Usage
<b>show mac-address-table vlan</b> <VLAN number> Displays all FDB entries on a single VLAN. <b>Command mode:</b> All
<b>no mac-address-table</b> <MAC address> <VLAN number> Removes the specified FDB entry from the selected VLAN. <b>Command mode:</b> Global configuration
<b>no mac-address-table multicast</b> {<MAC address> all} Removes static multicast FDB entries. <b>Command mode:</b> Global configuration
<b>no mac-address-table static</b> {<MAC address> all} Removes static FDB entries. <b>Command mode:</b> Global configuration
<b>clear mac-address-table</b> Clears the entire Forwarding Database from switch memory. <b>Command mode:</b> All except User EXEC

---

## Debugging Commands

The Miscellaneous Debug Commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug commands:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

**Note:** Lenovo Enterprise Network Operating System debug commands are intended for advanced users. Use debug commands with caution as they can disrupt the operation of the switch under high load conditions. When debug is running under high load conditions, the CLI prompt may appear unresponsive. Before debugging, check the MP utilization to verify there is sufficient processing capacity available to perform the debug operation.

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

**Table 398.** *Miscellaneous Debug Commands*

Command Syntax and Usage
<b>debug debug-flags</b> This command sets the flags that are used for debugging purposes. <b>Command mode:</b> All except User EXEC
<b>debug dumpbt</b> Displays the backtrace log. <b>Command mode:</b> All except User EXEC
<b>debug mp-snap</b> Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred. <b>Command mode:</b> All except User EXEC
<b>debug mp-trace</b> Displays the Management Processor trace buffer. Header information similar to the following is shown: MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748 The buffer information is displayed after the header. <b>Command mode:</b> All except User EXEC

**Table 398.** *Miscellaneous Debug Commands*

Command Syntax and Usage
<p><b>[no] debug lacp packet {receive transmit both}</b> <b>port</b> <i>&lt;port alias or numbers&gt;</i></p> <p>Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on specific ports running LACP.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none"><li>o receive filters only LACP packets received</li><li>o transmit filters only LACP packets sent</li><li>o both filters LACP packets either sent or received</li></ul> <p>By default, LACP debugging is disabled.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>[no] debug spanning-tree bpdu [receive transmit]</b></p> <p>Enables/disables debugging for Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames sent or received.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none"><li>o receive filters only BPDU frames received</li><li>o transmit filters only BPDU frames sent</li></ul> <p>By default, STP BPDU debugging is disabled.</p> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>[no] debug spanning-tree tc</b></p> <p>Enables or disables the display of messages relating to STP topology changes.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<p><b>[no] debug ssh client {all state}</b></p> <p>Enables or disables SSH client based debug messages.</p> <ul style="list-style-type: none"><li>o all: Enables or disables all SSH client debug messages</li><li>o state: Enables or disables SSH client state debug messages</li></ul> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>[no] debug ssh server {all disconnect msg packet state}</b></p> <p>Enables or disables SSH server based debug messages.</p> <ul style="list-style-type: none"><li>o all: Enables or disables all SSH server debug messages.</li><li>o disconnect: Enables or disables SSH server disconnect debug messages</li><li>o msg: Enables or disables SSH server type and protocol debug messages</li><li>o packet: Enables or disables SSH server type, protocol and packet debug messages</li><li>o state: Enables or disables SSH server state debug messages</li></ul> <p><b>Command mode:</b> All except User EXEC</p>
<p><b>[no] debug tacacs-client</b></p> <p>Enables or disables TACACS+ client based debug messages.</p> <p><b>Command mode:</b> All except User EXEC</p>

**Table 398.** *Miscellaneous Debug Commands*

<b>Command Syntax and Usage</b>
<b>clear flash-config</b> Deletes all flash configuration blocks. <b>Command mode:</b> All except User EXEC

## IP Security Debugging

The following table describes the options available.

**Table 399.** *IP Security Debug Options*

<b>Command Syntax and Usage</b>
<b>[no] debug sec all</b> Enables or disables all IP security debug messages. <b>Command mode:</b> All except User EXEC
<b>[no] debug sec crypto</b> Enables or disables all IP security cryptographic debug messages. <b>Command mode:</b> All except User EXEC
<b>[no] debug sec ike</b> Enables or disables all IP security IKEv2 debug messages. <b>Command mode:</b> All except User EXEC
<b>[no] debug sec info</b> Displays the current security debug settings. <b>Command mode:</b> All except User EXEC
<b>[no] debug sec ipsec</b> Enables or disables all IPsec debug messages. <b>Command mode:</b> All except User EXEC

---

## vLAG Debugging

The following table describes vLAG debugging commands.

**Table 400.** *vLAG Debugging Options*

Command Syntax and Usage
<b>[no] debug vlag cfg</b> Enable or disables vLAG configuration debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag fdb-database</b> Enable or disables vLAG Forwarding Database debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag ht1hchk</b> Enable or disables vLAG Health Check debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag isl</b> Enable or disables vLAG ISL debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag msg</b> Enable or disables vLAG debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag portmgr</b> Enable or disables vLAG Port Manager debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag sm</b> Enable or disables vLAG State Machine debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag trunk</b> Enable or disables vLAG aggregation debug messages. <b>Command mode:</b> Privileged EXEC
<b>[no] debug vlag vrrp</b> Enable or disables vLAG VRRP debug messages. <b>Command mode:</b> Privileged EXEC

---

## ARP Cache Maintenance

The following table displays ARP Cache maintenance commands.

**Table 401.** *Address Resolution Protocol Maintenance Commands*

Command Syntax and Usage
<b>show ip arp</b> Shows all ARP entries. <b>Command mode:</b> All except User EXEC
<b>show ip arp find</b> <IP address> Shows a single ARP entry by IP address. <b>Command mode:</b> All except User EXEC
<b>show ip arp interface port</b> <port number or alias> Shows ARP entries on selected ports. <b>Command mode:</b> All except User EXEC
<b>show ip arp reply</b> Shows the list of IP addresses which the switch will respond to for ARP requests. <b>Command mode:</b> All except User EXEC
<b>show ip arp vlan</b> <VLAN number> Shows ARP entries on a single VLAN. <b>Command mode:</b> All except User EXEC
<b>clear arp</b> Clears the entire ARP list from switch memory. <b>Command mode:</b> All except User EXEC

**Note:** To display all or a portion of ARP entries currently held in the switch, you can also refer to “ARP Information” on [page 97](#).



---

## IP Route Manipulation

The following table displays IP Route maintenance commands.

**Table 402.** *IP Route Manipulation Commands*

Command Syntax and Usage
<b>show ip route [all]</b> Shows all routes. <b>Command mode:</b> All
<b>show ip route address</b> <IP address> Shows a single route by destination IP address. <b>Command mode:</b> All
<b>show ip route gateway</b> <IP address> Shows routes to a default gateway. <b>Command mode:</b> All
<b>show ip route interface</b> <IP interface> Shows routes on a single interface. <b>Command mode:</b> All
<b>show ip route tag {address bgp broadcast fixed martian   multicast ospf rip static}</b> Shows routes of a single tag. For a description of IP routing tags, see <a href="#">Table 42 on page 95</a> . <b>Command mode:</b> All
<b>show ip route type {broadcast direct indirect local   martian multicast}</b> Shows routes of a single type. For a description of IP routing types, see <a href="#">Table 41 on page 95</a> . <b>Command mode:</b> All
<b>clear ip route</b> Clears the route table from switch memory. <b>Command mode:</b> All except User EXEC

**Note:** To display all routes, you can also refer to [“IP Routing Information” on page 94](#).

---

## LLDP Cache Manipulation

[Table 403](#) describes the LLDP cache manipulation commands.

**Table 403.** *LLDP Cache Manipulation commands*

Command Syntax and Usage
<b>show lldp [information]</b> Displays all LLDP information. <b>Command mode:</b> All
<b>show lldp port</b> <port alias or number> Displays Link Layer Discovery Protocol (LLDP) port information. <b>Command mode:</b> All
<b>show lldp receive</b> Displays information about the LLDP receive state machine. <b>Command mode:</b> All
<b>show lldp remote-device</b> [<1-256> detail] Displays information received from LLDP -capable devices. For more information, see <a href="#">page 69</a> . <b>Command mode:</b> All
<b>show lldp transmit</b> Displays information about the LLDP transmit state machine. <b>Command mode:</b> All
<b>clear lldp</b> Clears the LLDP cache. <b>Command mode:</b> All except User EXEC

---

## IGMP Group Maintenance

Table 404 describes the IGMP group maintenance commands.

**Table 404.** *IGMP Multicast Group Maintenance Commands*

Command Syntax and Usage
<b>show ip igmp groups</b> Displays information for all multicast groups. <b>Command mode:</b> All
<b>show ip igmp groups address &lt;IP address&gt;</b> Displays a single IGMP multicast group by its IP address. <b>Command mode:</b> All
<b>show ip igmp groups detail &lt;IP address&gt;</b> Displays detailed information about a single IGMP multicast group. <b>Command mode:</b> All
<b>show ip igmp groups interface port &lt;port number or alias&gt;</b> Displays all IGMP multicast groups on selected ports. <b>Command mode:</b> All
<b>show ip igmp groups portchannel &lt;LAG number&gt;</b> Displays all IGMP multicast groups on a single LAG. <b>Command mode:</b> All
<b>show ip igmp groups vlan &lt;VLAN number&gt;</b> Displays all IGMP multicast groups on a single VLAN. <b>Command mode:</b> All
<b>clear ip igmp groups</b> Clears the IGMP group table. <b>Command mode:</b> All except User EXEC

## IGMP Multicast Routers Maintenance

The following table describes the maintenance commands for IGMP multicast routers (Mrouters).

**Table 405.** IGMP Multicast Router Maintenance Commands

Command Syntax and Usage
<p><b>show ip igmp mrouter</b></p> <p>Displays information for all Mrouters.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp mrouter dynamic</b></p> <p>Displays all dynamic multicast router ports installed.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp mrouter information</b></p> <p>Displays IGMP snooping information for all Mrouters.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp mrouter interface port</b> <i>&lt;port alias or number&gt;</i></p> <p>Displays all multicast router ports installed on a specific port.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp mrouter portchannel</b> <i>&lt;LAG number&gt;</i></p> <p>Displays all multicast router ports installed on a specific portchannel group.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp mrouter static</b></p> <p>Displays all static multicast router ports installed.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp mrouter vlan</b> <i>&lt;VLAN number&gt;</i></p> <p>Displays IGMP Mrouter information for a single VLAN.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp relay</b></p> <p>Displays IGMP relay information.</p> <p><b>Command mode:</b> All</p>
<p><b>show ip igmp snoop [igmpv3]</b></p> <p>Displays IGMP snooping information. The <i>igmpv3</i> option displays IGMPv3 snooping information.</p> <p><b>Command mode:</b> All</p>
<p><b>clear ip igmp mrouter</b></p> <p>Clears the IGMP Mrouter port table.</p> <p><b>Command mode:</b> All except User EXEC</p>

## MLD Multicast Group Manipulation

Table 406 describes the Multicast Listener Discovery (MLD) manipulation options.

**Table 406.** *MLD Maintenance*

Command Syntax and Usage
<b>show ipv6 mld groups</b> Shows all MLD groups. <b>Command mode:</b> All
<b>show ipv6 mld interface</b> <interface number> Shows MLD groups on the specified interface. <b>Command mode:</b> All
<b>clear ipv6 mld dynamic</b> Clears all dynamic MLD group tables. <b>Command mode:</b> All except User EXEC
<b>clear ipv6 mld groups</b> Clears all dynamic MLD registered group tables. <b>Command mode:</b> All except User EXEC
<b>clear ipv6 mld mrouter</b> Clears all dynamic MLD multicast router group tables. <b>Command mode:</b> All except User EXEC

---

## IPv6 Neighbor Discovery Cache Manipulation

Table 407 describes the IPv6 Neighbor Discovery cache manipulation commands.

**Table 407.** *IPv6 Neighbor Discovery cache manipulation commands*

Command Syntax and Usage
<b>show ipv6 neighbors</b> Shows all IPv6 Neighbor Discovery cache entries. <b>Command mode:</b> All
<b>show ipv6 neighbors counters</b> Displays IPv6 Neighbor Cache statistics. <b>Command mode:</b> All
<b>show ipv6 neighbors find</b> <IPv6 address> Shows a single IPv6 Neighbor Discovery cache entry by IP address. <b>Command mode:</b> All
<b>show ipv6 neighbors interface port</b> <port number or alias> Shows IPv6 Neighbor Discovery cache entries on a single port. <b>Command mode:</b> All
<b>show ipv6 neighbors static</b> Shows static IPv6 Neighbor Discovery cache entries. <b>Command mode:</b> All
<b>show ipv6 neighbors vlan</b> <VLAN number> Shows IPv6 Neighbor Discovery cache entries on a single VLAN. <b>Command mode:</b> All
<b>clear ipv6 neighbors</b> Clears all IPv6 Neighbor Discovery cache entries from switch memory. <b>Command mode:</b> All except User EXEC
<b>clear ipv6 neighbors counters</b> Clears all IPv6 Neighbor Cache statistics from switch memory. <b>Command mode:</b> All except User EXEC

---

## IPv6 Route Maintenance

Table 408 describes the IPv6 route maintenance commands.

**Table 408.** *IPv6 Route Maintenance Options*

Command Syntax and Usage
<b>show ipv6 route</b> Shows all IPv6 routes. <b>Command mode:</b> All
<b>show ipv6 route address</b> <IPv6 address> Show a single route by destination IP address. <b>Command mode:</b> All
<b>show ipv6 route gateway</b> <IPv6 gateway number> Show routes to a single gateway. <b>Command mode:</b> All
<b>show ipv6 route interface</b> <interface number> Show routes on a single IP interface. <b>Command mode:</b> All
<b>show ipv6 route static</b> Show static IPv6 routes. <b>Command mode:</b> All
<b>show ipv6 route summary</b> Shows a summary of IPv6 route information. <b>Command mode:</b> All
<b>show ipv6 route type</b> {connected static ospf} Show routes of a single type. <b>Command mode:</b> All
<b>clear ipv6 route</b> Clears all IPv6 routes. <b>Command mode:</b> All except User EXEC

## Stacking Maintenance

The following table describes Stacking maintenance commands.

**Table 409.** *Stacking Maintenance Options*

Command Syntax and Usage
<p><b>show logging swn</b> <i>&lt;configured switch number (1-8)&gt;</i> [<b>messages</b>] [<b>severity</b> <i>&lt;0-7&gt;</i>] [<b>reverse</b>] [ <b>{include exclude section begin head</b> <i>&lt;1-2000&gt;</i> <b>last</b> <i>&lt;1-2000&gt;</i>}]</p> <p>Displays the current syslog settings for the specified configured switch, followed by the most recent 2000 syslog messages.</p> <ul style="list-style-type: none"> <li>o <b>messages</b> displays the most recent 2000 syslog messages only</li> <li>o <b>severity</b> displays syslog messages of the specified severity level</li> <li>o <b>reverse</b> displays syslog messages starting with the most recent message</li> <li>o <b> </b> displays syslog messages that match one of the following filters: <ul style="list-style-type: none"> <li>• <b>include</b> displays syslog messages that match the specified expression</li> <li>• <b>exclude</b> displays syslog messages that don't match the specified expression</li> <li>• <b>section</b> displays syslog messages that match the specified section</li> <li>• <b>begin</b> displays syslog messages beginning from the first message that matches the specified expression</li> <li>• <b>head</b> displays the oldest syslog messages for the specified value</li> <li>• <b>last</b> displays the most recent syslog messages for the specified value</li> </ul> </li> </ul> <p><b>Note:</b> This command is available only on the master switch.</p> <p><b>Command mode:</b> All</p>
<p><b>copy log swn</b> <i>&lt;configured switch number (1-8)&gt;</i> <b>sftp</b></p> <p>Saves the system log file from the specified configured switch via SFTP.</p> <p><b>Note:</b> This command is available only on the master switch.</p> <p><b>Command mode:</b> All</p>
<p><b>copy log swn</b> <i>&lt;configured switch number (1-8)&gt;</i> <b>tftp</b> [<b>address</b> <i>&lt;hostname or server IP address&gt;</i>] [<b>filename</b> <i>&lt;server-filename&gt;</i>] [<b>data-port</b>   <b>mgt-port</b>]</p> <p>Saves the system log file from the specified configured switch via TFTP.</p> <p><b>Note:</b> This command is available only on the master switch.</p> <p><b>Command mode:</b> All</p>
<p><b>clear logging</b> [<b>master backup</b>   <i>&lt;attached switch number (1-16)&gt;</i>] [<b>all</b>]</p> <p>Clears the system log file (SYSLOG) on the current switch. You can clear the syslog from the master switch, the backup switch or any attached switch. The <b>all</b> option will clear the system log files from all the switches in the stack.</p> <p><b>Note:</b> The optional command elements are available only on the master switch.</p> <p><b>Command mode:</b> Privileged EXEC</p>



---

## TFTP, SFTP or FTP System Dump Copy

Use these commands to put (save) the system dump to a TFTP or FTP server.

**Note:** If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified `copy flash-dump tftp` (or `ftp`) file must exist *prior* to executing the `copy flash-dump tftp` command (or `copy flash-dump ftp`), and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, enter:

```
EN 4093# copy flash-dump tftp [address|data-port|extm-port|filename|  
|mgt-port] <server filename>
```

You are prompted for the TFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via SFTP, enter:

```
EN 4093# copy flash-dump sftp [data-port|extm-port|mgt-port] <server filename>
```

You are prompted for the SFTP server IP address or hostname, your *username* and *password*, and the *filename* of the target dump file.

To save dump information via FTP, enter:

```
EN 4093# copy flash-dump ftp [data-port|extm-port|mgt-port] <server filename>
```

You are prompted for the FTP server IP address or hostname, your *username* and *password*, and the *filename* of the target dump file.

---

## Clearing Dump Information

To clear dump information from flash memory, enter:

```
EN 4093# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

---

## Appendix A. Enterprise NOS System Log Messages

The EN4093R 10Gb Ethernet Scalable Switch (EN4093R) uses the following syntax when outputting system log (syslog) messages:

*<Time stamp> <IP/Hostname> <Log Label> <Thread ID>: <Message>*

The following parameters are used:

- *<Timestamp>*

The time of the message event is displayed in the following format:

*<month (3 characters)> <day> <hour (1-24)>:<minute>:<second>*

For example: Aug 19 14:20:30

- *<IP/Hostname>*

The hostname is displayed when configured.

For example: 1.1.1.1

- *<Log Label>*

The following types of log messages are recorded: LOG\_CRIT, LOG\_WARNING, LOG\_ALERT, LOG\_ERR, LOG\_NOTICE and LOG\_INFO.

- *<Thread ID>*

This is the software thread that reports the log message.

For example: stg, ip, console, telnet, vrrp, system, web server, ssh, bgp

- *<Message>*: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the *<Thread ID>* and *<Message>* are shown. The messages are sorted by *<Log Label>*.

Where the *<Thread ID>* is listed as *mgmt*, one of the following may be shown: *console, telnet, web server, or ssh*.

## LOG\_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
BGP	session with <IP address> failed (bad event:<event>)
BGP	session with <IP address> failed <reason> Reasons: <ul style="list-style-type: none"> <li>● Connect Retry Expire</li> <li>● Holdtime Expire</li> <li>● Invalid</li> <li>● Keepalive Expire</li> <li>● Receive KEEPALIVE</li> <li>● Receive NOTIFICATION</li> <li>● Receive OPEN</li> <li>● Receive UPDATE</li> <li>● Start</li> <li>● Stop</li> <li>● Transport Conn Closed</li> <li>● Transport Conn Failed</li> <li>● Transport Conn Open</li> <li>● Transport Fatal Error</li> </ul>
HOTLINKS	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>
IP	cannot contact default gateway <IP address>
IP	Route table full
MGMT	Maximum number of login failures (<threshold>) has been exceeded.
oflow	Switch is configured to function in Normal Mode
oflow	WARNING! In Hybrid Mode with Openflow enabled, legacy switching features are not supported on Openflow ports. Features involving TCAM resources are not supported on all ports.
oflow	Switch is configured to function in Openflow Mode
oflow	WARNING! In Openflow Only Mode, legacy switching features are not supported on all ports.
oflow	Openflow Instance <x> disabled
oflow	Openflow Instance <x> deleted
oflow	Openflow Instance <x>: No Controller Available for Connection
oflow	Openflow Instance <x>: Failed to receive Hello Message from Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Connection stopped with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Version Negotiation Failed with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Connection established with Controller <y> A.B.C.D

Thread	LOG_ALERT Message (continued)
oflow	Openflow Instance <x>: port <z> administratively disabled by controller
oflow	Openflow Instance <x>: port <z> administratively enabled by controller
oflow	ACL table full. Could not add MPLS pop ACL entry for Openflow Flow Table
oflow	ACL table full. Could not add MPLS push ACL entry for Openflow Flow Table
oflow	Openflow Instance <x> Maximum permitted multicast FDB flows reached
oflow	Openflow Instance <x> Maximum permitted unicast FDB flows reached
oflow	Openflow Instance <x> Maximum permitted ACL flows reached
oflow	Openflow Instance <x> Maximum permitted MPLS PUSH flows reached
oflow	Openflow Instance <x> Maximum permitted MPLS POP flows reached
oflow	FDB table full. Could not add FDB entry to Openflow Flow Table
oflow	ACL table full. Could not add ACL entry for Openflow Flow Table
oflow	Openflow statistics cleared for all instances
oflow	Openflow instance <x> Openflow statistics cleared
oflow	Openflow instance <x> Memory not available. Could not modify flow entry in Openflow Flow Table
oflow	Openflow instance <x> Flow Limit reached. Could not perform Flow mod request
oflow	Openflow Instance <x>, change DPID from <0xAAAAA> to <0xBBBBB>
oflow	Memory not available. Could not add flow entry
oflow	Flow Limit reached. Could not add Flow entry to Flow Table
oflow	Openflow dynamic table cleared for all instances
oflow	Openflow dynamic table cleared for instance <x>
oflow	Openflow static table cleared for all instances
oflow	Openflow static table cleared for instance <x>
oflow	Openflow all tables cleared for all instances
oflow	Openflow all tables cleared for instance <x>

Thread	LOG_ALERT Message (continued)
OSPF	Interface IP <IP address>, Interface State {Down   Loopback   Waiting   P To P   DR   BackupDR   DR Other}; Interface down detached
OSPF	LS Database full: likely incorrect/missing routes or failed neighbors
OSPF	Neighbor Router ID <router ID>, Neighbor State {Down   Attempt   Init   2 Way   ExStart   Exchange   Loading   Full   Loopback   Waiting   P To P   DR   BackupDR   DR Other}
OSPF	OSPF Route table full: likely incorrect/missing routes
STP	CIST new root bridge
STP	CIST topology change detected
STP	own BPDU received from port <port>
STP	Port <port>, putting port into blocking state
STP	STG <STG>, new root bridge
STP	STG <STG>, topology change detected
SYSTEM	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>
VRRP	Received <x> virtual routers instead of <y>
VRRP	received errored advertisement from <IP address>
VRRP	received incorrect addresses from <IP address>
VRRP	received incorrect advertisement interval <interval> from <IP address>
VRRP	received incorrect VRRP authentication type from <IP address>
VRRP	received incorrect VRRP password from <IP address>
VRRP	VRRP : received incorrect IP addresses list from <IP address>

---

## LOG\_CRIT

Thread	LOG_CRIT Message
AUDIT	NTP: cannot contact NTP server %s
AUDIT	NTP: System clock not updated. Authentication failed
AUDIT	VRRP: received incorrect VRRP authentication from %s
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private   public key}
SYSTEM	System memory is at <n> percent

## LOG\_ERR

Thread	LOG_ERR Message
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN cannot be a private-VLAN.
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	TFTP {Copy cfgRcv} attempting to redirect a previously redirected output
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX APP advertise settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX APP willing settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PFC advertise settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PFC willing settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PG advertise settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PG willing settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX state settings.
MGMT	Apply is issued by another user. Try later
MGMT	Critical Error. Failed to add Interface <interface>
MGMT	Diff is issued by another user. Try later
MGMT	Dump is issued by another user. Try later
MGMT	Error: Apply not done
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory)
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.
MGMT	Save is issued by another user. Try later



Thread	LOG_ERR Message (continued)
NTP	unable to listen to NTP port
PFC	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different PFC settings.
PFC	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different PFC settings for priority <priority number>.
STP	Cannot set "{Hello Time   Max Age   Forward Delay   Aging}" (Switch is in MSTP mode)
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Not enough memory!

## LOG\_INFO

Thread	LOG_INFO Message
	System log cleared by user <username>.
	System log cleared via SNMP.
AUDIT	Audit log has been cleared by %s
AUDIT	Class of service for user %s is changed
AUDIT	HTTPS has been disabled
AUDIT	HTTPS has been enabled
AUDIT	IKEv2 has been changed on this switch. E.g. DH Group 12 change to DH Group 24
AUDIT	IPsec manual policy X has been applied to interface XX. Security mode:[ESP/AH] Integrity algorithm:[xx] Encryption algorithm:[xx] Protocol mode: [tunnel/transport]
AUDIT	IPsec manual policy X has been detached from interface XX
AUDIT	LDAP has been disabled
AUDIT	LDAP has been enabled
AUDIT	Password for %s changed by %s, notifying admin to save
AUDIT	RADIUS has been disabled
AUDIT	RADIUS has been enabled
AUDIT	SSH server has been disabled
AUDIT	SSH server has been enabled
AUDIT	Successful user login/logout
AUDIT	TACACS+ has been disabled
AUDIT	TACACS+ has been enabled
AUDIT	Test event initiated for snmpv3 account and path verify
AUDIT	User %s is created
HOTLINKS	"Error" is set to "{Active   Standby}"
HOTLINKS	"Learning" is set to "{Active   Standby}"
HOTLINKS	"None" is set to "{Active   Standby}"
HOTLINKS	"Side Max" is set to "{Active   Standby}"
HOTLINKS	has no "{Side Max   None   Learning   Error}" interface

Thread	LOG_INFO Message (continued)
MGMT	/* Config changes at <time> by <username> */ <config diff> /* Done */
MGMT	<username> ejected from BBI
MGMT	<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
MGMT	<username>(<user type>) login {on Console   from host <IP address>}
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	boot kernel downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via {Browser   BBI}
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Firmware download failed to {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}
MGMT	Firmware downloaded to {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <hostname>:<filename>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	image1   2 download completed. Now writing to flash.
MGMT	image1   2 downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	image1   2 downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()

Thread	LOG_INFO Message (continued)
MGMT	Invalid image being loaded for this switch type
MGMT	invalid image download completed. Now writing to flash.
MGMT	invalid image downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	invalid image downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	New config set
MGMT	new configuration applied [from BBI   EM   SCP   SNMP   Stacking Master]
MGMT	new configuration saved from {BBI   ISCLI   SNMP}
MGMT	scp <username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
MGMT	scp <username>(<user type>) login {on Console   from host <IP address>}
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	SP boot kernel downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Starting Firmware download for {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <hostname>:<filename>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.
MGMT	undefined downloaded {from host <hostname>   via browser}, filename too long to be displayed, software version <version>
MGMT	undefined downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	unsaved changes reverted [from BBI   from SNMP]
MGMT	Unsupported GBIC {accepted   refused}
MGMT	user {SNMP user   <username>} ejected from BBI
MGMT	Watchdog has been {enabled   disabled}
MGMT	Watchdog timeout interval is now <seconds> seconds)

Thread	LOG_INFO Message (continued)
MGMT	Wrong config file type
oflow	OpenFlow <OpenFlow ID>: Connection established with controller <1-4> <IP address>
oflow	Openflow Statistics Cleared
oflow	Openflow Flowtable Cleared
oflow	OpenFlow <OpenFlow ID>: Connection lost with controller <1-4> <IP address>
SSH	<username><user type> {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	<username><user type> login {on Console   from host <IP address>}
SSH	Error in setting the new config
SSH	New config set
SSH	scp <username><user type> {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	scp <username><user type> login {on Console   from host <IP address>}
SSH	server key autogen {starts   completes}
SSH	Wrong config file type
SYSTEM	booted version <version> from Flash image <image>, {active   backup   factory} config block

## LOG\_NOTICE

Thread	LOG_NOTICE Message
	ARP table is full.
	Current config successfully tftp'd <filename> from <hostname>
	Current config successfully tftp'd to <hostname>: <filename>
	Port <port> mode is changed to full duplex for 1000 Mbps operation.
AUDIT	DHCP: Offer was found invalid by ip configuration
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary   secondary server
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
HOTLINKS	"Error" is set to "Standby   Active"
HOTLINKS	"Learning" is set to "Standby   Active"
HOTLINKS	"None" is set to "Standby   Active"
HOTLINKS	"Side Max" is set to "Standby   Active"
HOTLINKS	has no "{Side Max   None   Learning   Error}" interface
MGMT	<username> automatically logged out from BBI because changing of authentication type
MGMT	<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {BBI   Console   Telnet/SSH}
MGMT	<username>(<user type>) login {on Console   from host <IP address>   from BBI}
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Password incorrect!
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed
MGMT	enable password changed
MGMT	Error in setting the new config
MGMT	Failed login attempt via {BBI   TELNET} from host <IP address>.

Thread	LOG_NOTICE Message (continued)
MGMT	Failed login attempt via the CONSOLE
MGMT	FLASH Dump cleared from BBI
MGMT	New config set
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper   operator} changed by {SNMP user   <username>}, notifying admin to save.
MGMT	QSFP: Port <port> changed to {10G 40G}, from {BBI SNMP CLI}.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact {primary   secondary} server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp <username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
MGMT	scp <username>(<user type>) login {on Console   from host <IP address>}
MGMT	second syslog host changed to {this host   <IP address>}
MGMT	selectable [boot] mode changed
MGMT	STP BPDU statistics cleared
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host   <IP address>}
MGMT	System clock set to <time>.
MGMT	System date set to <date>.
MGMT	Terminating BBI connection from host <IP address>
MGMT	User <username> deleted by {SNMP user   <username>}.
MGMT	User <username> is {deleted   disabled} and will be ejected by {SNMP user   <username>}
MGMT	User {oper   operator} is disabled and will be ejected by {SNMP user   <username>}.
MGMT	Wrong config file type
NTP	System clock updated

Thread	LOG_NOTICE Message (continued)
OSPF	Neighbor Router ID <router ID>, Neighbor State {Down   Loopback   Waiting   P To P   DR   BackupDR   DR Other   Attempt   Init   2 Way   ExStart   Exchange   Loading   Full}
SERVER	link {down   up} on port <port>
SSH	(remote disconnect msg)
SSH	<username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	<username>(<user type>) login {on Console   from host <IP address>}
SSH	Error in setting the new config
SSH	Failed login attempt via SSH
SSH	New config set
SSH	scp <username>(<user type>) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
SSH	scp <username>(<user type>) login {on Console   from host <IP address>}
SSH	Wrong config file type
SYSTEM	Change fiber GIG port <port> mode to full duplex
SYSTEM	Change fiber GIG port <port> speed to 1000
SYSTEM	Changed ARP entry for IP <IP address> to: MAC <MAC address>, Port <port>, VLAN <VLAN>
SYSTEM	Enable auto negotiation for copper GIG port: <port>
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Port <port> disabled
SYSTEM	Port <port> disabled due to reason code <reason code>



Thread	LOG_NOTICE Message (continued)
SYSTEM	rebooted (<reason>)[, administrator logged in] Reason: <ul style="list-style-type: none"> <li>● Boot watchdog reset</li> <li>● console PANIC command</li> <li>● console RESET KEY</li> <li>● hard reset by SNMP</li> <li>● hard reset by WEB-UI</li> <li>● hard reset from console</li> <li>● hard reset from Telnet</li> <li>● low memory</li> <li>● MM Cycled Power Domain</li> <li>● power cycle</li> <li>● Reset Button was pushed</li> <li>● reset by SNMP</li> <li>● reset by WEB-UI</li> <li>● reset from console</li> <li>● reset from EM</li> <li>● reset from Telnet/SSH</li> <li>● scheduled reboot</li> <li>● SMS-64 found an over-voltage</li> <li>● SMS-64 found an under-voltage</li> <li>● software ASSERT</li> <li>● software PANIC</li> <li>● software VERIFY</li> <li>● Telnet PANIC command</li> <li>● unknown reason</li> <li>● watchdog timer</li> </ul>
SYSTEM	Received BOOTP Offer: IP: <IP address>, Mask: <netmask>, Broadcast <IP address>, GW: <IP address>
SYSTEM	Watchdog threshold changed from <old value> to <new value> seconds
SYSTEM	Watchdog timer has been enabled
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VLAN	Default VLAN can not be deleted
VRRP	virtual router <IP address> is now {BACKUP   MASTER}
WEB	<username> ejected from BBI
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

## LOG\_WARNING

Thread	LOG_WARNING Message
AUDIT	BGP: authentication receive error from %s
AUDIT	BGP: change neighbor %d password
AUDIT	BGP: delete BGP neighbor %d password
AUDIT	BGP: Password authentication fail
AUDIT	BGP: peer ttl set to %s
AUDIT	BGP: ttl-security on peer %s ignored packet
AUDIT	DHCP: disable
AUDIT	DHCP: enable
AUDIT	DHCP: Enabling DHCP will overwrite IP interface %d and IP gateway %d's configurations.
AUDIT	DHCP: on External Management Interface disabled with I2C Control Register
AUDIT	DHCP: on External Management Interface enabled with I2C Control Register
AUDIT	DHCP: Use factory default while requesting for a new DHCP offer.
AUDIT	Failed login attempt via the %s
AUDIT	IP: ARP table is full.
AUDIT	IP: Changed ARP entry for IP %s to: \tMAC %02x:%02x:%02x:%02x:%02x:%02x
AUDIT	IP: gateway %s is down
AUDIT	IP: gateway %s is up
AUDIT	IP: New Management Gateway %s configured
AUDIT	IP: New Management IP Address %s configured
AUDIT	IP: Route table full
AUDIT	LDAP security does not meet security strict mode requirements
AUDIT	OSPF: area %s authentication type is %s
AUDIT	OSPF: delete OSPF authentication key
AUDIT	OSPF: received incorrect authentication
AUDIT	OSPF: Route table full
AUDIT	OSPF: set OSPF authentication key %d

Thread	LOG_WARNING Message (continued)
AUDIT	OSPF: use OSPF authentication key
AUDIT	OSPFv3: authentication enable
AUDIT	OSPFv3: authentication reset to default
AUDIT	OSPFv3: authentication spi %d auth %s
AUDIT	OSPFv3: disable OSPFv3 authentication spi %d
AUDIT	OSPFv3: disable OSPFv3 encryption spi %d
AUDIT	OSPFv3: encryption enable
AUDIT	OSPFv3: encryption reset to default
AUDIT	OSPFv3: encryption spi %d esp auth %s encrypt %s
AUDIT	RADIUS security does not meet security strict mode requirements
AUDIT	RIP: change authentication key
AUDIT	RIP: delete RIP authentication
AUDIT	RIP: received incorrect authentication
AUDIT	TACACS+ security does not meet security strict mode requirements
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <interface>.
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <interface>.
HOTLINKS	"Error" is set to "Standby   Active"
HOTLINKS	"Learning" is set to "Standby   Active"
HOTLINKS	"None" is set to "Standby   Active"
HOTLINKS	"Side Max" is set to "Standby   Active"
HOTLINKS	has no "{Side Max   None   Learning   Error}" interface
MGMT	The software demo license for Upgrade2 will expire in 10 days. The switch will automatically reset to the factory configuration after the license expires. Please backup your configuration or enter a valid license key so the configuration will not be lost.
NTP	cannot contact [primary   secondary] NTP server <IP address>
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked

Thread	LOG_WARNING Message (continued)
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled

---

## Appendix B. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

**Note:** This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the System x, Flex System, and NeXtScale System products.

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check the [Lenovo ServerProven website](#) to make sure that the hardware and software is supported by your product.
- Go to the [Lenovo Support portal](#) to check for information to help you solve the problem.
- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (Lenovo 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs

- Start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

---

## Appendix C. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.  
1009 Think Place - Building One  
Morrisville, NC 27560  
U.S.A.

Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties.

Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.



---

## Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and X-Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

---

## Important Notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as total bytes written (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

---

## Recycling Information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to:

<http://www.lenovo.com/recycling>

## Particulate Contamination

**Attention:** Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Contaminant	Limits
Particulate	<ul style="list-style-type: none"> <li>The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2<sup>1</sup>.</li> <li>Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282.</li> <li>The deliquescent relative humidity of the particulate contamination must be more than 60%<sup>2</sup>.</li> <li>The room must be free of conductive contamination such as zinc whiskers.</li> </ul>
Gaseous	<ul style="list-style-type: none"> <li>Copper: Class G1 as per ANSI/ISA 71.04-1985<sup>3</sup></li> <li>Silver: Corrosion rate of less than 300 Å in 30 days</li> </ul>

<sup>1</sup> ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

<sup>2</sup> The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

<sup>3</sup> ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

---

## Telecommunication Regulatory Statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

---

## Electronic Emission Notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

### Federal Communications Commission (FCC) Statement

**Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used to meet FCC emission limits. Lenovo is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

### Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

### Avis de Conformité à la Réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.


### Australia and New Zealand Class A Statement

**Attention:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## European Union - Compliance to the Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC (until April 19, 2016) and EU Council Directive 2014/30/EU (from April 20, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class A equipment according to European Standards harmonized in the Directives in compliance. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

 Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

**Warning:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## Germany Class A Statement

**Deutschsprachiger EU Hinweis:**

### **Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit**

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der Klasse A der Norm gemäß Richtlinie.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

**Deutschland:**

### **Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln**

Dieses Produkt entspricht dem „Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln“ EMVG (früher „Gesetz über die elektromagnetische Verträglichkeit von Geräten“). Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) in der Bundesrepublik Deutschland.

**Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EU Richtlinie 2014/30/EU (früher 2004/108/EC), für Geräte der Klasse A.**

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Meitnerstr. 9, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

Nach der EN 55022: „Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.“

Nach dem EMVG: „Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.“ (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

## Japan VCCI Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.



## Japan Electronics and Information Technology Industries Association (JEITA) Statement

高調波ガイドライン適合品

Japan Electronics and Information Technology Industries Association (JEITA)  
Confirmed Harmonics Guidelines (products less than or equal to 20 A per phase)

高調波ガイドライン準用品

Japan Electronics and Information Technology Industries Association (JEITA)  
Confirmed Harmonics Guidelines with Modifications (products greater than 20 A per phase).

## Korea Communications Commission (KCC) Statement

이 기기는 업무용(A급)으로 전자파적합기기로  
서 판매자 또는 사용자는 이 점을 주의하시기  
바라며, 가정외의 지역에서 사용하는 것을 목  
적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A).  
Sellers and users need to pay attention to it. This is for any areas other than home.

## Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.  
В жилых помещениях оно может создавать радиопомехи, для  
снижения которых необходимы дополнительные меры

## People's Republic of China Class A electronic emission Statement

中华人民共和国“A类”警告声明

声明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

## Taiwan Class A compliance Statement

警告使用者：  
這是甲類的資訊產品，在  
居住的環境中使用時，可  
能會造成射頻干擾，在這種  
情況下，使用者會被要求  
採取某些適當的對策。



---

# Index

## Numerics

- 802.1p
    - and ETS 558
    - configuration 384, 409
    - DCBX PFC information 194
    - information 139, 140, 141, 197
    - PFC configuration 560
    - Priority Group mapping 197
    - priority level 368, 391, 402
      - IPv6 396
    - priority value 411
  - 802.1X
    - configuration 416
    - guest VLAN 418
    - information 57, 75
    - operations-level commands 611
    - port configuration 419
- ## A
- abbreviating commands (CLI) 28
  - access control
    - switch 358
    - user 360
  - Access Control List (see ACL) 142
  - ACL
    - add group 377
    - and VMAP 402
    - configuration 390
    - Ethernet matching criteria 392
    - filtering criteria 391
    - groups 390
    - information 142, 143
    - IPv4 matching criteria 393
    - IPv6 396
    - list of FIPS ACLs 199, 200
    - management ACL filtering 400
    - metering configuration 408
    - Packet Format matching criteria 395
    - port ACL configuration 377
    - port configuration commands 377
    - QoS parameters 377
    - re-marking 409
    - re-marking (IPv6) 399, 411
    - remove group 377
    - statistics 307, 308
    - TCP matching criteria 394
    - UDP matching criteria 394
  - active
    - configuration block 321, 636
    - IP interface 542
    - switch configuration
      - ptcfg 606
      - restoring 607

- saving and loading 607
  - VLAN port 542
- addr (IP route tag) 95
- administrator account 29
- aging (STP information) 83
- asnum (attached switch number) 383
- assistance, getting 685
- Australia Class A statement 694
- autonomous system filter path
  - action 481
  - as 481
  - aspath 481

## B

- backup configuration block 636
- bandwidth allocation, Priority Groups 558
- BGP 95
  - aggregation configuration 511
  - configuration 508
  - eBGP 508
  - filters, aggregation configuration 511
  - iBGP 508
  - in route 510
  - IP address, border router 509
  - keep-alive time 511
  - operations-level commands 613
  - peer 509
  - peer configuration 509
  - redistribution configuration 513
  - remote autonomous system 510
  - router hops 510
- bgp (IP route tag) 95
- boot
  - options 623 to ??
- Boot Management menu 639
- BOOTP
  - configuration 534
  - relay broadcast domain configuration 534
- Bootstrap Protocol (see BOOTP) 534
- Border Gateway Protocol (see BGP) 23
- bridge priority 80, 84
- Bridge Protocol Data Unit (BPDU) 81, 84, 85, 429
- Bridge Spanning-Tree parameters 430
- broadcast (IP route tag) 96
- broadcast (IP route type) 95

## C

- Canada Class A electronic emission statement 694
- CEE
  - configuration 557
  - DCBX 656
  - information 189
- China Class A electronic emission statement 697

- Cisco Ether Channel 439
- CIST information 86
- Class A electronic emission notice 694
- clear
  - ACL statistics 307
  - all defined management networks 358
  - all IPv4 statistics 238, 242
  - all IPv6 statistics 239, 247
  - ARP statistics 238
  - DNS statistics 238
  - dump information 666
  - FCoE statistics 309
  - Hot Links statistics 228
  - ICMP statistics 238
  - IGMP statistics 238
  - LACP statistics 227
  - MLD statistics 260
  - OSPF statistics 238
  - RIP statistics 238
  - static route 471
  - statistics for specific ports 206, 228
  - statistics on a specific trunk group 226
  - TCP statistics 239
  - UDP statistics 239
  - VRRP statistics 239
- commands
  - abbreviations 28
  - conventions used in this manual 18
  - help with 26
  - shortcuts 28
  - tab completion 28
- configuration
  - 802.1X 416
  - commands 319 to 607
  - default gateway interval, for health checks 469
  - default gateway IP address 469
  - dump command 605
  - failover 450
  - flow control 374, 380
  - IGMP 516
  - IP static route 471
  - port link speed 374
  - port mirroring 413
  - port trunking 439
  - RIP 482
  - RIP commands 482
  - save changes 321
  - SNMP 344
  - switch IP address 465
  - TACACS+ 335
  - VLAN default (PVID) 371
  - VLAN IP interface 466
  - VLAN tagging 370
  - VMware 576
  - VRRP 535

- configuration block
  - active 636
  - backup 636
  - factory 636
  - selection 636
- contamination, particulate and gaseous 692
- Control Plane Protection, configuration 386
- Converged Enhanced Ethernet (see CEE) 189
- COPP, configuration 386
- COS queue information 140
- cost
  - STP information 83
- cost (STP information) 80, 86
- CPU use
  - history 306
  - statistics 304, 306

## D

- daylight saving time 323
- DCB Capability Exchange Protocol (see DCBX) 190
- DCBX
  - Application Protocol information 195
  - configuration 562
  - control information 191
  - debugging 656
  - ETS information 193
  - feature information 192
  - information 190
  - PFC information 194
- debugging 647
- default gateway
  - information 92
  - interval, for health checks 469
  - IPv6 549
- default password 29
- delete
  - ACL statistics 307
  - all defined management networks 358
  - all IPv4 statistics 238, 242
  - all IPv6 statistics 239, 247
  - ARP statistics 238
  - DNS statistics 238
  - dump information 666
  - Hot Links statistics 228
  - ICMP statistics 238
  - IGMP statistics 238
  - LACP statistics 227
  - MLD statistics 260
  - OSPF statistics 238
  - RIP statistics 238
  - static route 471
  - statistics for specific ports 206, 228
  - statistics on a specific trunk group 226
  - TCP statistics 239
  - UDP statistics 239
  - VRRP statistics 239

- DHCP
  - and BOOTP commands 534
  - and managed address configuration flag 467
  - and Netboot configuration 628
  - and other stateful configuration flag 467
  - packets logged 299
  - Snooping 556
- DiffServ Code Point (see DSCP) 385
- direct (IP route type) 95
- directed broadcasts 476
- disconnect idle timeout 30
- downloading software 633
- DSCP
  - configuration 385
  - disable for in-profile traffic 410
  - re-mark for in-profile traffic 412
  - re-mark for out-profile traffic 412
  - re-marking configuration 368, 385
  - set value of in-profile packets 410
  - set value of out-profile packets 410
- dump
  - configuration command 605
  - maintenance 647
- duplex mode
  - interface status 31
  - link status 158
- Dynamic Host Configuration Protocol (see DHCP) 534
- dynamic routes 657

## E

- ECMP route information 116
- ECN (Explicit Congestion Notification) 388
- Edge Virtual Bridging, configuration 584
- electronic emission Class A notice 694
- Enhanced Transmission Selection (see ETS) 197
- ENode 564
- Error Disable and Recovery
  - port 373
  - system 326
- EtherChannel, and port trunking 439
- ETS
  - configuration 558
  - information 190, 193, 197
  - Priority Group configuration 558
- European Union EMC Directive conformance statement 695
- EVB
  - configuration 584
  - configuration mode 25
  - information 173
- Explicit Congestion Notification (ECN) 388

## F

- factory configuration block 636

- failover
  - auto monitor configuration 451
  - configuration 450
  - Layer 2 configuration 450
  - Layer 2 information 58, 64
  - manual monitor port configuration 452
  - trigger configuration 451
  - uplink, for vNIC group 578
- FCC Class A notice 694
- FCC, Class A 694
- FCF port 564
- FCoE
  - configuration 563
  - FIPS port configuration 564
  - forwarding 564
  - information 199
  - Initialization Protocol (see FIP) 564
  - statistics 309
- FDB
  - configuration 431
  - configuring static entries 434
  - hot links update 454
  - information 60
  - learning 369
  - maintenance 647, 649
  - troubleshooting 647, 649
- Fiber Channel Initialization Protocol (see FIP) 199
- Fibre Channel over Ethernet (see FCoE) 199
- FIP
  - Snooping (see FIPS) 564
  - snooping information 199
- FIPS
  - list of ACLs 199
  - port configuration 564
- fixed (IP route tag) 95
- flag field 98
- flow control
  - configuring 374, 380
  - configuring for port link 374
  - information 31, 158
  - Ingress Back Pressure 217
  - pause packets 215, 216
  - priority (see PFC) 194
- Forwarding Database (see FDB) 60
- forwarding state
  - (FWD) 80, 84, 85
- forwarding state (FWD) 61, 88
- FWD (port state) 61
- fwd (STP bridge option) 429
- FwdDel (forward delay), bridge port 80, 83, 84, 85

## G

- gaseous contamination 692
- Germany Class A statement 695
- getting help 685
- gtcfcg (TFTP load command) 607

## H

- health checks
  - default gateway interval, retries 469
  - retry, number of failed health checks 469
- hello (STP information) 81, 83, 84, 85
- help
  - online 26
  - sources of 685
- help, getting 685
- Hot Links configuration 454
- hot-standby failover 540
- http
  - controlling access 356
  - port 356
- HTTPS 363

## I

- ICMP statistics 253
- idle timeout, setting 30
- IEEE standards
  - 802.1p 384
  - 802.1X 75
- IGMP
  - advanced parameters 523
  - configuration 516
  - filter definition commands 520
  - filtering configuration 519
  - filtering port configuration 520
  - group information 120
  - group maintenance 659
  - mrouter maintenance commands 660
  - multicast group information 117
    - multicast
      - group information 117
  - multicast router information 121
  - relay configuration 519
  - relay mrouter configuration 521
  - snooping configuration 517
  - static mrouter configuration 522
  - statistics 258
- IGMPv3
  - configuration 518
  - information 120
  - snooping information 660
  - statistics 258
- IKEv2
  - configuration 526
  - configuration mode 24
  - debugging 654
  - identification configuration 527
  - information 91, 130
  - information commands 129
  - preshare key configuration 527
  - proposal configuration 526
- image
  - downloading 633
  - software, selecting 634
- indirect (IP route type) 95
- information
  - VMware 169
- Information Commands 31 to 201
- Interface change stats 271
- IP address
  - ARP information 97
  - configuring default gateway 469
- IP forwarding
  - configuration 476
  - directed broadcasts 476
  - information 92
- IP Information 92, 128
- IP interfaces 95
  - active 542
  - configuring address 465
  - configuring VLANs 466
  - information 92
  - IP route tag 95
  - priority increment value (ifs) for VRRP 544
- IP network filter configuration 477
- IP route
  - manipulation 657
  - tag parameters 95
- IP Static Route commands 471
- IP statistics 240
- IPMC group information 121
- IPsec
  - configuration 528
  - debugging 654
  - dynamic policy configuration 529
  - information 131
  - Layer 3 configuration 502, 505
  - manual policy configuration 530
  - manual policy information 132
  - traffic selector configuration 529
  - transform set configuration 528
- IPv6
  - ACL configuration 396
  - default gateway configuration 549
  - interface information 126
  - Neighbor Discovery
    - cache configuration 551
    - cache information 114
    - cache information commands 114
    - cache manipulation 662
    - configuration commands 467
    - prefix configuration 551
    - prefix information 115
  - Path MTU
    - configuration 554
    - information 127
  - re-mark configuration 399
  - re-marking
    - configuration 411
    - in-profile configuration 412

- out-of-profile configuration 412
- routing information 112, 113
- static route 550
- statistics 243
- IPv6 route 249
- ISCLI command modes 22
- ISCLI commands
  - basics 21 to ??

## J

- Japan Class A electronic emission statement 696
- Japan Electronics and Information Technology Industries Association statement 697
- JEITA statement 697

## K

- Korea Class A electronic emission statement 697

## L

- LACP
  - add trunk to vNIC Group 579
  - admin key
    - add to Auto Monitor 451
    - add to Backup interface 457
    - add to Manual Monitor Control 453
    - add to Manual Monitor Port 452
    - add to Master interface 456
    - add to VM group 571
  - aggregator information 63
  - and trunk hash configuration 440
  - configuration 447
  - information 63
  - port configuration 448
  - port status information 63
  - remove trunk from vNIC group 579
  - statistics 227, 229
  - virtual (see vLAG) 444
- Layer 2 commands 57
- Layer 3 commands 91
- LDAP server configuration 339
- Lightweight Directory Access Protocol (see LDAP) 339
- Link Layer Discovery Protocol (see LLDP) 68
- link speed, configuring 374
- link status 31
  - command 158
  - duplex mode 31, 158
  - information 158
  - port speed 31, 158
- linkt (SNMP option) 345

- LLDP
  - cache manipulation commands 658
  - disable 435
  - enable 435
  - information 68
  - packets received 295
  - PDU logged 300
  - remote device information 69
  - statistics 227, 231
  - TLV configuration 437
- local (IP route type) 95
- log, syslog messaging options 329
- LRN (port state) 80, 84, 85

## M

- MAC address
  - ARP information 97
  - display 33
  - FDB information 60
  - FDB maintenance 649
  - multicast, configuring 433
  - switch management processor 46
- MAC address spoof prevention 574
- Maintenance commands 647
- Management Processor (see MP) 33
- manual style conventions 18
- martian
  - IP route tag (filtered) 96
  - IP route type (filtered out) 95
- MaxAge (STP information) 80, 83, 84, 85
- MD5
  - cryptographic authentication 486
  - key 489
  - key configuration, OSPF 493
- meter
  - ACL
    - configuring 408
    - current parameters 408
    - delete 408
    - port metering 404
    - configuring vNIC bandwidth 578
- Miscellaneous Debug commands 651
- MLD
  - configuration 514
  - configuration mode 24
  - global statistics 261
  - information 93, 122
  - mrouter information 123
  - statistics 260
- monitor port 413
- MP
  - display MAC address 33, 46
  - packet statistics 292
  - snap trace buffer 651
  - statistics 291
  - trace buffer 651
- Mrouter information 121

- MST
  - configuration mode 24
- MTU 554
- multicast
  - IP route type 95
  - router information 121
  - static MAC configuration 433
- Multicast Listener Discovery protocol (see MLD) 24
- multiple management VLANs 458
- mxage (STP bridge option) 429

## N

- nbr change statistics 270
- Neighbor Discovery
  - cache configuration, IPv6 551
  - cache manipulation, IPv6 662
  - IPv6, configuration 467
  - prefix 551
- Neighbor Discovery prefix 551
- Network Configuration Protocol (NETCONF) 359
- New Zealand Class A statement 694
- notes, important 690
- notice 324
- notices 687
- NTP synchronization 341

## O

- OAM
  - information 71
  - statistics 206, 227, 233
- online help 26
- OpenFlow
  - configuration 587
  - configuration mode 24
  - information 144
    - flow allocation 147
    - flow configuration 150
    - flow tables 152
    - global configuration 145
  - static flows 597
    - actions 599
    - qualifiers 597
  - statistics 275
- Operations commands 609
- operations-level
  - 802.1X port commands 611
  - BGP commands 613
  - port commands 610
  - VRRP options 612
- OSPF
  - area index 486
  - authentication key 489
  - configuration 485
    - host entry 492
    - interface 489
    - MD5 key 493

- route redistribution 493
  - summary range 488
  - virtual link 491
- cost of the selected path 489
- cost value of the host 492
- dead
  - declaring a silent router to be down 489
  - health parameter of a hello packet 491
- export 493
- fixed routes 508
- general information 103
- hello, authentication parameter of a hello packet 491
- host routes 485
- information
  - commands 102
  - database 105
  - general 103
  - interface 104
  - interface loopback 104
  - route 104
- interface 485
- link state database 486, 494
- Not-So-Stubby Area 487, 497
- priority value of the switch interface 490
- range number 485
- SPF, shortest path first 486
- statistics
  - commands 263
  - delete 238
  - global 264
- stub area 487, 497
- transit area 487, 497
- transit delay 490
- type 487
- virtual link 485
- virtual neighbor, router ID 491
- ospf (IP route tag) 95
- OSPFv3
  - configuration 494
    - area index 496
    - interface 500
    - virtual link 504
- dead
  - declaring a silent router to be down 500
  - health parameter of a hello packet 504
- hello, authentication parameter of a hello packet 504
- information
  - commands 107
  - database 110
  - dump of 108
  - interface 109
  - route 109
- statistics
  - commands 268
  - global 269
- type 497
- virtual neighbor, router ID 504



## P

- parameters
  - tag 95
  - type 95
- particulate contamination 692
- passwords 29
  - administrator account 29
  - changing 360
  - default 29
  - user account 29
- Path MTU 554
- path-cost (STP port option) 431
- People's Republic of China Class A electronic emission statement 697
- PFC configuration 560
- PIM mode 546
- ping 26
- poisoned reverse, as used with split horizon 483
- port
  - ACL configuration 377
  - configuration 368
  - disabling temporarily 374
  - Error Disable and Recovery 373
  - failover manual monitor configuration 452
  - FIPS configuration 564
  - HTTP 356
  - IGMP filtering configuration 520
  - information 160
  - LACP
    - configuration 448
    - status information 63
  - link configuration 374
  - link speed, configuring 374
  - management, configuring 380
  - membership of the VLAN 58, 90
  - mirroring, configuring 413
  - number 158
  - priority 80, 86
  - reference 61
  - speed 31, 158
  - state information 61
  - telnet 356
  - TFTP 356
  - trunking
    - configuration 439
    - description 439
  - VLAN ID 31, 160
- port ECN configuration 378
- port WRED configuration 378
- preemption
  - assuming VRRP master routing authority 539
  - hot links trigger, configuring 455
  - virtual router, configuring 537
  - VRRP, configuring 540
- Priority Flow Control 560

- Priority Groups
  - 802.1p mapping to 197
  - configuration 558
  - information 193
- Private VLAN 462
- Protected Mode 614
- Protocol-based VLAN (see PVLAN) 460
- ptcfg (TFTP save command) 606
- PTP
  - configuration 602
  - statistics 316
- PVID (port VLAN ID) 31, 160
- PVLAN
  - configuration 459, 460
  - current parameters 461

## Q

- QoS
  - ACL parameters 377
  - configuration 377, 384
  - control plane protection 386
  - DSCP configuration 385
  - ECN information 141
  - information 139
  - transmit-queue information 140
  - WRED information 141

## R

- RADIUS server
  - 802.1X response timeout, setting 417
  - and 802.1X configuration 416
  - configuration commands 333
  - current parameters 334
  - packets logged 301
  - primary 333
  - shared secret 333
- receive flow control 374, 380
- reference ports 61
- re-mark
  - ACL
    - configuration 405, 409
    - parameters 143
  - DSCP
    - configuration 368
    - global configuration 385
  - in-profile
    - configuration 410
    - settings 405
  - IPv6 ACL 399
    - configuration 411
    - in-profile configuration 412
    - out-of-profile configuration 412
    - parameters 412
  - out-of-profile
    - configuration 410

- settings 405
  - TOS precedence, configuring 405
  - user update priority 405
- Remote Monitoring (RMON) 565
- Rendezvous Point (RP) 546
- retries
  - health checks for default gateway 469
  - radius server 333
- RIP
  - configuration 482
    - BGP redistribution 513
    - route redistribution 484
  - configuration mode 24, 482
  - information 111
    - interface 111
    - routes 111
    - user configuration 92, 111
  - IPv4 route statistics 248
  - packets logged 301
  - poisoned reverse 483
  - split horizon 483
  - statistics 237, 238, 274
  - version 484
- rip (IP route tag) 95
- RMON
  - configuration 565
  - information 154
- route statistics
  - IPv4 248
  - IPv6 249
- router hops 510
- Routing Information Protocol (see RIP) 24
- RSTP information 82
- Russia Class A electronic emission statement 697
- Rx/Tx statistics 264, 269

## S

- save (global command) 321
- secret, RADIUS server 333
- Secure Shell 331
- service and support
  - before you call 685
- shortcuts (CLI) 28
- SLP
  - configuration 604
  - information 179
  - statistics 317
- snap trace buffer 651
- SNMP
  - configuration
    - commands 344
    - current 346
    - link traps 345
    - location 345
    - read community string 345
    - source interface for traps 345
    - system authentication trap 344

- system contact 344
  - timeout 345
  - trap host server 344
  - version 347
  - write community string 345
- options 344
- statistics 310
- SNMPv3
  - configuration
    - access rights 346
    - commands 346
    - community table 346, 352
    - destination 347
    - display 347
    - group 346, 351
    - MIB views 347
    - Notify table 355
    - parameters 347
    - target address table 353
    - target parameters 354
    - user access 350
    - user security 348
    - USM 347, 348
    - version 347
    - view 349
  - information 44
    - access 39
    - commands 36
    - community table 40
    - group 40
    - Notify table 43
    - target address table 41
    - target parameters table 42
    - USM user table 37
    - View Table 38
- software
  - image 633
  - image file and version 33, 46
- SPAR. *See* Switch Partition.
- split horizon 483
- Stacking
  - boot options 624
  - configuration 381
- state (STP information) 80, 83, 86
- static (IP route tag) 95
- static multicast MAC 433
- static route
  - add 471
  - delete 471
  - IPv6 550

- statistics
  - 249
  - 802.1X 207
  - ACL 307
  - ARP 250
  - bridging 211
  - commands 203 to 318
  - CPU 304
  - DNS 252
  - ethernet 212
  - FCoE 309
  - hot links 230
  - ICMP 253
  - IGMP 258
  - interface 215
  - interface protocol 218
  - IPv4 240
  - IPv4 route 248
  - IPv6 243
  - LACP 229
  - Layer 2 227
  - Layer 3 236
  - link 218
  - LLDP 231
  - logged packet 299
  - management processor 291
  - MLD 260
  - NTP 314
  - OAM 233
  - OSPF 263
  - OSPFv3 268
  - port 205
  - RIP 274
  - RMON 219
  - SNMP 310
  - TCP 255, 303
  - trunk group 226
  - UDP 257, 304
  - VMAP 308
  - VRRP 272
- STG
  - information 57
- STP
  - and trunk groups 88
  - bridge parameters 430
  - bridge priority 80, 84
  - configuration 421
  - information 423
  - path-cost option 431
  - root bridge 80, 84, 430
  - RSTP/PVRST 427
  - switch reset effect 637
- switch
  - name and location 33, 46
  - resetting 637
- Switch Partition (SPAR)
  - configuration 600

- Switch Partition (SPAR)
  - configuration 25
- system
  - date and time 33, 46
  - information 33, 46
- System Error Disable and Recovery 326

## T

- tab completion (CLI) 28
- TACACS+ 335
- Taiwan Class A electronic emission statement 697
- TCP statistics 255, 303
- technical assistance 685
- telnet
  - configuring switches using 605
  - controlling access 356
  - port 356
  - radius server 333, 334, 339
- text conventions 18
- TFTP 633
  - port 356
  - PUT and GET commands 606
  - server 606
- timeout
  - idle connection 30
  - radius server 334
- timers kickoff 267, 271
- TLV 437
- trace buffer 651
- traceroute 27
- trademarks 689
- transceiver status 161, 162
- transmit flow control 380
- Trunk group information 88
- trunk hash algorithm 440
- type of area
  - OSPF 487
  - OSPFv3 497
- type parameters 95
- typographic conventions, manual 18

## U

- UCB statistics 304
- UDLD
  - configuration 375
  - information 70
  - statistics 294, 299
- UDP statistics 257
- UFP. *See* Unified Fabric Port.
- UFP. *See* Universal Fabric Port.
- Unified Fabric Port (UFP)
  - configuration 581
- United States FCC Class A notice 694
- Universal Fabric Port (UFP)
  - configuration 25
- unknown (UNK) port state 61

- upgrade
  - switch software 633
- user access control configuration 360
- user account 29

## V

- Virtual Link Aggregation Control protocol (see vLAG) 444
- virtual router
  - description 537
  - increasing priority level of 539
  - priority increment values (vrs) for VRRP 544
  - tracking criteria 539
- virtual router group
  - configuration 540
  - priority tracking 542
- Virtual Router Redundancy Protocol (see VRRP) 24
- virtualization
  - configuration 569
  - information 163
- Virtualization Configuration 569
- vLAG
  - configuration 444
  - information 445
- VLAN
  - active port 542
  - ARP entry information 97
  - configuration 458
  - information 90
  - name 58, 90
  - Number 90
  - port membership 58, 90
  - setting access VLAN 371
  - setting default number (PVID) 371
  - tagging 160
    - port configuration 370
    - port restrictions 459
    - port use of 31
  - Type 90
- VLAN Map (see VMAP) 402
- VM
  - bandwidth management 570
  - Distributed Virtual Switch 618
  - Edge Virtual Bridge configuration 584
  - group configuration 571
  - information 167
  - policy configuration 570
  - profile configuration 575
  - VMready configuration 577
  - VMware
    - configuration 576
    - dvSwitch operations 618, 619
    - information 169
    - operations 616
- VM Check
  - configuration 572, 574, 576

- VMAP
  - configuration 402
  - definition 402
  - information 89, 142
  - statistics 308
  - VLAN statistics 307
  - VMAP statistics 307
- VMware
  - configuration 576
  - distributed port group operations 619
  - dvSwitch administration 618
  - information 169
  - operations 616
- VNIC
  - configuration 578
  - group configuration 578
  - information 177
- VRRP
  - authentication parameters for IP interfaces 543
  - configuration 535
  - configuration mode 24
  - information 124
  - interface configuration 543
  - master advertisements 538
  - master advertisements, time interval 540
  - operations-level options 612
  - priority tracking options 509, 539
  - statistics 272
  - tracking configuration 544
- VSI
  - configuration mode 25

## W

- watchdog timer 647
- weight
  - COS queue 139, 384
  - COS scheduling 140
  - route map 479
  - setting virtual router priority values 544
  - VRRP priority 544
- Weighted Random Early Detection (WRED) 388
- WRED (Weighted Random Early Detection) 388



**Lenovo**<sup>™</sup>

Part Number: 00MY385

Printed in USA

(IP) P/N: 00MY385