UBIQUITI
NETWORKS



EdgeSwitch™

CLI for PoE Switches
Models: ES-24-250W, ES-24-500W,
ES-48-500W, ES-48-750W

CLI Command Reference

Table of Contents

About This Document 25
Purpose and Audience 26
Document Organization 26
Products and Models 26
Related Documents 26
Typographical Conventions 27

Chapter 1: Using the Command Line Interface 28
Command Syntax 29
Command Conventions 29
Common Parameter Values 29
slot/port Naming Convention 30
Using the "no" Form of a Command 30
Executing "show" Commands 30
CLI Output Filtering 31
EdgeSwitch Modules 32
Command Modes 32
Command Completion and Abbreviation 34
CLI Error Messages 34
CLI Line-Editing Conventions 35
Using CLI Help 35
Accessing the CLI 36

Chapter 2: Management Commands 37
Network Interface Commands 38
enable (Privileged EXEC access) 38
do (Privileged EXEC commands) 38
network parms 38
network protocol 38
network protocol dhcp 39
network mac-address 39
network mac-type 39
network javamode 39
show network 40
Console Port Access Commands 42
configure 42
line 42
serial baudrate 42
serial timeout 42
show serial 43

Telnet Commands 44
ip telnet server enable 44
transport input telnet 44
telnetcon maxsessions 44
telnetcon timeout 45
show telnetcon 45
Secure Shell Commands 46
ip ssh 46
ip ssh protocol 46
ip ssh server enable 46
sshcon maxsessions 46
sshcon timeout 47
show ip ssh 47
Management Security Commands 48
crypto certificate generate 48
crypto key generate rsa 48
crypto key generate dsa 48
Hypertext Transfer Protocol Commands 49
ip http accounting exec, ip https accounting exec 49
ip http authentication 49
ip https authentication 50
ip http server 50
ip http secure-server 50
ip http session hard-timeout 51
ip http session maxsessions 51
ip http session soft-timeout 51
ip http secure-session hard-timeout 52
ip http secure-session maxsessions 52
ip http secure-session soft-timeout 52
ip http secure-port 52
ip http secure-protocol 53
show ip http 53
Access Commands 54
disconnect 54
show loginsession 54
show loginsession long 54
User Account Commands 55
aaa authentication login 55
aaa authentication enable 55
aaa authorization 57
show authorization methods 57
enable authentication 58
username (Global Config) 58

username name nopassword 59
username name unlock 59
show users 60
show users long 60
show users accounts 60
show users login-history [long] 61
show users login-history [username] 61
login authentication 61
password 62
password (Line Configuration) 62
password (User EXEC) 63
password (aaa IAS User Config) 63
enable password (Privileged EXEC) 63
passwords min-length 64
passwords history 64
passwords aging 64
passwords lock-out 65
passwords strength-check 65
passwords strength maximum consecutive-characters 65
passwords strength maximum repeated-characters 65
passwords strength minimum uppercase-letters 66
passwords strength minimum lowercase-letters 66
passwords strength minimum numeric-characters 66
passwords strength minimum special-characters 66
passwords strength minimum character-classes 67
passwords strength exclude-keyword 67
show passwords configuration 67
show passwords result 68
write memory 68
aaa ias-user username 68
aaa session-id 68
aaa accounting 69
password (AAA IAS User Configuration) 70
clear aaa ias-users 70
show aaa ias-users 71
accounting 71
show accounting 72
show accounting methods 72
clear accounting statistics 72
SNMP Commands 73
snmp-server 73
snmp-server community 73
snmp-server community-group 73

snmp-server enable traps violation 74
snmp-server enable traps 74
snmp trap link-status 74
snmp trap link-status all 74
snmp-server enable traps linkmode 75
snmp-server enable traps multiusers 75
snmp-server enable traps stpmode 75
snmp-server engineID local 76
snmp-server filter 76
snmp-server group 76
snmp-server host 77
snmp-server user 78
snmp-server view 78
snmp-server v3-host 79
snmptrap source-interface 79
show snmp 80
show snmp engineID 80
show snmp filters 80
show snmp group 81
show snmp source-interface 81
show snmp user 81
show snmp views 81
show trapflags 82
RADIUS Commands 83
radius accounting mode 83
radius server attribute 4 83
radius server host 83
radius server key 84
radius server msgauth 85
radius server primary 85
radius server retransmit 86
radius source-interface 86
radius server timeout 86
show radius 87
show radius servers 87
show radius accounting 89
show radius accounting statistics 89
show radius source-interface 91
show radius statistics 91
TACACS+ Commands 93
tacacs-server host 93
tacacs-server key 93
tacacs-server keystring 94

tacacs-server source-interface 94
tacacs-server timeout 94
key 95
keystring. 95
port 95
priority (TACACS Config). 95
timeout. 95
show tacacs. 96
show tacacs source-interface 96
Configuration Scripting Commands. 97
script apply 97
script delete 97
script list. 98
script show 98
script validate. 98
Prelogin Banner, System Prompt, and Host Name Commands. 99
copy (pre-login banner) 99
set prompt. 99
hostname. 99
show clibanner. 99
set clibanner 100

Chapter 3: Utility Commands 101
AutoInstall Commands 102
boot autoinstall 102
boot host retrycount 102
boot host dhcp 102
boot host autosave. 103
boot host autoreboot 103
erase startup-config. 103
erase factory-defaults 103
show autoinstall 104
CLI Output Filtering Commands 105
show *xxx* | include "*string*" 105
show *xxx* | include "*string*" exclude "*string2*" 105
show *xxx* | exclude "*string*" 105
show *xxx* | begin "*string*" 106
show *xxx* | section "*string*" 106
show *xxx* | section "*string*" "*string2*". 106
show *xxx* | section "*string*" include "*string2*" 106

Dual Image Commands . . . 107
delete . . . 107
boot system . . . 107
show bootvar . . . 107
filedescr . . . 107
update bootcode . . . 107
System Information and Statistics Commands . . . 108
show arp switch . . . 108
show eventlog . . . 108
show hardware . . . 108
show version . . . 109
show platform vpd . . . 109
show interface . . . 109
show interfaces status . . . 110
show interfaces traffic . . . 110
show interface counters . . . 111
show interface ethernet . . . 112
show interface ethernet switchport . . . 115
show interface lag . . . 115
show fiber-ports optical-transceiver . . . 115
show fiber-ports optical-transceiver-info . . . 116
show mac-addr-table . . . 117
process cpu threshold . . . 118
show process app-list . . . 118
show process app-resource-list . . . 118
show process cpu . . . 119
show process proc-list . . . 119
show running-config . . . 120
show running-config interface . . . 120
show . . . 121
dir . . . 123
show sysinfo . . . 123
show tech-support . . . 124
length . . . 124
terminal length . . . 124
show terminal length . . . 124
memory free low-watermark processor . . . 125
Logging Commands . . . 126
logging buffered . . . 126
logging buffered wrap . . . 126
logging cli-command . . . 126
logging console . . . 126
logging host . . . 127
logging host reconfigure . . . 127

logging host remove 127
logging port 127
logging syslog 128
logging syslog port 128
logging syslog source-interface 128
show logging 129
show logging buffered 129
show logging hosts 130
show logging persistent 130
show logging traplogs 130
clear logging buffered 131
Email Alerting and Mail Server Commands 132
logging email 132
logging email urgent 132
logging email message-type to-addr 132
logging email from-addr 132
logging email message-type subject 133
logging email logtime 133
logging traps 133
logging email test message-type 134
show logging email config 134
show logging email statistics 134
clear logging email statistics 134
mail-server 134
security 135
port 135
username (Mail Server Config) 135
password 135
show mail-server config 135
System Utility and Clear Commands 136
traceroute 136
clear config 138
clear counters 138
clear igmpsnooping 138
clear pass 138
clear traplog 138
clear vlan 138
logout 139
ping 139
quit 140
reload 140
copy 140
file verify 143

Simple Network Time Protocol Commands 144
sntp broadcast client poll-interval 144
sntp client mode 144
sntp client port. 144
sntp unicast client poll-interval 144
sntp unicast client poll-timeout. 145
sntp unicast client poll-retry 145
sntp server. 145
sntp source-interface. 146
show sntp 146
show sntp client 146
show sntp server 147
show sntp source-interface 147
Time Zone Commands 148
clock set 148
clock summer-time date. 148
clock summer-time recurring 149
clock timezone. 149
show clock 150
show clock detail. 150
DHCP Server Commands 151
ip dhcp pool 151
client-identifier. 151
client-name 151
default-router 152
dns-server 152
hardware-address 152
host 152
lease. 153
network (DHCP Pool Config) 153
bootfile 153
domain-name. 153
domain-name enable 154
netbios-name-server 154
netbios-node-type 154
next-server 155
option 155
ip dhcp excluded-address 155
ip dhcp ping packets 156
service dhcp 156
ip dhcp bootp automatic 156
ip dhcp conflict logging 156
clear ip dhcp binding. 157

clear ip dhcp server statistics 157
clear ip dhcp conflict 157
show ip dhcp binding 157
show ip dhcp global configuration 157
show ip dhcp pool configuration 158
show ip dhcp server statistics 158
show ip dhcp conflict 159
DNS Client Commands 160
ip domain lookup 160
ip domain name 160
ip domain list 160
ip name-server 161
ip name source-interface 161
ip host 161
ipv6 host 162
ip domain retry 162
ip domain timeout 162
clear host 162
show hosts 163
show ip name source-interface 163
IP Address Conflict Commands 164
ip address-conflict-detect run 164
show ip address-conflict 164
clear ip address-conflict-detect 164
Serviceability Packet Tracing Commands 165
capture start 165
capture stop 165
capture file|remote|line 165
capture remote port 166
capture file size 166
capture line wrap 166
show capture packets 166
debug aaa accounting 166
debug aaa authorization 166
debug arp 167
debug authentication 167
debug auto-voip 167
debug clear 168
debug console 168
debug crashlog 168
debug debug-config 169
debug dhcp packet 169
debug dot1x packet 169

debug igmpsnooping packet....169
debug igmpsnooping packet transmit....170
debug igmpsnooping packet receive....170
debug ip acl....171
debug ipv6 dhcp....171
debug lacp packet....171
debug ping packet....172
debug spanning-tree bpdu....172
debug spanning-tree bpdu receive....172
debug spanning-tree bpdu transmit....173
debug tacacs....174
debug transfer....174
show debugging....174
exception protocol....174
exception dump tftp-server....175
exception dump nfs....175
exception dump filepath....175
exception core-file....175
exception switch-chip-register....176
write core....176
show exception....176
logging persistent....177
mbuf....177
show mbuf....177
show mbuf total....178
Cable Test Command....179
cablestatus....179
Remote Monitoring Commands....180
rmon alarm....180
rmon hcalarm....180
rmon event....182
rmon collection history....182
show rmon....183
show rmon collection history....184
show rmon events....185
show rmon history....185
show rmon log....187
show rmon statistics interfaces....188
show rmon hcalarms....189
Statistics Application Commands....191
stats group....191
stats flow-based....192
stats flow-based reporting....192

stats group. 193
stats flow-based. 193
show stats group. 194
show stats flow-based. 194

Chapter 4: Switching Commands. 196
Port Configuration Commands. 197
interface. 197
auto-negotiate. 197
auto-negotiate all. 197
description 197
media-type 198
mtu. 198
shutdown. 199
shutdown all. 199
speed 199
speed all. 199
show interface media-type 200
show port. 200
show port advertise. 201
show port description. 202
Spanning Tree Protocol Commands. 203
spanning-tree. 203
spanning-tree auto-edge. 203
spanning-tree bpdumigrationcheck 203
spanning-tree configuration name. 203
spanning-tree configuration revision 204
spanning-tree cost 204
spanning-tree edgeport. 204
spanning-tree forceversion 205
spanning-tree forward-time 205
spanning-tree max-age. 205
spanning-tree max-hops 205
spanning-tree mst 206
spanning-tree mst instance. 206
spanning-tree mst priority. 207
spanning-tree mst vlan. 207
spanning-tree port mode. 208
spanning-tree port mode all. 208
spanning-tree tcnguard 208
spanning-tree transmit. 208
show spanning-tree. 209
show spanning-tree brief. 210

show spanning-tree interface....210
show spanning-tree mst detailed....211
show spanning-tree mst port detailed....212
show spanning-tree mst port summary....214
show spanning-tree mst port summary active....215
show spanning-tree mst summary....215
show spanning-tree summary....216
show spanning-tree vlan....216
VLAN Commands....217
vlan database....217
network mgmt_vlan....217
vlan....217
vlan acceptframe....217
vlan ingressfilter....218
vlan internal allocation....218
vlan makestatic....218
vlan name....218
vlan participation....219
vlan participation all....219
vlan port acceptframe all....219
vlan port ingressfilter all....220
vlan port pvid all....220
vlan port tagging all....220
vlan pvid....220
vlan tagging....221
vlan association mac....221
show vlan....221
show vlan internal usage....222
show vlan brief....222
show vlan port....222
Private VLAN Commands....224
switchport private-vlan....224
switchport mode private-vlan....224
private-vlan....225
Voice VLAN Commands....226
voice vlan (Global Config)....226
voice vlan (Interface Config)....226
voice vlan data priority....226
show voice vlan....227
Provisioning (IEEE 802.1p) Commands....228
vlan port priority all....228
vlan priority....228

Protected Ports Commands 229
switchport protected (Global Config) 229
switchport protected (Interface Config) 229
show switchport protected 230
show interfaces switchport 230
GARP Commands 231
set garp timer join 231
set garp timer leave 231
set garp timer leaveall 231
show garp 232
GVRP Commands 233
set gvrp adminmode 233
set gvrp interfacemode 233
show gvrp configuration 233
GMRP Commands 235
set gmrp adminmode 235
set gmrp interfacemode 235
show gmrp configuration 235
show mac-address-table gmrp 236
Port-Based Network Access Control Commands 237
aaa authentication dot1x default 237
clear dot1x statistics 237
clear dot1x authentication-history 237
clear radius statistics 237
dot1x eapolflood 237
dot1x guest-vlan 238
dot1x initialize 238
dot1x max-req 238
dot1x max-users 238
dot1x port-control 239
dot1x port-control all 239
dot1x mac-auth-bypass 239
dot1x re-authenticate 240
dot1x re-authentication 240
dot1x system-auth-control 240
dot1x system-auth-control monitor 240
dot1x timeout 241
dot1x unauthenticated-vlan 241
dot1x user 242
show authentication methods 242
show dot1x 243
show dot1x authentication-history 246
show dot1x clients 246
show dot1x users 247

802.1X Supplicant Commands 248
dot1x pae 248
dot1x supplicant port-control 248
dot1x supplicant max-start 248
dot1x supplicant timeout start-period 248
dot1x supplicant timeout held-period 249
dot1x supplicant timeout auth-period 249
dot1x supplicant user 249
show dot1x statistics 249
Storm-Control Commands 251
storm-control broadcast 251
storm-control broadcast level 251
storm-control broadcast rate 252
storm-control multicast 252
storm-control multicast level 253
storm-control multicast rate 253
storm-control unicast 253
storm-control unicast level 254
storm-control unicast rate 254
show storm-control 255
Port-Channel/LAG (802.3ad) Commands 256
port-channel 256
addport 256
deleteport (Interface Config) 256
deleteport (Global Config) 257
lacp admin key 257
lacp collector max-delay 257
lacp actor admin key 257
lacp actor admin state individual 258
lacp actor admin state longtimeout 258
lacp actor admin state passive 258
lacp actor admin state 259
lacp actor port priority 259
lacp partner admin key 259
lacp partner admin state individual 260
lacp partner admin state longtimeout 260
lacp partner admin state passive 260
lacp partner port id 261
lacp partner port priority 261
lacp partner system-id 261
lacp partner system priority 262
interface lag 262
port-channel static 262

port lacpmode 262
port lacpmode enable all 263
port lacptimeout (Interface Config) 263
port lacptimeout (Global Config) 263
port-channel adminmode 264
port-channel linktrap 264
port-channel load-balance 264
port-channel local-preference 265
port-channel min-links 265
port-channel name 265
port-channel system priority 265
show lacp actor 266
show lacp partner 266
show port-channel brief 266
show port-channel 267
show port-channel system priority 267
show port-channel counters 268
clear port-channel counters 268
clear port-channel all counters 268
Port Mirroring Commands 269
monitor session 269
no monitor 270
show monitor session 270
show vlan remote-span 270
Static MAC Filtering Commands 271
macfilter 271
macfilter adddest 271
macfilter adddest all 272
macfilter addsrc 272
macfilter addsrc all 272
show mac-address-table static 273
show mac-address-table staticfiltering 273
DHCP Client Commands 274
dhcp client vendor-id-option 274
dhcp client vendor-id-option-string 274
show dhcp client vendor-id-option 274
DHCP Snooping Configuration Commands 275
ip dhcp snooping 275
ip dhcp snooping vlan 275
ip dhcp snooping verify mac-address 275
ip dhcp snooping database 275
ip dhcp snooping database write-delay 276
ip dhcp snooping binding 276

ip dhcp filtering trust 276
ip dhcp snooping limit 276
ip dhcp snooping log-invalid 277
ip dhcp snooping trust 277
show ip dhcp snooping 277
show ip dhcp snooping binding 278
show ip dhcp snooping database 278
show ip dhcp snooping interfaces 278
show ip dhcp snooping statistics 279
clear ip dhcp snooping binding 280
clear ip dhcp snooping statistics 280
IGMP Snooping Configuration Commands 281
set igmp 281
set igmp interfacemode 281
set igmp fast-leave 282
set igmp groupmembership-interval 282
set igmp maxresponse 282
set igmp mcrtrexpiretime 283
set igmp mrouter 283
set igmp mrouter interface 283
set igmp report-suppression 284
show igmpsnooping 284
show igmpsnooping mrouter interface 285
show igmpsnooping mrouter vlan 285
show igmpsnooping ssm 286
show mac-address-table igmpsnooping 286
IGMP Snooping Querier Commands 287
set igmp querier 287
set igmp querier query-interval 287
set igmp querier timer expiry 288
set igmp querier version 288
set igmp querier election participate 288
show igmpsnooping querier 288
Port Security Commands 290
port-security 290
port-security max-dynamic 290
port-security max-static 290
port-security mac-address 291
port-security mac-address move 291
port-security mac-address sticky 291
show port-security 291
show port-security dynamic 292
show port-security static 292
show port-security violation 293

LLDP (802.1AB) Commands 294
lldp transmit 294
lldp receive 294
lldp timers 294
lldp transmit-tlv 295
lldp transmit-mgmt 295
lldp notification 295
lldp notification-interval 295
clear lldp statistics 296
clear lldp remote-data 296
show lldp 296
show lldp interface 296
show lldp statistics 297
show lldp remote-device 297
show lldp remote-device detail 298
show lldp local-device 299
show lldp local-device detail 299
LLDP-MED Commands 300
lldp med 300
lldp med confignotification 300
lldp med transmit-tlv 300
lldp med all 301
lldp med confignotification all 301
lldp med faststartrepeatcount 301
lldp med transmit-tlv all 301
show lldp med 302
show lldp med interface 302
show lldp med local-device detail 303
show lldp med remote-device 304
show lldp med remote-device detail 304
Denial of Service Commands 306
dos-control all 306
dos-control sipdip 306
dos-control firstfrag 307
dos-control tcpfrag 307
dos-control tcpflag 307
dos-control l4port 308
dos-control smacdmac 308
dos-control tcpport 308
dos-control udpport 309
dos-control tcpflagseq 309
dos-control tcpoffset 309
dos-control tcpsyn 310

dos-control tcpsynfin....310
dos-control tcpfinurgpsh....310
dos-control icmpv4....310
dos-control icmpv6....311
dos-control icmpfrag....311
show dos-control....311
MAC Database Commands....313
bridge aging-time....313
show forwardingdb agetime....313
show mac-address-table multicast....313
show mac-address-table stats....314

Chapter 5: Routing Commands....315
Address Resolution Protocol Commands....316
arp....316
arp cachesize....316
arp dynamicrenew....316
arp purge....317
arp resptime....317
arp retries....317
arp timeout....317
clear arp-cache....318
clear arp-switch....318
show arp....318
show arp brief....319
show arp switch....319
IP Routing Commands....320
routing....320
ip routing....320
ip address....320
ip address dhcp....321
ip default-gateway....321
release dhcp....322
renew dhcp....322
renew dhcp network-port....322
renew dhcp service-port....322
ip route....322
ip route default....323
ip route distance....323
ip netdirbcast....324
ip mtu....324
encapsulation....324
show dhcp lease....325

show ip brief 325
show ip interface 326
show ip interface brief 327
show ip route 327
show ip route ecmp-groups 329
show ip route summary 329
clear ip route counters 331
show ip route preferences 331
show ip stats 332
show routing heap summary 332
Routing Policy Commands 333
ip policy route-map 333
ip prefix-list 333
ip prefix-list description 334
route-map 334
match ip address 335
match ip address *access-list-number* | *access-list-name* 335
match length 337
match mac-list 338
set interface 339
set ip next-hop 339
set ip default next-hop 339
set ip precedence 340
show ip policy 340
show ip prefix-list 341
show route-map 342
clear ip prefix-list 342
Router Discovery Protocol Commands 343
ip irdp 343
ip irdp address 343
ip irdp holdtime 343
ip irdp maxadvertinterval 343
ip irdp minadvertinterval 344
ip irdp multicast 344
ip irdp preference 344
show ip irdp 345
Virtual LAN Routing Commands 346
vlan routing 346
interface vlan 348
show ip vlan 348
IP Helper Commands 349
clear ip helper statistics 350
ip helper-address (Global Config) 350

ip helper-address (Interface Config) 351
ip helper enable 352
show ip helper-address 353
show ip helper statistics 353
ICMP Throttling Commands 355
ip unreachables 355
ip redirects 355
ip icmp echo-reply 355
ip icmp error-interval 356

Chapter 6: IPv6 Management Commands 357
IPv6 Management Commands 358
network ipv6 enable 358
network ipv6 address 358
network ipv6 gateway 359
network ipv6 neighbor 359
show network ipv6 neighbors 359
ping ipv6 360
ping ipv6 interface 360

Chapter 7: Quality of Service Commands 361
Class of Service Commands 362
classofservice dot1p-mapping 362
classofservice ip-dscp-mapping 362
classofservice ip-precedence-mapping 362
classofservice trust 363
cos-queue max-bandwidth 363
cos-queue min-bandwidth 363
cos-queue random-detect 363
cos-queue strict 364
random-detect 364
random-detect exponential weighting-constant 364
random-detect queue-parms 365
traffic-shape 365
show classofservice dot1p-mapping 365
show classofservice ip-dscp-mapping 366
show classofservice ip-precedence-mapping 366
show classofservice trust 366
show interfaces cos-queue 366
show interfaces random-detect 367
show interfaces tail-drop-threshold 367
Differentiated Services Commands 368
diffserv 368

DiffServ Class Commands....369
class-map....369
class-map rename....369
match ethertype....370
match any....370
match class-map....370
match cos....371
match secondary-cos....371
match destination-address mac....371
match dstip....371
match dstl4port....371
match ip dscp....372
match ip precedence....372
match ip tos....372
match protocol....373
match signature....373
match source-address mac....373
match srcip....373
match srcl4port....373
match src port....374
match vlan....374
match secondary-vlan....374
DiffServ Policy Commands....375
assign-queue....375
drop....375
mirror....375
redirect....375
conform-color....376
class....376
mark cos....376
mark secondary-cos....376
mark cos-as-sec-cos....377
mark ip-dscp....377
mark ip-precedence....377
police-simple....377
police-single-rate....378
police-two-rate....378
policy-map....378
policy-map rename....379
DiffServ Service Commands....380
service-policy....380
DiffServ Show Commands....381
show class-map....381

show diffserv 381
show policy-map....382
show diffserv service 383
show diffserv service brief....384
show policy-map interface 384
show service-policy 385
MAC Access Control List Commands 386
mac access-list extended 386
mac access-list extended rename 386
{deny | permit} (MAC ACL) 386
mac access-group 388
show mac access-lists 388
IP Access Control List Commands 390
access-list....390
no access-list....392
ip access-list 392
ip access-list rename 392
{deny | permit} (IP ACL) 393
ip access-group 395
acl-trapflags 396
show ip access-lists....396
show access-lists 397
show access-lists vlan 398
IPv6 Access Control List Commands....399
ipv6 access-list....399
ipv6 access-list rename....399
{deny | permit} (IPv6) 400
ipv6 traffic-filter....402
show ipv6 access-lists 403
Time Range Commands for Time-Based ACLs....404
time-range....404
absolute 404
periodic....405
show time-range....405
Auto-Voice over IP Commands....406
auto-voip 406
auto-voip oui 406
auto-voip oui-based priority....407
auto-voip protocol-based 407
auto-voip vlan 407
show auto-voip 408
show auto-voip oui-table....409

Chapter 8: Power over Ethernet (PoE) Commands. 410
PoE Management Commands 411
show poe counters 411
clear poe counters 411
show poe port 411
show poe status. 412
poe opmode 412

Appendix A: Log Messages 413
Core 414

Appendix B: Contact Information 431
Ubiquiti Networks Support 431
Online Resources. 431

About This Document

This section contains the following information about this document:

- **"Purpose and Audience" on page 26**
- **"Document Organization" on page 26**
- **"Document Organization" on page 26**
- **"Products and Models" on page 26**
- **"Related Documents" on page 26**
- **"Typographical Conventions" on page 27**

Purpose and Audience

This reference lists the commands to configure the EdgeSwitch software features using the EdgeSwitch command line interface (CLI). The information in this reference is intended for system administrators who are responsible for configuring and operating a network using EdgeSwitch devices.

To obtain the greatest benefit from this reference, you should have an understanding of the base software and should have read the specification for your networking device platform. You should also have basic knowledge of Ethernet and networking concepts.

Document Organization

This guide contains the following sections:

- **"Chapter 1: Using the Command Line Interface" on page 28**
- **"Chapter 2: Management Commands" on page 37**
- **"Chapter 3: Utility Commands" on page 101**
- **"Chapter 4: Switching Commands" on page 196**
- **"Chapter 5: Routing Commands" on page 315**
- **"Chapter 6: IPv6 Management Commands" on page 357**
- **"Chapter 7: Quality of Service Commands" on page 361**
- **"Chapter 8: Power over Ethernet (PoE) Commands" on page 410**
- **"Appendix A: Log Messages" on page 413**
- **"Appendix B: Contact Information" on page 431**

Products and Models

This document covers the following Ubiquiti products and models:

Table 1. Affected Products

Name	Description	Part Number
EdgeSwitch 48-port 750W	Managed PoE+ Gigabit Switch with SFP+	ES-48-750W
EdgeSwitch 48-port 500W	Managed PoE+ Gigabit Switch with SFP+	ES-48-500W
EdgeSwitch 24-port 500W	Managed PoE+ Gigabit Switch with SFP	ES-24-500W
EdgeSwitch 24-port 250W	Managed PoE+ Gigabit Switch with SFP	ES-24-250W

Related Documents

Related documents for EdgeSwitch products include the following:

- *EdgeSwitch Administration Guide*
- *EdgeSwitch ES-24 Quick Start Guide*
- *EdgeSwitch ES-48 Quick Start Guide*

To download EdgeSwitch documents:

1. Go to the *Downloads* page on the Ubiquiti website: http://www.ubnt.com/download/
2. Select **EdgeMAX** from the *Platform* drop-down box.
3. Select **EdgeSwitch** from the *Product Group* drop-down box.
4. Select your EdgeSwitch model from the *Model* drop-down box.
5. Scroll down to *Documentation PDFs* and click the document to download.

For additional information, refer to the EdgeSwitch community web site: community.ubnt.com/edgemax

Typographical Conventions

Table 2 lists typographical conventions used throughout this document.

Table 2. Typographical Conventions

Convention	Indicates	Example
Bold	User selection User-entered text	Select **VLAN 2** from the *VLAN ID* list; Click **Submit** enter **3** to assign VLAN 3 as the default VLAN
Italic	Name of a field Name of UI page, dialog box, window, etc.	delete the existing name in the *Username* field Use the *IP Address Conflict Detection* page
>	Order of navigation selections to access a page	To access the *Session* page, click **System** > **Users** > **Session**
`Courier` font	CLI commands and their output	`show network`

Chapter 1: Using the Command Line Interface

The command line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

- **"Command Syntax" on page 29**
- **"Command Conventions" on page 29**
- **"Common Parameter Values" on page 29**
- **"slot/port Naming Convention" on page 30**
- **"Using the "no" Form of a Command" on page 30**
- **"Executing "show" Commands" on page 30**
- **"CLI Output Filtering" on page 31**
- **"EdgeSwitch Modules" on page 32**
- **"Command Modes" on page 32**
- **"Command Completion and Abbreviation" on page 34**
- **"CLI Error Messages" on page 34**
- **"CLI Line-Editing Conventions" on page 35**
- **"Using CLI Help" on page 35**
- **"Accessing the CLI" on page 36**

Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as show network or clear vlan, do not require parameters. Other commands, such as network parms, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the network parms command syntax:

`network parms ipaddr netmask [gateway]`

- `network parms` is the command name.
- `ipaddr` and `netmask` are parameters and represent required values that you must enter after you type the command keywords.
- `[gateway]` is an optional parameter; you are not required to enter a value in place of the parameter.

The *CLI Command Reference* lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The `show` commands also contain a description of the information that the command shows.

Command Conventions

The parameters for a command might include mandatory values, optional values, or keyword choices. Parameters are order-dependent. Table 3 describes the conventions this document uses to distinguish between value types.

Table 3. Parameter Conventions

Symbol	Example	Description
[ ] square brackets	`[value]`	Indicates an optional parameter
italic font	*value* or *[value]*	Indicates a variable value. Specify an appropriate value (name or number).
{ } curly braces	`{choice1 | choice2}`	Indicates that you must select a parameter from the list of choices
| vertical bar	`choice1 | choice2`	Separates mutually exclusive choices
[{ }] braces within square brackets	`[{choice1 | choice2}]`	Indicates a choice within an optional element

Common Parameter Values

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. Table 4 describes common parameter values and value formatting.

Table 4. Parameter Descriptions

Parameter	Description
ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats: `a` (32 bits) `a.b` (8.24 bits) `a.b.c` (8.8.16 bits) `a.b.c.d` (8.8.8.8 bits) In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where n is any valid hexadecimal, octal or decimal number): `0xn` (CLI assumes hexadecimal format) `0n` (CLI assumes octal format with leading zeros) `n` (CLI assumes decimal format)

Table 4. Parameter Descriptions (Continued)

Parameter	Description
ipv6-address	`FE80:0000:0000:0000:020F:24FF:FEBF:DBCB`, or `FE80:0:0:0:20F:24FF:FEBF:DBCB`, or `FE80::20F24FF:FEBF:DBCB`, or `FE80:0:0:0:20F:24FF:128:141:49:32` For additional information, refer to RFC 3513.
Interface or *slot/port*	Valid slot and port number separated by a forward slash. For example, 0/1 represents slot 0 and port 1.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, "System Name with Spaces". An empty string ("") is not valid.

slot/port Naming Convention

The EdgeSwitch software references physical entities such as cards and ports using a slot/port naming convention. The software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 5. Types of Slots

Parameter	Description
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces. The value of logical slot numbers depend on the type of logical interface and can vary from platform to platform.
CPU slot numbers	The CPU slots immediately follow the logical slots.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, "System Name with Spaces". An empty string ("") is not valid.

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 6. Types of Ports

Parameter	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from one. For example, port 1 on slot 0 (an internal port) for a standalone switch is 0/1, port 2 is 0/2, port 3 is 0/3, etc.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces only used for bridging functions. • VLAN routing interfaces are only used for routing functions.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

Using the "no" Form of a Command

The `no` keyword is a specific form of an existing command and does not represent a new or distinct command. Only configuration commands have an available `no` form. Almost every configuration command has a `no` form. In general, use the `no` form to reverse the action of a command or reset a value back to its default. For example, the `no shutdown` configuration command reverses the shutdown of an interface. Use the command without `no` to re-enable a disabled feature or to enable a feature that is disabled by default.

Executing "show" Commands

All `show` commands can be issued from any configuration mode (Global Configuration, Interface Configuration, VLAN Configuration, etc.). The `show` commands provide information about system and feature-specific configuration, status, and statistics. Previously, `show` commands could be issued only in User EXEC or Privileged EXEC modes.

CLI Output Filtering

Many CLI show commands include considerable content to display to the user. This can make output confusing and cumbersome to parse through to find the information of desired importance. The CLI Output Filtering feature allows the user, when executing CLI show display commands, to optionally specify arguments to filter the CLI output to display only desired information. The result is to simplify the display and make it easier for the user to find the information the user is interested in.

The main functions of the CLI Output Filtering feature are:

- Pagination Control
  - Supports enabling/disabling paginated output for all show CLI commands. When disabled, output is displayed in its entirety. When enabled, output is displayed page-by-page such that content does not scroll off the terminal screen until the user presses a key to continue. `--More--` or `(q)uit` is displayed at the end of each page.
  - When pagination is enabled, press the return key to advance a single line, press **q** or **Q** to stop pagination, or press any other key to advance a whole page. These keys are not configurable.



Note: Although some EdgeSwitch `show` commands already support pagination, the implementation is unique per command and not generic to all commands.

- Output Filtering
  - "Grep"-like control for modifying the displayed output to only show the user-desired content.
    - Filter-displayed output to only include lines containing a specified string match.
    - Filter-displayed output to exclude lines containing a specified string match.
    - Filter-displayed output to only include lines including and following a specified string match.
    - Filter-displayed output to only include a specified section of the content (e.g. "interface 0/1") with a configurable end-of-section delimiter.
    - String matching should be case-insensitive.
    - Pagination, when enabled, also applies to filtered output.

Example: The following shows an example of the extensions made to the CLI show commands for the Output Filtering feature.

```
(UBNT EdgeSwitch) #show running-config ?
<cr> Press enter to execute the command.
| Output filter options.
<scriptname> Script file name for writing active configuration.
all Show all the running configuration on the switch.
interface Display the running configuration for specificed interface on the
switch.
(UBNT EdgeSwitch) #show running-config | ?
begin Begin with the line that matches
exclude Exclude lines that matches
include Include lines that matches
section Display portion of lines
```

EdgeSwitch Modules

The EdgeSwitch software consists of flexible modules that can be applied in various combinations to develop advanced products for Layer 2 and above. The commands and command modes available on your switch depend on the installed modules. Additionally, for some show commands, the output fields might change based on the modules included in the EdgeSwitch software.

The EdgeSwitch software suite includes the following modules:

- Switching (Layer 2)
- Routing (Layer 3)



Note: Only static routing is available. Dynamic routing protocols are not available in the EdgeSwitch software.

- Quality of Service
- Management (CLI, browser-based UI, and SNMP)
- IPv6 Management—Allows management of the EdgeSwitch device through an IPv6 through an IPv6 address without requiring the IPv6 Routing package in the system. The management address can be associated with the network port (front-panel switch ports), a routine interface (port or VLAN) and the Service port.
- Secure Management

Not all modules are available for all platforms or software releases.

Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific EdgeSwitch software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 7 describes the command modes and the prompts visible in that mode.



Note: The command modes available on your switch depend on the software modules that are installed.

Table 7. CLI Command Modes

Command Mode	Prompt	Mode Description
User EXEC	`Switch>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`Switch#`	Allows you to issue any EXEC command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	`Switch (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	`Switch (Vlan)#`	Groups all the VLAN commands.
Interface Config	`Switch (Interface slot/port)#`	Manages the operation of an interface and provides access to the router interface configuration commands.
	`Switch (Interface slot/port-slot/port#`	Use this mode to manage a range of interfaces. For example: `Switch (Interface 0/1-0/4) #`
	`Switch (Interface lag lag-intf-num)#`	Enters LAG Interface configuration mode for the specified LAG.
	`Switch (Interface vlan vlan-id)#`	Enters VLAN routing interface configuration mode for the specified VLAN ID.
Line SSH	`Switch (config-ssh)#`	Contains commands to configure SSH login/enable authentication.

Table 7. CLI Command Modes (Continued)

Symbol	Example	Description
Line Telnet	`Switch (config-telnet)#`	Contains commands to configure telnet login/enable authentication.
AAA IAS User Config	`Switch (Config-IAS-User)#`	Allows password configuration for a user in the IAS database.
Mail Server Config	`Switch (Mail-Server)#`	Allows configuration of the email server.
Policy Map Config	`Switch (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.
Policy Class Config	`Switch (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
TACACS Config	`Switch (Tacacs)#`	Contains commands to configure properties for the TACACS servers.
DHCP Pool Config	`Switch (Config dhcp-pool)#`	Contains the DHCP server IP address pool configuration commands.
Support Mode	`Switch (Support)#`	Allows access to the support commands, which should only be used by the manufacturer's technical support personnel as improper use could cause unexpected system behavior and/or invalidate product warranty.

Table 8 explains how to enter or exit each mode.

Table 8. CLI Mode Access and Exit

Command Mode	Access Method	Exit or Access Previous Mode
User EXEC	This is the first level of access.	To exit, enter **logout**.
Privileged EXEC	From User EXEC mode, enter: `enable`	To exit to User EXEC mode, enter **exit** or press Ctrl-Z.
Global Config	From Privileged EXEC mode, enter: `configure`	To exit to Privileged EXEC mode, enter **exit** or press Ctrl-Z.
VLAN Config	From Privileged EXEC mode, enter: `vlan database`	To exit to Privileged EXEC mode, enter **exit** or press Ctrl-Z.
Interface Config	From Global Config mode, enter one of the following: `interface` *`slot/port`* `interface` *`slot/port-slot/port`* `interface lag` *`lag-intf-num`* `interface vlan` *`vlan-id`*	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
Line SSH	From Global Config mode, enter: `line ssh`	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
Line Telnet	From Global Config mode, enter: `line telnet`	To exit to Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter Ctrl-Z.
AAA IAS User Config	From Global Config mode, enter: `aaa ias-user username name`	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
Mail Server Config	From Global Config mode, enter: `mail-server address`	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
Policy-Map Config	From Global Config mode, enter: `policy-map`	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
Policy-Class-Map Config	From Policy Map Config mode enter: `class`	To exit to Policy Map Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.

Table 8. CLI Mode Access and Exit (Continued)

Command Mode	Access Method	Exit or Return to Previous Mode
Class-Map Config	From Global Config mode, enter: `class-map` (see **"class-map" on page 369**)	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
MAC Access-list Config	From Global Config mode, enter: `mac access-list extended name`	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
TACACS Config	From Global Config mode, enter: `tacacs-server host ip-addr` where `ip-addr` is the IP address of the TACACS server on your network.	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
DHCP Pool Config	From Global Config mode, enter: `ip dhcp pool pool-name`	To exit to Global Config mode, enter **exit**. To return to Privileged EXEC mode, enter Ctrl-Z.
Support	From Privileged EXEC mode, enter: `support` Note: The `support` command is available only if the `techsupport enable` command has been issued.	To exit to Privileged EXEC mode, enter exit or press Ctrl-Z.

Command Completion and Abbreviation

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 9 describes the most common CLI error messages.

Table 9. CLI Error Messages

Message Text	Description
`% Invalid input detected at '^' marker.`	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.
`Command not found / Incomplete command. Use ? to list commands.`	Indicates that you did not enter the required keywords or values.
`Ambiguous command`	Indicates that you did not enter enough letters to uniquely identify the command.

CLI Line-Editing Conventions

Table 10 describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering help from the User or Privileged EXEC modes.

Table 10. CLI Editing Conventions

Key Sequence	Description
DEL or backspace	Delete previous character
Ctrl-A	Go to beginning of line
Ctrl-E	Go to end of line
Ctrl-F	Go forward one character
Ctrl-B	Go backward one character
Ctrl-D	Delete current character
Ctrl-U, X	Delete to beginning of line
Ctrl-K	Delete to end of line
Ctrl-W	Delete previous word.
Ctrl-T	Transpose previous character.
Ctrl-P	Go to previous line in history buffer.
Ctrl-R	Rewrites or pastes the line.
Ctrl-N	Go to next line in history buffer.
Ctrl-Y	Prints last deleted character.
Ctrl-Q	Enables serial flow.
Ctrl-S	Disables serial flow.
Ctrl-Z	Return to root command prompt.
Tab, <SPACE>	Command-line completion.
Exit	Go to next lower command prompt.
?	List available commands, keywords, or parameters.

Using CLI Help

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(UBNT EdgeSwitch) >?

enable        Enter into user privilege mode.
help          Display help for various special keys.
logout        Exit this session. Any unsaved changes are lost.
password      Change an existing user's password.
ping          Send ICMP echo packets to a specified IP address.
quit          Exit this session. Any unsaved changes are lost.
show          Display Switch Options and Settings.
telnet        Telnet to a remote host.
```

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(UBNT EdgeSwitch) #network ?

ipv6          Configure IPv6 parameters for system network.
javamode      Enable/Disable.
mac-address   Configure MAC Address.
mac-type      Select the locally administered or burned-in MAC address.
mgmt_vlan     Configure the Management VLAN ID of the switch.
parms         Configure Network Parameters of the device.
protocol      Select DHCP, BootP, or None as the network config protocol.
```

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(UBNT EdgeSwitch) #network parms ?

<ipaddr>      Enter the IP Address.
none          Reset IP address and gateway on management interface
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr> Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(UBNT EdgeSwitch) #show m?

mac                 mac-addr-table      mac-address-table
mail-server         mbuf                monitor
```

Accessing the CLI

After you have connected the EdgeSwitch to your network, you can access the CLI using a direct console connection or by a telnet or SSH connection from a remote management host.

For on how to connect the switch to your network, refer to the *Quick Start Guide* that came with the EdgeSwitch.

Chapter 2: Management Commands

This chapter describes the management commands available in the EdgeSwitch CLI.

The chapter contains the following sections:

- **"Network Interface Commands" on page 38**
- **"Telnet Commands" on page 44**
- **"Secure Shell Commands" on page 46**
- **"Management Security Commands" on page 48**
- **"Hypertext Transfer Protocol Commands" on page 49**
- **"Access Commands" on page 54**
- **"User Account Commands" on page 55**
- **"SNMP Commands" on page 73**
- **"RADIUS Commands" on page 83**
- **"TACACS+ Commands" on page 93**
- **"Configuration Scripting Commands" on page 97**
- **"Prelogin Banner, System Prompt, and Host Name Commands" on page 99**



Note: The commands in this chapter consist of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Network Interface Commands



Note: Only static routing is available. Dynamic routing protocols are not available in the EdgeSwitch software.

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see **"network mgmt_vlan" on page 217**.

enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format	`enable`
Mode	User EXEC

do (Privileged EXEC commands)

This command executes Privileged EXEC mode commands from any of the configuration modes.

Format	`do` *`Priv_Exec_Mode_Command`*
Mode	• Global Config • Interface Config • VLAN Config • Routing Config

Example: The following is an example of the `do` command that executes the Privileged Exec command script list in Global Config Mode.

```
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch)(config)#do script list
Configuration Script Name Size(Bytes)
-------------------------------- -----------
backup-config 2105
running-config 4483
startup-config 445
3 configuration script(s) found.
2041 Kbytes free.
Routing(config)#
```

network parms

This command sets the device's IP address, subnet mask, and gateway. The IP address and gateway must be on the same subnet. If you specify the `none` option, the IP address and subnet mask are set to the factory defaults.

Format	`network parms {`*`ipaddr netmask [gateway]`*` | none}`
Mode	Privileged EXEC

network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the `bootp` parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the `dhcp` parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the `none` parameter, you must configure the network information for the switch manually.

Default	none
Format	`network protocol {none | bootp | dhcp}`
Mode	Privileged EXEC

network protocol dhcp

This command enables the DHCPv4 client on a Network port. If the `client-id` optional parameter is given, the DHCP client messages are sent with the client identifier option.

Default	none
Format	`network protocol dhcp [client-id]`
Mode	Global Config

There is no support for the `no` form of the command `network protocol dhcp client-id`. To remove the `client-id` option from the DHCP client messages, issue the command `network protocol dhcp` without the `client-id` option. The command `network protocol none` can be used to disable the DHCP client and `client-id` option on the interface.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) # network protocol dhcp client-id
```

network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format	`network mac-address macaddr`
Mode	Privileged EXEC

network mac-type

This command specifies whether the switch uses the burned-in or the locally administered MAC address.

Default	burnedin
Format	`network mac-type {local | burnedin}`
Mode	Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format	`no network mac-type`
Mode	Privileged EXEC

network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the web interface. When access is enabled, the Java applet can be viewed from the web interface. When access is disabled, the user cannot view the Java applet.

Default	enabled
Format	`network javamode`
Mode	Privileged EXEC

no network javamode

This command disallows access to the Java applet in the header frame of the web interface. When access is disabled, the user cannot view the Java applet.

Format `no network javamode`

Mode Privileged EXEC

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether or not any member ports are up; therefore, the `show network` command will always show `Interface Status` as Up.

Format `show network`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface Status	The network interface status; it is always considered to be "Up".
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as 12 hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are `bootp | dhcp | none`.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are `dhcp | none`.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the network port. See **"network protocol dhcp" on page 39**.

Example: The following shows example CLI display output for the network port.

```
(admin) #show network
Interface Status.............................. Always Up
IP Address.................................... 10.250.3.1
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.250.3.3
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ............................... 2003::1/128
```

```
IPv6 Default Router is ..... fe80::204:76ff:fe73:423a
Burned In MAC Address..... 00:10:18:82:06:4C
Locally Administered MAC address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Configured IPv4 Protocol ..... None
Configured IPv6 Protocol ..... DHCP
DHCPv6 Client DUID ..... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode..... Disabled
Management VLAN ID..... 1
```

Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

configure

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

Format `configure`

Mode Privileged EXEC

line

This command gives you access to the Line Console mode, which allows you to configure various Telnet settings and the console port, as well as to configure console login/enable authentication.

Format `line {console | telnet | ssh}`

Mode Global Config

Term	Definition
console	Console terminal line.
telnet	Virtual terminal for remote console access (Telnet).
ssh	Virtual terminal for secured remote console access (SSH).

Example: The following shows an example of the CLI command.

```
(UBNT EdgeSwitch)(config)#line telnet
(UBNT EdgeSwitch)(config-telnet)#
```

serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default 9600

Format `serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`

Mode Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`

Mode Line Config

serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default 5

Format `serial timeout 0-160`

Mode Line Config

no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format `no serial timeout`

Mode Line Config

show serial

This command displays serial communication settings for the switch.

Format `show serial`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The factory default is 9600 baud.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity Type	The Parity Method used on the Serial Port. The Parity Method is always None.

Telnet Commands

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default	enabled
Format	`ip telnet server enable`
Mode	Privileged EXEC

no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format	`no ip telnet server enable`
Mode	Privileged EXEC

transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.



Note: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the `ip telnet server enable` command to enable Telnet Server Admin Mode.

Default	enabled
Format	`transport input telnet`
Mode	Line Config

no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format	`no transport input telnet`
Mode	Line Config

telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

Default	5
Format	`telnetcon maxsessions` *`0-5`*
Mode	Privileged EXEC

no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format	`no telnetcon maxsessions`
Mode	Privileged EXEC

telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

Note: When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default	5
Format	`telnetcon timeout` *`1-160`*
Mode	Privileged EXEC

no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

Note: Changing the timeout value for active sessions does not become effective until the session is accessed again. Also, any keystroke activates the new timeout duration.

Format	`no telnetcon timeout`
Mode	Privileged EXEC

show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format	`show telnetcon`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

Secure Shell Commands

This section describes the commands you use to configure Secure Shell (SSH) access to the switch. Use SSH to access the switch from a remote management host.



Note: The system allows a maximum of 5 SSH sessions.

ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the `ip ssh server enable` command.)

Default	disabled
Format	`ip ssh`
Mode	Privileged EXEC

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default	2
Format	`ip ssh protocol [1] [2]`
Mode	Privileged EXEC

ip ssh server enable

This command enables the IP secure shell server. No new SSH connections are allowed, but the existing SSH connections continue to work until timed-out or logged-out.

Default	enabled
Format	`ip ssh server enable`
Mode	Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server.

Format	`no ip ssh server enable`
Mode	Privileged EXEC

sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no SSH connection can be established. The range is 0 to 5.

Default	5
Format	`sshcon maxsessions` *`0-5`*
Mode	Privileged EXEC

no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format	`no sshcon maxsessions`
Mode	Privileged EXEC

sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Default	5
Format	`sshcon timeout` *`1-160`*
Mode	Privileged EXEC

no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re-accessed. Also, any keystroke activates the new timeout duration.

Format	`no sshcon timeout`
Mode	Privileged EXEC

show ip ssh

This command displays the SSH settings.

Format	`show ip ssh`
Mode	Privileged EXEC

Term	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

Management Security Commands

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

crypto certificate generate

Use this command to generate a self-signed certificate for HTTPS. The generated RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format	`crypto certificate generate`
Mode	Global Config

no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self-signed or downloaded from an outside source.

Format	`no crypto certificate generate`
Mode	Global Config

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format	`crypto key generate rsa`
Mode	Global Config

no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format	`no crypto key generate rsa`
Mode	Global Config

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format	`crypto key generate dsa`
Mode	Global Config

no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format	`no crypto key generate dsa`
Mode	Global Config

Hypertext Transfer Protocol Commands

This section describes the commands you use to configure Hypertext Transfer Protocol (HTTP) and secure HTTP access to the switch. Access to the switch by using a web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the web.

ip http accounting exec, ip https accounting exec

This command applies user exec (start-stop/stop-only) accounting list to the line methods HTTP and HTTPS.

The user exec accounting list should be created using the command **"aaa accounting" on page 69**.

Format `ip {http|https} accounting exec {default|listname}`

Mode Global Config

Parameter	Description
`http/https`	The line method for which the list needs to be applied.
`default`	The default list of methods for authorization services.
`listname`	An alphanumeric character string used to name the list of accounting methods.

no ip http/https accounting exec

This command deletes the authorization method list.

Format `no ip {http|https} accounting exec {default|listname}`

Mode Global Config

ip http authentication

Use this command to specify authentication methods for http server users. The default configuration is the local user database is checked. This action has the same effect as the command `ip http authentication local`. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example, if none is specified as an authentication method after RADIUS, no authentication is used if the RADIUS server is down.

Default local

Format `ip http authentication method1 [method2...]`

Mode Global Config

The following table lists the possible values for the *method* parameter.

Parameter Value	Description
`local`	Uses the local username database for authentication.
`none`	Uses no authentication.
`radius`	Uses the list of all RADIUS servers for authentication.
`tacacs`	Uses the list of all TACACS+ servers for authentication.

Example: The following example configures the http authentication.

```
(UBNT EdgeSwitch)(config)# ip http authentication radius local
```

no ip http authentication

Use this command to return to the default.

Format `no ip http authentication`

Mode Global Config

ip https authentication

Use this command to specify authentication methods for https server users. The default configuration is the local user database is checked. This action has the same effect as the command `ip https authentication local`. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example, if none is specified as an authentication method after RADIUS, no authentication is used if the RADIUS server is down.

Default	local
Format	`ip https authentication method1 [method2...]`
Mode	Global Config

The following table lists the possible values for the *method* parameter.

Parameter Value	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Example: The following example configures https authentication.

```
(UBNT EdgeSwitch)(config)# ip https authentication radius local
```

no ip https authentication

Use this command to return to the default.

Format	`no ip https authentication`
Mode	Global Config

ip http server

This command enables access to the switch through the web interface. When access is enabled, the user can login to the switch from the web interface. When access is disabled, the user cannot login to the switch's web server. Disabling the web interface takes effect immediately. All interfaces are affected.

Default	enabled
Format	`ip http server`
Mode	Privileged EXEC

no ip http server

This command disables access to the switch through the web interface. When access is disabled, the user cannot login to the switch's web server.

Format	`no ip http server`
Mode	Privileged EXEC

ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Default	disabled
Format	`ip http secure-server`
Mode	Privileged EXEC

no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Format	`no ip http secure-server`
Mode	Privileged EXEC

ip http session hard-timeout

This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to reauthenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default	24
Format	`ip http session hard-timeout` *`1-168`*
Mode	Privileged EXEC

no ip http session hard-timeout

This command restores the hard timeout for un-secure HTTP sessions to the default value.

Format	`no ip http session hard-timeout`
Mode	Privileged EXEC

ip http session maxsessions

This command limits the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

Default	16
Format	`ip http session maxsessions` *`0-16`*
Mode	Privileged EXEC

no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Format	`no ip http session maxsessions`
Mode	Privileged EXEC

ip http session soft-timeout

This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to reauthenticate. This timer begins on initiation of the web session and is restarted with each access to the switch.

Default	5
Format	`ip http session soft-timeout` *`1-60`*
Mode	Privileged EXEC

no ip http session soft-timeout

This command resets the soft timeout for un-secure HTTP sessions to the default value.

Format	`no ip http session soft-timeout`
Mode	Privileged EXEC

ip http secure-session hard-timeout

This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to reauthenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

Default	24
Format	`ip http secure-session hard-timeout 1-168`
Mode	Privileged EXEC

no ip http secure-session hard-timeout

This command resets the hard timeout for secure HTTP sessions to the default value.

Format	`no ip http secure-session hard-timeout`
Mode	Privileged EXEC

ip http secure-session maxsessions

This command limits the number of secure HTTP sessions. Zero is the configurable minimum.

Default	16
Format	`ip http secure-session maxsessions 0-16`
Mode	Privileged EXEC

no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Format	`no ip http secure-session maxsessions`
Mode	Privileged EXEC

ip http secure-session soft-timeout

This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to reauthenticate. This timer begins on initiation of the web session and is restarted with each access to the switch. The secure-session soft-timeout cannot be set to zero (infinite).

Default	5
Format	`ip http secure-session soft-timeout 1-60`
Mode	Privileged EXEC

no ip http secure-session soft-timeout

This command restores the soft timeout for secure HTTP sessions to the default value.

Format	`no ip http secure-session soft-timeout`
Mode	Privileged EXEC

ip http secure-port

This command is used to set the SSL port where port can be 1025-65535 and the default is port 443.

Default	443
Format	`ip http secure-port portid`
Mode	Privileged EXEC

no ip http secure-port

This command is used to reset the SSL port to the default value.

Format `no ip http secure-port`

Mode Privileged EXEC

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default SSL3 and TLS1

Format `ip http secure-protocol [SSL3] [TLS1]`

Mode Privileged EXEC

show ip http

This command displays the http settings for the switch.

Format `show ip http`

Mode Privileged EXEC

Term	Definition
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

disconnect

Use the disconnect command to close HTTP, HTTPS, Telnet or SSH sessions. Use all to close all active sessions, or use `session-id` to specify the session ID to close. To view the possible values for `session-id`, use the `show loginsession` command.

Format	`disconnect {session_id | all}`
Mode	Privileged EXEC

show loginsession

This command displays current Telnet, SSH and serial port connections to the switch. This command displays truncated user names. Use the `show loginsession long` command to display the complete usernames.

Format	`show loginsession`
Mode	Privileged EXEC

Term	Definition
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be HTTP, HTTPS, telnet, serial, or SSH.

show loginsession long

This command displays the complete user names of the users currently logged in to the switch.

Format	`show loginsession long`
Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #show loginsession long

User Name
------------
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

User Account Commands

This section describes the commands you use to add, manage, and delete system users. The EdgeSwitch software has one default user account: ubnt. The ubnt user can view and configure system settings.



Note: You cannot delete the default read/write user account (ubnt). You can configure up to five additional user accounts on the system. Additional user accounts can be read-only or read/write.

aaa authentication login

Use this command to set authentication at login. The default and optional list names created with the command are used with the `aaa authentication login` command. Create a list by entering the `aaa authentication login list-name method` command, where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify none as the fInal method in the command line. For example, if none is specified as an authentication method after RADIUS, no authentication is used if the RADIUS server is down.

Default	`networkList`. Used by telnet and SSH and only contains the method local.
Format	`aaa authentication login {default | list-name} method1 [method2...]`
Mode	Global Config

Parameter	Definition
`default`	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
`list-name`	Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.
`method1 [method2...]`	At least one from the following: • `enable` Uses the enable password for authentication. • `local` Uses the local username database for authentication. • `none` Uses no authentication. • `radius` Uses the list of all RADIUS servers for authentication. • `tacacs` Uses the list of all TACACS servers for authentication.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch)(config)# aaa authentication login default radius local enable none
```

no aaa authentication login

This command returns to the default.

Format	`aaa authentication login {default | list-name}`
Mode	Global Config

aaa authentication enable

Use this command to set authentication for accessing higher privilege levels. The default enable list is `enableList`. It is used by console, telnet and SSH, and contains the method as `enable` followed by `none`.

The default and optional list names created with the `aaa authentication enable` command are used with the `enable authentication` command. Create a list by entering the `aaa authentication enable list-name method` command where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries in the given sequence.

The user manager returns ERROR (not PASS or FAIL) for enable and line methods if no password is configured, and moves to the next configured method in the authentication list. The method none reflects that there is no authentication needed.

The user will only be prompted for an enable password if one is required. The following authentication methods do not require passwords:

- none
- deny
- enable (if no enable password is configured)
- line (if no line password is configured)

Example: See the examples below.

a. `aaa authentication enable default enable none`
b. `aaa authentication enable default line none`
c. `aaa authentication enable default enable radius none`
d. `aaa authentication enable default line tacacs none`

Examples a and b do not prompt for a password, however because examples c and d contain the RADIUS and TACACS methods, the password prompt is displayed.

If the login methods include only enable, and there is no enable password configured, then the EdgeSwitch software does not prompt for a username. In such cases, the EdgeSwitch software only prompts for a password. the EdgeSwitch software supports configuring methods after the local method in authentication and authorization lists. If the user is not present in the local database, then the next configured method is tried.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

Use the command **"show authorization methods" on page 57** to display information about the authentication methods.



Note: Requests sent by the switch to a RADIUS server include the username `$enabx$,` where `x` is the requested privilege level. For enable to be authenticated on RADIUS servers, add `$enabx$` users to them. The login user ID is now sent to TACACS+ servers for enable authentication.

Default	default
Format	`aaa authentication enable {default | list-name} method1 [method2...]`
Mode	Global Config

Parameter	Definition
`default`	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
`list-name`	Character string (15 characters max.) used to name the list of authentication methods activated when a user logs in.
`method1` `[`*`method2...`*`]`	Specify at least one from the following: • `deny` Used to deny access. • `enable` Uses the enable password for authentication. • `line` Uses the line password for authentication. • `none` Uses no authentication. • `radius` Uses the list of all RADIUS servers for authentication. • `tacacs` Uses the list of all TACACS servers for authentication.

Example: The following example sets authentication when accessing higher privilege levels.

```
(UBNT EdgeSwitch)(config)# aaa authentication enable default enable
```

no aaa authentication enable

Use this command to return to the default configuration.

Format	`no aaa authentication enable {default | list-name}`
Mode	Global Config

aaa authorization

Use this command to configure command and exec authorization method lists. This list is identified by `default` or a user-specified `list-name`. If `tacacs` is specified as the authorization method, authorization commands are notified to a TACACS+ server. If `none` is specified as the authorization method, command authorization is not applicable. A maximum of five authorization method lists can be created for the `commands` type.



Note: Local method is not supported for command authorization. Command authorization with RADIUS will work if, and only if, the applied authentication method is also RADIUS.

Format	`aaa authorization {commands|exec} {default|list-name} method1[method2]`
Mode	Global Config

Parameter	Description
`commands`	Provides authorization for all user-executed commands.
`exec`	Provides exec authorization.
`default`	The default list of methods for authorization services.
`list-name`	Alphanumeric character string used to name the list of authorization methods.
`method1` `[`*`method2...`*`]`	TACACS+/RADIUS/Local and none are supported.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#aaa authorization exec default  tacacs+ none
(UBNT EdgeSwitch) (Config)#aaa authorization commands default tacacs+ none
```

show authorization methods

This command displays the configured authorization method lists.

Format	`show authorization methods`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show authorization methods

Command Authorization List           Method
-------------------------- -------------------------------------
dfltCmdAuthList                      tacacs         none
list2                                none           undefined
list4                                tacacs         undefined

Line            Command Method List
------------ ------------------------------
Telnet          dfltCmdAuthList
SSH             dfltCmdAuthList

Exec Authorization List       Method
----------------------   -------------------------------------
dfltExecAuthList                     tacacs         none
list2                                none           undefined
list4                                tacacs         undefined

Line           Exec Method List
------------ ------------------------------
Telnet          dfltExecAuthList
SSH             dfltExecAuthList
```

enable authentication

Use this command to specify the authentication method list when accessing a higher privilege level from a remote telnet.

Format `enable authentication {default | list-name}`

Mode Line Config

Parameter	Description
`default`	Uses the default list created with the aaa authentication enable command.
`list-name`	Uses the indicated list created with the aaa authentication enable command.

Example: The following example specifies the default authentication method when accessing a higher privilege level telnet.

```
(UBNT EdgeSwitch) (config)#line telnet
(UBNT EdgeSwitch) (config-telnet)#enable authentication default
```

no enable authentication

Use this command to return to the default specified by the `enable authentication` command.

Format `no enable authentication`

Mode Line Config

username (Global Config)

Use the `username` command in Global Config mode to add a new user to the local user database. The default privilege level is 1. Using the `encrypted` keyword allows the administrator to transfer local user passwords between devices without having to know the passwords. When the `password` parameter is used along with `encrypted` parameter, the password must be exactly 128 hexadecimal characters in length. If the password strength feature is enabled, this command checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. Giving the optional parameter `override-complexity-check` disables the validation of the password strength.

Format `username` *`name`* `{password` *`password`* `[encrypted [override-complexity-check] | level` *`level`* `[encrypted [override-complexity-check]] | override-complexity-check]} | {level` *`level`* `[override-complexity-check] password}`

Mode Global Config

Parameter	Description
`name`	The name of the user. Range: 1-64 characters.
`password`	The authentication password for the user. Range 8-64 characters. This value can be zero if the `no passwords min-length` command has been executed. The special characters allowed in the password include: ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
`level`	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15. Enter access level 1 for Read Access or 15 for Read/Write Access. If not specified where it is optional, the privilege level is 1.
`encrypted`	Encrypted password entered, copied from another switch configuration.
`override-complexity-check`	Disables the validation of the password strength.

Example: The following example configures user *bob* with password *xxxyyymmmm* and user level *15*.

```
(UBNT EdgeSwitch)(config)# username bob password xxxyyymmmm level 15
```

Example: The following example configures user *test* with password *testPassword* and assigns a user level of *1* (read-only). The password strength will not be validated.

```
(UBNT EdgeSwitch)(config)# username test password testPassword level 1 override-complexity-check
```

Example: A third example.

```
(UBNT EdgeSwitch) (Config)#username test password testtest
```

Example: A fourth example.

```
(UBNT EdgeSwitch) (Config)# username test password e8d63677741431114f9e39a853a15e8fd35ad059e2e1b
49816c243d7e08152b052eafbf23b528d348cdba1b1b7ab91be842278e5e970dbfc62d16dcd13c0b864 level 1 encr
ypted override-complexity-check

(UBNT EdgeSwitch) (Config)#  username test level 15 password

Enter new password:********

Confirm new password:********
```

Example: A fifth example.

```
(UBNT EdgeSwitch) (Config)# username test level 15 override-complexity-check  password

Enter new password:********

Confirm new password:********
```

no username

Use this command to remove a user name.

Format	`no username` *`name`*
Mode	Global Config

username name nopassword

Use this command to remove an existing user's password (NULL password).

Format	`username` *`name`* `nopassword [level` *`level`*`]`
Mode	Global Config

Parameter	Description
`name`	The name of the user. Range: 1-32 characters.
password	The authentication password for the user. Range 8-64 characters.
`level`	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15.

username name unlock

Use this command to allow a locked user account to be unlocked. Only a user with read/write access can reactivate a locked user account.

Format	`username` *`name`* `unlock`
Mode	Global Config

show users

This command displays the configured user names and their settings. The `show users` command displays truncated user names. Use the `show users long` command to display the complete user names. The `show users` command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format `show users`

Mode Privileged EXEC

Term	Definition
User Name	The name the user enters to login using the serial port, telnet or web.
Access Mode	Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the "ubnt" user has Read/Write access.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and web access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users long

This command displays the complete usernames of the configured users on the switch.

Format `show users long`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #show users long
User Name
------------
ubnt
test1111test1111test1111test1111
```

show users accounts

This command displays local user status with respect to user account lockout and password aging. Displayed user names are truncated. Use the `show users long` command to show the complete user names.

Format `show users accounts [detail]`

Mode Privileged EXEC

Term	Definition
User Name	The local user account's user name.
Access Level	The user's access level (1 for read-only or 15 for read/write).
Password Aging	Number of days, since the password was configured, until the password expires.
Password Expiry Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).

If the `detail` keyword is included, the following additional fields are displayed.

Term	Definition
Override Complexity Check	Displays the user's Password override complexity check status. By default it is disabled.
Password Strength	Displays the user password's strength (Strong or Weak). This field is displayed only if the Password Strength feature is enabled.

Example: The following example displays information about the local user database.

```
(UBNT EdgeSwitch)#show users accounts

UserName            Privilege Password Password     Lockout
                              Aging    Expiry date
------------------- --------- -------- ------------ -------
ubnt                15        ---      ---          False

(UBNT EdgeSwitch) #show users accounts detail

UserName..................................... admin
Privilege.................................... 15
Password Aging............................... ---
Password Expiry.............................. ---
Lockout...................................... False
Override Complexity Check.................... Disable
Password Strength............................ ---
```

show users login-history [long]

Use this command to display information about the login history of users.

Format	`show users login-history [long]`
Mode	Privileged EXEC

show users login-history [username]

Use this command to display information about the login history of users.

Format	`show users login-history [username` *`name`*`]`
Mode	Privileged EXEC

Parameter	Description
`name`	Name of the user. Range: 1-20 characters.

Example: The following example shows user login history outputs.

```
(UBNT EdgeSwitch) #show users login-history
Login Time            Username  Protocol  Location
--------------------  --------- --------- ---------------
Jan 19 2005 08:23:48  Bob       Serial
Jan 19 2005 08:29:29  Robert    HTTP      172.16.0.8
Jan 19 2005 08:42:31  John      SSH       172.16.0.1
Jan 19 2005 08:49:52  Betty     Telnet    172.16.1.7
```

login authentication

Use this command to specify the login authentication method list for a line (console, telnet or SSH). The default configuration uses the default set with the command `aaa authentication login`.

Format	`login authentication {default |` *`list-name`*`}`
Mode	Line Configuration

Parameter	Definition
`default`	Uses the default list created with the aaa authentication login command.
`list-name`	Uses the indicated list created with the aaa authentication login command.

Example: The following example specifies the default authentication method for telnet.

```
(UBNT EdgeSwitch) (config)#line telnet
(UBNT EdgeSwitch) (config-telnet)#login authentication default
```

no login authentication

Use this command to return to the default specified by the authentication login command.

password

This command allows the currently logged in user to change his or her password without having read/write privileges.

Format	`password`
Mode	User EXEC

Example: The following is an example of the command.

```
(UBNT EdgeSwitch) #password

Enter old password:********

Enter new password:********

Confirm new password:********
```

password (Line Configuration)

Use the password command in Line Configuration mode to specify a password on a line. The default configuration is no password is specified.

Format	`password [`*`password`* `[encrypted]]`
Mode	Line Config

Parameter	Definition
`password`	Password for this level. Range: 8-64 characters
`encrypted`	Encrypted password to be entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

Example: The following example specifies a password `mcmxxyyy` on a line.

```
(UBNT EdgeSwitch)(config-line)# password mcmxxyyy
```

Example: The following is another example of the command.

```
(UBNT EdgeSwitch)(Config-line)# password testtest

(UBNT EdgeSwitch) (Config-line)# password e8d63677741431114f9e39a853a15e8fd35ad059e2 e1b49816c24
3d7e08152b052eafbf23b528d348cdba1b1b7ab91be842278e5e970dbfc62d16dcd13c0b864 encrypted

(UBNT EdgeSwitch) (Config-line)# password

Enter new password:********

Confirm new password:********
```

no password (Line Configuration)

Use this command to remove the password on a line.

Format	`no password`
Mode	Line Config

password (User EXEC)

Use this command to allow a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

Format	`password`
Mode	User EXEC

Example: The following example shows the prompt sequence for executing the `password` command.

```
(UBNT EdgeSwitch)>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

password (aaa IAS User Config)

This command is used to configure a password for a user. An optional parameter [`encrypted`] is provided to indicate that the password given to the command is already preencrypted.

Format	`password` *`password`* `[encrypted]`
Mode	aaa IAS User Config

no password (aaa IAS User Config)

This command is used to clear the password of a user.

Format	`no password`
Mode	aaa IAS User Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#aaa ias-user username client-1
(UBNT EdgeSwitch) (Config-aaa-ias-User)#password client123
(UBNT EdgeSwitch) (Config-aaa-ias-User)#no password
```

Example: The following is an example of adding a MAB Client to the Internal user database.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#aaa ias-user username 1f3ccb1157
(UBNT EdgeSwitch) (Config-aaa-ias-User)#password 1f3ccb1157
(UBNT EdgeSwitch) (Config-aaa-ias-User)#exit
(UBNT EdgeSwitch) (Config)#
```

enable password (Privileged EXEC)

Use the `enable password` configuration command to set a local password to control access to the privileged EXEC mode.

Format	`enable password [`*`password`* `[encrypted]]`
Mode	Privileged EXEC

Parameter	Definition
`password`	Password string. Range: 8-64 characters.
`encrypted`	Encrypted password you entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #enable password testtest

(UBNT EdgeSwitch) #enable password e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e0815
2b052eafbf23b528d348cdba1b1b7ab91be842278e5e970dbfc62d16dcd13c0b864 encrypted

(UBNT EdgeSwitch) #enable password

Enter old password:********

Enter new password:********

Confirm new password:********
```

no enable password (Privileged EXEC)

Use the `no enable` password command to remove the password requirement.

Format	`no enable password`
Mode	Privileged EXEC

passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 8-64.

Default	8
Format	`passwords min-length` *`8-64`*
Mode	Global Config

no passwords min-length

Use this command to set the minimum password length to the default value.

Format	`no passwords min-length`
Mode	Global Config

passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don't reuse their passwords often. The valid range is 0-10.

Default	0
Format	`passwords history` *`0-10`*
Mode	Global Config

no passwords history

Use this command to set the password history to the default value.

Format	`no passwords history`
Mode	Global Config

passwords aging

Use this command to implement aging on passwords for local users. When a user's password expires, the user is prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

Default	0
Format	`passwords aging` *`1-365`*
Mode	Global Config

no passwords aging

Use this command to set the password aging to the default value.

Format	`no passwords aging`
Mode	Global Config

passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can reactivate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

Default	0
Format	`passwords lock-out` *`1-5`*
Mode	Global Config

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format	`no passwords lock-out`
Mode	Global Config

passwords strength-check

Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Default	Disable
Format	`passwords strength-check`
Mode	Global Config

no passwords strength-check

Use this command to set the password strength checking to the default value.

Format	`no passwords strength-check`
Mode	Global Config

passwords strength maximum consecutive-characters

Use this command to set the maximum number of consecutive characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default	0
Format	`passwords strength maximum consecutive-characters` *`0-15`*
Mode	Global Config

passwords strength maximum repeated-characters

Use this command to set the maximum number of repeated characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default	0
Format	`passwords strength maximum repeated-characters` *`0-15`*
Mode	Global Config

passwords strength minimum uppercase-letters

Use this command to enforce a minimum number of uppercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum uppercase-letters`
Mode	Global Config

no passwords strength minimum uppercase-letters

Use this command to reset the minimum uppercase letters required in a password to the default value.

Format	`no passwords strength minimum uppercase-letters`
Mode	Global Config

passwords strength minimum lowercase-letters

Use this command to enforce a minimum number of lowercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum lowercase-letters`
Mode	Global Config

no passwords strength minimum lowercase-letters

Use this command to reset the minimum lower letters required in a password to the default value.

Format	`no passwords strength minimum lowercase-letters`
Mode	Global Config

passwords strength minimum numeric-characters

Use this command to enforce a minimum number of numeric characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum numeric-characters`
Mode	Global Config

no passwords strength minimum numeric-characters

Use this command to reset the minimum numeric characters required in a password to the default value.

Format	`no passwords strength minimum numeric-characters`
Mode	Global Config

passwords strength minimum special-characters

Use this command to enforce a minimum number of special characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum special-characters`
Mode	Global Config

no passwords strength minimum special-characters

Use this command to reset the minimum special characters required in a password to the default value.

Format	`no passwords strength minimum special-characters`
Mode	Global Config

passwords strength minimum character-classes

Use this command to enforce a minimum number of characters classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The valid range is 0-4. The default is 4.

Default 4

Format `passwords strength minimum character-classes`

Mode Global Config

no passwords strength minimum character-classes

Use this command to reset the minimum number of character classes required in a password to the default value.

Format `no passwords strength minimum character-classes`

Mode Global Config

passwords strength exclude-keyword

Use this command to exclude the specified *keyword* while configuring the password. The password does not accept the keyword in any form (in between the string, case insensitive and reverse) as a substring. You can configure up to a maximum of 3 keywords.

Format `passwords strength exclude-keyword keyword`

Mode Global Config

no passwords strength exclude-keyword

Use this command to reset the restriction for the specified keyword or all the keywords configured.

Format `no passwords strength exclude-keyword [keyword]`

Mode Global Config

show passwords configuration

Use this command to display the configured password management settings.

Format `show passwords configuration`

Mode Privileged EXEC

Term	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required in a password.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required in a password.
Minimum Password Numeric Characters	Minimum number of numeric characters required in a password.
Maximum Password Consecutive Characters	Maximum number of consecutive characters allowed in a password.
Maximum Password Repeated Characters	Maximum number of repeated characters allowed in a password.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

show passwords result

Use this command to display the last password set result information.

Format `show passwords result`

Mode Privileged EXEC

Term	Definition
Last User Whose Password Is Set	Shows the name of the user with the most recently set password.
Password Strength Check	Shows whether password strength checking is enabled.
Last Password Set Result	Shows if the attempt to set a password succeeded; if not, the reason for the failure is included.

write memory

Use this command to save running configuration changes to NVRAM so that changes will persist across a reboot. This command is the same as `copy system:running-config nvram:startup-config`. Use the `confirm` keyword to directly save the configuration to NVRAM without prompting for confirmation.

Format `write memory [confirm]`

Mode Privileged EXEC

aaa ias-user username

The Internal Authentication Server (IAS) database is a dedicated internal database used for local authentication of users for network access through the IEEE 802.1X feature. Use the `aaa ias-user username` command in Global Config mode to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format aaa ias-user username user

Mode Global Config

no aaa ias-user username

Use this command to remove the specified user from the internal user database.

Format no aaa ias-user username user

Mode Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#aaa ias-user username client-1
(UBNT EdgeSwitch) (Config-aaa-ias-User)#exit
(UBNT EdgeSwitch) (Config)#no aaa ias-user username client-1
(UBNT EdgeSwitch) (Config)#
```

aaa session-id

Use this command in Global Config mode to specify if the same session-id is used for Authentication, Authorization and Accounting service type within a session.

Default common

Format `aaa session-id [common | unique]`

Mode Global Config

Parameter	Definition
`common`	Use the same session-id for all AAA Service types.
`unique`	Use a unique session-id for all AAA Service types.

no aaa session-id

Use this command in Global Config mode to reset the aaa session-id behavior to the default.

Format	`no aaa session-id [unique]`
Mode	Global Config

aaa accounting

Use this command in Global Config mode to create an accounting method list for user EXEC sessions, user-executed commands, or 802.1X. This list is identified by `default` or a user-specified *`list_name`*. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (`start-stop`) or only at the end (`stop-only`). If `none` is specified, then accounting is disabled for the specified list. If `tacacs` is specified as the accounting method, accounting records are notified to a TACACS+ server. If `radius` is the specified accounting method, accounting records are notified to a RADIUS server.



Note: Please note the following:

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- Only the default Accounting Method list can be created for 802.1X. There is no provision to create more.
- The same list-name can be used for both exec and commands accounting type
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Start-stop or None are the only supported record types for 802.1X accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for 802.1X accounting.

Format	`aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stop-only |none} method1 [method2...]`
Mode	Global Config

Parameter	Definition
`exec`	Provides accounting for a user EXEC terminal sessions.
`commands`	Provides accounting for all user executed commands.
`dot1x`	Provides accounting for 802.1X user commands.
`default`	The default list of methods for accounting services.
`list-name`	Character string used to name the list of accounting methods.
`start-stop`	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the beginning of a process and a stop accounting notice at the end of a process.
`stop-only`	Sends a stop accounting notice at the end of the requested user process.
`none`	Disables accounting services on this line.
`method`	Use either `tacacs` or `radius` server for accounting purposes.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) #aaa accounting commands default stop-only tacacs
(UBNT EdgeSwitch) #aaa accounting exec default start-stop radius
(UBNT EdgeSwitch) #aaa accounting dot1x default start-stop radius
(UBNT EdgeSwitch) #aaa accounting dot1x default none
(UBNT EdgeSwitch) #exit
```

For the same set of accounting type and list name, the administrator can change the record type, or the methods list, without having to first delete the previous configuration.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) #aaa accounting exec ExecList stop-only tacacs
(UBNT EdgeSwitch) #aaa accounting exec ExecList start-stop tacacs
(UBNT EdgeSwitch) #aaa accounting exec ExecList start-stop tacacs radius
```

The first `aaa` command creates a method list for exec sessions with the name `ExecList`, with `record-type` as `stop-only` and the `method` as `tacacs` (TACACS+). The second command changes the `record-type` to `start-stop` from `stop-only` for the same method list. The third command, for the same list changes the methods list to `{tacacs, radius}` from `{tacacs}`.

no aaa accounting

This command deletes the accounting method list.

Default	none
Format	`no aaa accounting {exec | commands | dot1x} {default | list_name default}`
Mode	Global Config

The following shows an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) #aaa accounting commands userCmdAudit stop-only tacacs radius
(UBNT EdgeSwitch) #no aaa accounting commands userCmdAudit
(UBNT EdgeSwitch) #exit
```

password (AAA IAS User Configuration)

Use this command to specify a password for a user in the IAS database. An optional parameter encrypted is provided to indicate that the password given to the command is already preencrypted.

Format	`password` *`password`* `[encrypted]`
Mode	AAA IAS User Config

Parameter	Definition
`password`	Password for this level. Range: 8-64 characters
`encrypted`	Encrypted password to be entered, copied from another switch configuration.

no password (AAA IAS User Configuration)

Use this command to clear the password of a user.

Format	`no password`
Mode	AAA IAS User Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#aaa ias-user username client-1
(UBNT EdgeSwitch) (Config-aaa-ias-User)#password client123
(UBNT EdgeSwitch) (Config-aaa-ias-User)#no password
```

Example: The following is an example of adding a MAB Client to the Internal user database.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#aaa ias-user username 1f3ccb1157
(UBNT EdgeSwitch) (Config-aaa-ias-User)#password 1f3ccb1157
(UBNT EdgeSwitch) (Config-aaa-ias-User)#exit
```

clear aaa ias-users

Use this command to remove all users from the IAS database.

Format	`clear aaa ias-users`
Mode	Privileged Exec

The following is an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #clear aaa ias-users
(UBNT EdgeSwitch) #
```

show aaa ias-users

Use this command to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Format	`show aaa ias-users [username]`
Mode	Privileged EXEC

Example: The following is an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #show aaa ias-users

UserName
------------------
Client-1
Client-2
```

Example: Following are the IAS configuration commands shown in the output of `show running-config` command. Passwords shown in the command output are always encrypted.

```
aaa ias-user username client-1
password a45c74fdf50a558a2b5cf05573cd633bac2c6c598d54497ad4c46104918f2c encrypted
exit
```

accounting

Use this command in Line Configuration mode to apply the accounting method list to a line config (telnet/ssh).

Format	`accounting {exec | commands } {default | listname}`
Mode	Line Configuration

Parameter	Definition
`exec`	Causes accounting for an EXEC session.
`commands`	This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out.
`default`	The default Accounting List.
`listname`	Enter a string of not more than 15 characters.

Example: The following is a example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#line telnet
(UBNT EdgeSwitch)(Config-line)# accounting exec default
(UBNT EdgeSwitch) #exit
```

no accounting

Use this command to remove accounting from a Line Configuration mode.

Format	`no accounting {exec|commands]`
Mode	Line Configuration

show accounting

Use this command to display ordered methods for accounting lists.

Format	`show accounting`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show accounting
Number of Accounting Notifications sent at beginning of an EXEC session:                0
Errors when sending Accounting Notifications beginning of an EXEC session:              0
Number of Accounting Notifications at end of an EXEC session:                          0
Errors when sending Accounting Notifications at end of an EXEC session:                0
Number of Accounting Notifications sent at beginning of a command execution:           0
Errors when sending Accounting Notifications at beginning of a command execution:      0
Number of Accounting Notifications sent at end of a command execution:                 0
Errors when sending Accounting Notifications at end of a command execution:            0
```

show accounting methods

Use this command to display configured accounting method lists.

Format	`show accounting methods`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #show accounting methods

Acct Type       Method Name     Record Type    Method Type
----------     ------------    ------------   ------------
Exec           dfltExecList      start-stop     TACACS
Commands       dfltCmdsList      stop-only      TACACS
Commands       UserCmd Audit     start-stop     TACACS
DOT1X          dfltDot1xList     start-stop     radius

Line     EXEC Method List    Command Method List
------  ------------------------------------
Telnet   dfltExecList          dfltCmdsList
SSH      dfltExecList          UserCmdAudit
```

clear accounting statistics

This command clears the accounting statistics.

Format	`clear accounting statistics`
Mode	Privileged EXEC

SNMP Commands

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The parameters *name*, *loc*, and *con* can be up to 255 characters in length.

Default none

Format `snmp-server {sysname name | location loc | contact con}`

Mode Global Config

snmp-server community

This command adds (and names) a new SNMP community, and optionally sets the access mode, allowed IP address, and create a view for the community.



Note: Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default
- Public and private, which you can rename.
- Default values for the remaining four community names are blank.

Format `snmp-server community community-name [{ro | rw |su }] [ipaddress ip-address] [view view-name]`

Mode Global Config

Parameter	Definition
community-name	A name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of community-name can be up to 16 case-sensitive characters.
ro | rw | su	The access mode of the SNMP community, which can be public (Read-Only/RO), private (Read-Write/RW), or Super User (SU).
ip-address	The associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses.
view-name	The name of the view to create or update.

no snmp-server community

This command removes this community name from the table. The name is the community name to be deleted.

Format `no snmp-server community community-name`

Mode Global Config

snmp-server community-group

This command configures a community access string to permit access via the SNMPv1 and SNMPv2 protocols.

Format `snmp-server community-group community-string group-name [ipaddress ipaddress]`

Mode Global Config

Parameter	Definition
community-string	The community which is created and then associated with the group. The range is 1 to 20 characters.
group-name	The name of the group that the community is associated with. The range is 1 to 30 characters.
ipaddress	Optionally, the IPv4 address that the community may be accessed from.

snmp-server enable traps violation

The Port MAC locking component interprets this command and configures violation action to send an SNMP trap with default trap frequency of 30 seconds. The Global command configures the trap violation mode across all interfaces valid for port-security (for other port security commands, see **"Port Security Commands" on page 290**). There is no global trap mode as such.

Default	disabled
Format	`snmp-server enable traps violation`
Mode	• Global Config • Interface Config

no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format	`no snmp-server enable traps violation`
Mode	Interface Config

snmp-server enable traps

This command enables the Authentication Flag.

Default	enabled
Format	`snmp-server enable traps`
Mode	Global Config

no snmp-server enable traps

This command disables the Authentication Flag.

Format	`no snmp-server enable traps`
Mode	Global Config

snmp trap link-status

This command enables link status traps on an interface or range of interfaces.



Note: This command is valid only when the Link Up/Down Flag is enabled.

Format	`snmp trap link-status`
Mode	Interface Config

no snmp trap link-status

This command disables link status traps by interface.



Note: This command is valid only when the Link Up/Down Flag is enabled.

Format	`no snmp trap link-status`
Mode	Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.



Note: This command is valid only when the Link Up/Down Flag is enabled.

Format	`snmp trap link-status all`
Mode	Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

 Note: This command is valid only when the Link Up/Down Flag is enabled.

Format	`no snmp trap link-status all`
Mode	Global Config

snmp-server enable traps linkmode

 Note: This command may not be available on all platforms.

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See **"show snmp" on page 80**.

Default	enabled
Format	`snmp-server enable traps linkmode`
Mode	Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format	`no snmp-server enable traps linkmode`
Mode	Global Config

snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default	enabled
Format	`snmp-server enable traps multiusers`
Mode	Global Config

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format	`no snmp-server enable traps multiusers`
Mode	Global Config

snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default	enabled
Format	`snmp-server enable traps stpmode`
Mode	Global Config

no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format	`no snmp-server enable traps stpmode`
Mode	Global Config

snmp-server engineID local

This command configures the SNMP engine ID on the local device.

Default The engineID is configured automatically, based on the device MAC address.

Format `snmp-server engineID local {engineid-string|default}`

Mode Global Config

Parameter	Definition
engineid-string	A hexadecimal string identifying the engine ID, used for localizing configuration. The engine ID must be an even length in the range of 6 to 32 hexadecimal characters.
default	Sets the engine ID to the default string, based on the device MAC address.

⚠ **CAUTION:** Changing the engine ID will invalidate all SNMP configuration that exists on the box.

no snmp-server engineID local

This command removes the specified engine ID.

Default The engineID is configured automatically, based on the device MAC address.

Format `no snmp-server engineID local`

Mode Global Config

snmp-server filter

This command creates a filter entry for use in limiting which traps will be sent to a host.

Default No filters are created by default.

Format `snmp-server filter filtername oid-tree {included|excluded}`

Mode Global Config

Parameter	Definition
filtername	The label for the filter being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the filter. Subtrees may be specified numerically (1.3.6.2.4) or by keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
included	The tree is included in the filter.
excluded	The tree is excluded from the filter.

no snmp-server filter

This command removes the specified filter.

Default No filters are created by default.

Format `snmp-server filter filtername [oid-tree]`

Mode Global Config

snmp-server group

This command creates an SNMP access group.

Default Generic groups are created for all versions and privileges using the default views.

Format `snmp-server group group-name {v1 | v2 | v3 {noauth | auth | priv}} [context context-name] [read read-view] [write write-view] [notify notify-view]`

Mode Global Config

Parameter	Definition
group-name	The group name to be used when configuring communities or users. The range is 1 to 30 characters.
v1	This group can only access via SNMPv1.
v2	This group can only access via SNMPv2.
v3	This group can only access via SNMPv3.
noauth	This group can be accessed only when not using Authentication or Encryption. Applicable only if SNMPv3 is selected.
auth	This group can be accessed only when using Authentication but not Encryption. Applicable only if SNMPv3 is selected.
priv	This group can be accessed only when using both Authentication and Encryption. Applicable only if SNMPv3 is selected.
context-name	The SNMPv3 context used during access. Applicable only if SNMPv3 is selected.
read-view	The view this group will use during GET requests. The range is 1 to 30 characters.
write-view	The view this group will use during SET requests. The range is 1 to 30 characters.
notify-view	The view this group will use when sending out traps. The range is 1 to 30 characters.

no snmp-server group

This command removes the specified group.

Format `no snmp-server group group-name {v1|v2 | 3 {noauth|auth|priv}} [context context-name]`

Mode Global Config

snmp-server host

This command configures traps to be sent to the specified host.

Default No default hosts are configured.

Format `snmp-server host host-addr {informs [timeout seconds] [retries retries] | traps version {1|2}} community-string [udp-port port] [filter filter-name]`

Mode Global Config

Parameter	Definition
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
informs	Send SNMPv2 informs to the host.
seconds	The number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	The number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
traps	Send SNMP traps to the host. This option is selected by default.
version 1	Sends SNMPv1 traps. This option is not available if informs is selected.
version 2	Sends SNMPv2 traps. This option is not available if informs is selected. This option is selected by default.
community-string	Community string sent as part of the notification. The range is 1 to 20 characters.
port	The SNMP Trap receiver port. The default is port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

no snmp-server host

This command removes the specified host entry.

Format `no snmp-server host host-addr [traps|informs]`

Mode Global Config

snmp-server user

This command creates an SNMPv3 user for access to the system.

Default No default users are created.

Format `snmp-server user username groupname [remote engineid-string] [ {auth-md5 password | auth-sha password | auth-md5-key md5-key | auth-sha-key sha-key} [priv-des password | priv-des-key des-key]`

Mode Global Config

Parameter	Definition
username	The username the SNMPv3 user will connect to the switch as. The range is 1 to 30 characters.
groupname	The name of the group the user belongs to. The range is 1 to 30 characters.
engineid-string	The engine-id of the remote management station that this user will be connecting from. The range is 5 to 32 characters.
password	The password the user will use for the authentication or encryption mechanism. The range is 1 to 32 characters.
md5-key	A pregenerated MD5 authentication key. The length is 32 characters.
sha-key	A pregenerated SHA authentication key. The length is 48 characters.
des-key	A pregenerated DES encryption key. The length is 32 characters if MD5 is selected, 48 characters if SHA is selected.

no snmp-server user

This command removes the specified SNMPv3 user.

Format `no snmp-server user username`

Mode Global Config

snmp-server view

This command creates or modifies an existing view entry that is used by groups to determine which objects can be accessed by a community or user.

Default Views are created by default to provide access to the default groups.

Format `snmp-server viewname oid-tree {included|excluded}`

Mode Global Config

Parameter	Definition
viewname	The label for the view being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the view. Subtrees may be specified numerically (1.3.6.2.4) or by keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
included	The tree is included in the view.
excluded	The tree is excluded from the view.

no snmp-server view

This command removes the specified view.

Format `no snmp-server view viewname [oid-tree]`

Mode Global Config

snmp-server v3-host

This command configures traps to be sent to the specified host.

Default No default hosts are configured.

Format `snmp-server v3-host host-addr username [traps | informs [timeout seconds] [retries retries]] [auth | noauth | priv] [udpport port] [filter filter-name]`

Mode Global Config

Parameter	Definition
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
username	User used to send a Trap or Inform message. This user must be associated with a group that supports the version and access method. The range is 1 to 30 characters.
traps	Send SNMP traps to the host. This is the default option.
informs	Send SNMP informs to the host.
seconds	Number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	Number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
auth	Enables authentication but not encryption.
noauth	No authentication or encryption. This is the default.
priv	Enables authentication and encryption.
port	The SNMP Trap receiver port. This value defaults to port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

snmptrap source-interface

Use this command in Global Configuration mode to configure the global source-interface (Source IP address) for all SNMP communication between the SNMP client and the server.

Format `snmptrap source-interface {slot/port | vlan vlan-id}`

Mode Global Configuration

Parameter	Definition
slot/port	The unit identifier assigned to the switch.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

no snmptrap source-interface

Use this command in Global Configuration mode to remove the global source-interface (Source IP selection) for all SNMP communication between the SNMP client and the server.

Format `no snmptrap source-interface`

Mode Global Configuration

show snmp

This command displays the current SNMP configuration.

Format `show snmp`

Mode Privileged EXEC

Term	Definition
Community Table:	
Community-String	The community string for the entry. This is used by SNMPv1 and SNMPv2 protocols to access the switch.
Community-Access	The type of access the community has: • Read only • Read write • su
View Name	The view this community has access to.
IP Address	Access to this community is limited to this IP address.
Community Group Table:	
Community-String	The community this maping configures
Group Name	The group this community is assigned to.
IP Address	The IP address this community is limited to.
Host Table:	
Target Address	The address of the host that traps will be sent to.
Type	The type of message that will be sent, either traps or informs.
Community	The community traps will be sent to.
Version	The version of SNMP the trap will be sent as.
UDP Port	The UDP port the trap or inform will be sent to.
Filter name	The filter the traps will be limited by for this host.
TO Sec	The number of seconds before informs will time out when sending to this host.
Retries	The number of times informs will be sent after timing out.

show snmp engineID

This command displays the currently configured SNMP engineID.

Format `show snmp engineID`

Mode Privileged EXEC

Term	Definition
Local SNMP EnginID	The current configuration of the displayed SNMP engineID.

show snmp filters

This command displays the configured filters used when sending traps.

Format `show snmp filters [filtername]`

Mode Privileged EXEC

Term	Definition
Name	The filter name for this entry.
OID Tree	The OID tree this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID Tree.

show snmp group

This command displays the configured groups.

Format `show snmp group [groupname]`

Mode Privileged EXEC

Term	Definition
Name	The name of the group.
Security Model	Indicates which protocol can access the system via this group.
Security Level	Indicates the security level allowed for this group.
Read View	The view this group provides read access to.
Write View	The view this group provides write access to.
Notify View	The view this group provides trap access to.

show snmp source-interface

Use this command in Privileged EXEC mode to display the configured global source-interface (Source IP address) details used for an SNMP client.

Format `show snmp source-interface`

Mode Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)# show snmp source-interface
SNMP trap Client Source Interface.............. (not configured)
```

show snmp user

This command displays the currently configured SNMPv3 users.

Format `show snmp user [username]`

Mode Privileged EXEC

Term	Definition
Name	The name of the user.
Group Name	The group that defines the SNMPv3 access parameters.
Auth Method	The authentication algorithm configured for this user.
Privilege Method	The encryption algorithm configured for this user.
Remote Engine ID	The engineID for the user defined on the client machine.

show snmp views

This command displays the currently configured views.

Format `show snmp views [viewname]`

Mode Privileged EXEC

Parameter	Definition
Name	The view name for this entry.
OID Tree	The OID tree that this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID tree.

show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 and OSPFv3 trapflags. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Mode Privileged EXEC

Term	Definition
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.

RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default	disable
Format	`radius accounting mode`
Mode	Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format	`no radius accounting mode`
Mode	Global Config

radius server attribute 4

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format	`radius server attribute 4 [ipaddr]`
Mode	Global Config

Parameter	Definition
`4`	NAS-IP-Address attribute to be used in RADIUS requests.
`ipaddr`	The IP address of the server.

no radius server attribute 4

The `no` version of this command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format	`no radius server attribute 4 [ipaddr]`
Mode	Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config) #radius server attribute 4  192.168.37.60
(UBNT EdgeSwitch) (Config) #radius server attribute 4
```

radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the Default_RADIUS_Auth_Server and Default_RADIUS_Acct_Server as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum of 32 authenticating and accounting servers.

If you use the `auth` parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the `no` form of the command. If you use the optional *`port`* parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The *`port`* number range is 1-65535, with a default of 1812.

Note: To reconfigure a RADIUS authentication server to use the default UDP port, set the *port* parameter to 1812.

If you use the acct parameter, the command configures the IP address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the no form of the command to remove it from the configuration. The IP address or hostname you specify must match that of a previously configured accounting server. If you use the optional *port* parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a port is already configured for the accounting server, the new port replaces the previously configured port. The *port* value must be in the range 0-65535, with a default of 1813.

Note: To reconfigure a RADIUS accounting server to use the default UDP port, set the *port* parameter to 1813.

Format	radius server host {auth | acct} {*ipaddr*|*dnsname*} [name *servername*] [port *0-65535*]
Mode	Global Config

Parameter	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
0-65535	The port number to use to connect to the specified RADIUS server.
servername	The alias name to identify the server.

no radius server host

The no form of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. If auth is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if acct is used, the previously configured RADIUS accounting server is removed from the configuration. The *ipaddr*|*dnsname* parameter must match the IP address or DNS name of the previously configured RADIUS authentication/accounting server.

Format	no radius server host {auth | acct} {*ipaddr*|*dnsname*}
Mode	Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config) #radius server host acct 192.168.37.60
(UBNT EdgeSwitch) (Config) #radius server host acct 192.168.37.60 port 1813
(UBNT EdgeSwitch) (Config) #radius server host auth 192.168.37.60 name Network1_RS port 1813
(UBNT EdgeSwitch) (Config) #radius server host acct 192.168.37.60 name Network2_RS
(UBNT EdgeSwitch) (Config) #no radius server host acct 192.168.37.60
```

radius server key

This command configures the key to be used in RADIUS client communication with the specified server. Depending on whether the auth or acct keyword is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports RADIUS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running-config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Note: The secret must be an alphanumeric value not exceeding 16 characters.

Format `radius server key {auth | acct} {ipaddr|dnsname} encrypted password`

Mode Global Config

Parameter	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
password	The password in encrypted format.

Example: The following shows an example of the CLI command.

```
radius server key acct 10.240.4.10 encrypted encrypt-string
```

radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format `radius server msgauth ipaddr|dnsname`

Mode Global Config

Parameter	Definition
ip addr	The IP address of the server.
dnsname	The DNS name of the server.

no radius server msgauth

The `no` version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format `no radius server msgauth ipaddr|dnsname`

Mode Global Config

radius server primary

This command specifies a configured server that should be the primary server in the group of servers which have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the Secondary type.

Format `radius server primary {ipaddr|dnsname}`

Mode Global Config

Parameter	Definition
ip addr	The IP address of the RADIUS Authenticating server.
dnsname	The DNS name of the server.

radius server retransmit

This command configures the RADIUS client global parameter that specifies the maximum number of message transmissions before using the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries is reached for the RADIUS accounting server and no response is received, the client does not communicate with any other server.

Default 4

Format `radius server retransmit retries`

Mode Global Config

Parameter	Definition
retries	The maximum number of transmission attempts in the range of 1 to 15.

no radius server retransmit

The `no` form of this command sets the value of this global parameter to the default value.

Format `no radius server retransmit`

Mode Global Config

radius source-interface

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (source IP address). If configured, the address of `source-interface` is used for all RADIUS communications between the RADIUS server and the RADIUS client. The selected `source-interface` IP address is used for filling the IP header of RADIUS management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a `source-interface i`s not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

Format `radius source-interface {slot/port | vlan vlan-id}`

Mode Global Config

Parameter	Definition
slot/port	The unit identifier assigned to the switch.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

no radius source-interface

Use this command to reset the RADIUS source interface to the default settings.

Format `no radius source-interface`

Mode Global Config

radius server timeout

This command configures the RADIUS client global parameter that specifies the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default 5

Format `radius server timeout seconds`

Mode Global Config

Parameter	Definition
seconds	Timeout value in seconds in the range 1–30.

no radius server timeout

The `no` version of this command sets the timeout global parameter to the default value.

Format	`no radius server timeout`
Mode	Global Config

show radius

This command displays the values configured for the global parameters of the RADIUS client.

Format	`show radius`
Mode	Privileged EXEC

Term	Definition
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show radius

        Number of Configured Authentication Servers..... 32
        Number of Configured Accounting Servers......... 32
        Number of Named Authentication Server Groups.... 15
        Number of Named Accounting Server Groups........ 3
        Number of Retransmits........................... 4
        Time Duration................................... 10
        RADIUS Accounting Mode.......................... Disable
        RADIUS Attribute 4 Mode......................... Enable
        RADIUS Attribute 4 Value ....................... 192.168.37.60
```

show radius servers

This command displays the summary and details of the RADIUS authenticating servers configured for the RADIUS client.

Format	`show radius servers [{`*`ipaddr`*`|`*`dnsname`*` | name [`*`servername`*`]}]`
Mode	Privileged EXEC

Parameter	Definition
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.

Term	Definition
Current	The * symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	Global parameter that indicates whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	Global parameter that indicates whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	Global parameter that indicates whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	Global parameter that specifies the IP address to use in NAS-IP-Address attribute used in RADIUS requests.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show radius servers

Cur  Host Address              Server Name                      Port  Type
rent
---- ------------------------ -------------------------------- ----- ----------
 *   192.168.37.200           Network1_RADIUS_Server           1813  Primary
     192.168.37.201           Network2_RADIUS_Server           1813  Secondary
     192.168.37.202           Network3_RADIUS_Server           1813  Primary
     192.168.37.203           Network4_RADIUS_Server           1813  Secondary

(UBNT EdgeSwitch) #show radius servers name

Current Host Address     Server Name                      Type
------------------------ -------------------------------- ----------
192.168.37.200           Network1_RADIUS_Server           Secondary
192.168.37.201           Network2_RADIUS_Server           Primary
192.168.37.202           Network3_RADIUS_Server           Secondary
192.168.37.203           Network4_RADIUS_Server           Primary

(UBNT EdgeSwitch) #show radius servers name Default_RADIUS_Server

Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.58
Secret Configured............................... No
Message Authenticator .......................... Enable
Number of Retransmits........................... 4
Time Duration................................... 10
RADIUS Accounting Mode.......................... Disable
RADIUS Attribute 4 Mode......................... Enable
RADIUS Attribute 4 Value ....................... 192.168.37.60

(UBNT EdgeSwitch) #show radius servers 192.168.37.58

Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.58
Secret Configured............................... No
Message Authenticator .......................... Enable
Number of Retransmits........................... 4
Time Duration................................... 10
RADIUS Accounting Mode.......................... Disable
RADIUS Attribute 4 Mode......................... Enable
RADIUS Attribute 4 Value ....................... 192.168.37.60
```

show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format `show radius accounting name [servername]`

Mode Privileged EXEC

Parameter/Term	Definition
servername	An alias name to identify the server.

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	Definition
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show radius accounting name

Host Address            Server Name                       Port     Secret
                                                                   Configured
---------------------- --------------------------------- -------- -----------
192.168.37.200          Network1_RADIUS_Server            1813     Yes
192.168.37.201          Network2_RADIUS_Server            1813     No
192.168.37.202          Network3_RADIUS_Server            1813     Yes
192.168.37.203          Network4_RADIUS_Server            1813     No

(UBNT EdgeSwitch) #show radius accounting name Default_RADIUS_Server

Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.200
RADIUS Accounting Mode.......................... Disable
Port ........................................... 1813
Secret Configured .............................. Yes
```

show radius accounting statistics

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format `show radius accounting statistics {ipaddr|dnsname | name servername}`

Mode Privileged EXEC

Parameter	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.

Term	Definition
RADIUS Accounting Server Name	The name of the accounting server.
Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0

(UBNT EdgeSwitch) #show radius accounting statistics name Default_RADIUS_Server

RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0
```

show radius source-interface

Use this command in Privileged EXEC mode to display the configured RADIUS client source-interface (Source IP address) information.

Format	`show radius source-interface`
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)# show radius source-interface
RADIUS Client Source Interface.............. (not configured)
```

show radius statistics

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format	`show radius statistics {`*`ipaddr`*`|`*`dnsname`*`	name `*`servername`*`}`
Mode	Privileged EXEC

Parameter	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.

Term	Definition
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show radius statistics 192.168.37.200

RADIUS Server Name..... Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0

(UBNT EdgeSwitch) #show radius statistics name Default_RADIUS_Server

RADIUS Server Name..... Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

tacacs-server host

Use the `tacacs-server host` command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The *`ip-address|hostname`* parameter is the IP address or hostname of the TACACS+ server. To specify multiple hosts, multiple `tacacs-server host` commands can be used.

Format	`tacacs-server host` *`ip-address|hostname`*
Mode	Global Config

no tacacs-server host

Use the `no tacacs-server host` command to delete the specified hostname or IP address. The *`ip-address|hostname`* parameter is the IP address of the TACACS+ server.

Format	`no tacacs-server host` *`ip-address|hostname`*
Mode	Global Config

tacacs-server key

Use the `tacacs-server key` command to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *`key-string`* parameter has a range of 0-128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. The `show running-config` command displays these secret keys in encrypted format. You cannot show these keys in plain text format.

Format	`tacacs-server key [`*`key-string`* `| encrypted` *`key-string`*`]`
Mode	Global Config

no tacacs-server key

Use the `no tacacs-server key` command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *`key-string`* parameter has a range of 0-128 characters. This key must match the key used on the TACACS+ daemon.

Format	`no tacacs-server key` *`key-string`*
Mode	Global Config

tacacs-server keystring

Use the `tacacs-server keystring` command to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format	`tacacs-server keystring`
Mode	Global Config

Example: The following shows an example of the CLI command.

```
(UBNT EdgeSwitch)(Config)#tacacs-server keystring
Enter tacacs key:********
Re-enter tacacs key:********
```

tacacs-server source-interface

Use this command in Global Configuration mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format	`tacacs-server source-interface {slot/port | vlan vlan-id}`
Mode	Global Config

Parameter	Definition
slot/port	The unit identifier assigned to the switch, in slot/port format.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

Example: The following shows an example of the command.

```
(Config)#tacacs-server source-interface 0/1
(Config)#no tacacs-server source-interface
```

no tacacs-server source-interface

Use this command in Global Configuration mode to remove the global source interface (Source IP selection) for all TACACS+ communications between the TACACS+ client and the server.

Format	`no tacacs-server source-interface`
Mode	Global Config

tacacs-server timeout

Use the `tacacs-server timeout` command to set the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1-30 and is the timeout value in seconds.

Default	5
Format	`tacacs-server timeout timeout`
Mode	Global Config

no tacacs-server timeout

Use the `no tacacs-server timeout` command to restore the default timeout value for all TACACS servers.

Format	`no tacacs-server timeout`
Mode	Global Config

key

Use the `key` command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon. The *`key-string`* parameter specifies the key name. For an empty string use " ". The range is 0-128 characters.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running-config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	`key [`*`key-string`* `|` `encrypted` *`key-string`*`]`
Mode	TACACS Config

keystring

Use the `keystring` command in TACACS Server Configuration mode to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format	`keystring`
Mode	TACACS Server Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch)(Config)#tacacs-server host 1.1.1.1
(UBNT EdgeSwitch)(Tacacs)#keystring

Enter tacacs key:********
Re-enter tacacs key:********
```

port

Use the `port` command in TACACS Configuration mode to specify a server port number. The server *`port-number`* range is 0 - 65535.

Default	49
Format	`port` *`port-number`*
Mode	TACACS Config

priority (TACACS Config)

Use the `priority` command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The priority parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

Default	0
Format	`priority` *`priority`*
Mode	TACACS Config

timeout

Use the `timeout` command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used. The *`timeout`* parameter has a range of 1-30 and is the timeout value in seconds.

Format	`timeout` *`timeout`*
Mode	TACACS Config

show tacacs

Use the `show tacacs` command to display the configuration, statistics, and source interface details of the TACACS+ client.

Format `show tacacs [ip-address|hostname|client|server]`

Mode Privileged EXEC

Parameter/Term	Definition
Host address	The IP address or hostname of the configured TACACS+ server.
Port	The configured TACACS+ server port number.
TimeOut	The timeout in seconds for establishing a TCP conection.
Priority	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.
client	Display SNTP client information.
server	Display SNTP server information.

show tacacs source-interface

Use the `show tacacs source-interface` command in Global Config mode to display the configured global source interface details used for a TACACS+ client. The IP address of the selected interface is used as source IP for all communications with the server.

Format `show tacacs source-interface`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Config)# show tacacs source-interface

TACACS Client Source IPv4 Address  : 1.1.1.1 [UP]
```

Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command (see **"show running-config" on page 120**) to capture the running configuration into a script. Use the `copy` command (see **"copy" on page 140**) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with "`!`" is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```



Note: To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user jane from a blank password to hello, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

script apply

This command applies the commands in the script to the switch. The *`scriptname`* parameter is the name of the script to apply.

Format	`script apply` *`scriptname`*
Mode	Privileged EXEC

script delete

This command deletes a specified script where the *`scriptname`* parameter is the name of the script to delete. The `all` option deletes all the scripts present on the switch.

Format	`script delete {`*`scriptname`* `| all}`
Mode	Privileged EXEC

script list

This command lists all scripts present on the switch as well as the remaining available space.

Format `script list`

Mode Privileged EXEC

Term	Definition
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

This command displays the contents of a script file, which is named *scriptname*.

Format `script show scriptname`

Mode Privileged EXEC

Term	Definition
Output Format	line number: line contents

script validate

This command validates a script file by parsing each line in the script file where *scriptname* is the name of the script to validate.The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format `script validate scriptname`

Mode Privileged EXEC

Prelogin Banner, System Prompt, and Host Name Commands

This section describes the commands you use to configure the prelogin banner and the system prompt. The prelogin banner is the text that displays before you login at the `User:` prompt.

copy (pre-login banner)

The `copy` command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, SFTP, SCP, or Xmodem.

Note: The parameter *`ipaddr`* is either an IPv4 address, or an IPv6 address for routing packages that support IPv6.

Default	none
Format	Copy banner to the switch: `copy tftp://`*`ipaddr/filepath/filename`* `nvram:clibanner` Copy banner from the switch: `copy nvram:clibanner tftp://`*`ipaddr/filepath/filename`*
Mode	Privileged EXEC

set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format	`set prompt` *`prompt_string`*
Mode	Privileged EXEC

hostname

This command sets the system hostname. It also changes the prompt. The length of name may be up to 64 alphanumeric, case-sensitive characters.

Format	`hostname` *`hostname`*
Mode	Privileged EXEC

show clibanner

Use this command to display the configured prelogin CLI banner. The prelogin banner is the text that displays before displaying the CLI prompt.

Default	No contents to display before displaying the login prompt.
Format	`show clibanner`
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show clibanner

Banner Message configured :
=========================


-------------------------
         TEST
-------------------------
```

set clibanner

Use this command to configure the prelogin CLI banner before displaying the login prompt.

Format `set clibanner line`

Mode Global Config

Parameter	Definition
line	Banner text where “” (double quote) is a delimiting character. The banner message can be up to 2000 characters.

no set clibanner

Use this command to unconfigure the prelogin CLI banner.

Format `no set clibanner`

Mode Global Config

Chapter 3: Utility Commands

This chapter describes the utility commands available in the EdgeSwitch CLI.

The chapter contains the following sections:

- **"AutoInstall Commands" on page 102**
- **"CLI Output Filtering Commands" on page 105**
- **"Dual Image Commands" on page 107**
- **"System Information and Statistics Commands" on page 108**
- **"Logging Commands" on page 126**
- **"Email Alerting and Mail Server Commands" on page 132**
- **"System Utility and Clear Commands" on page 136**
- **"Simple Network Time Protocol Commands" on page 144**
- **"Time Zone Commands" on page 148**
- **"DHCP Server Commands" on page 151**
- **"DNS Client Commands" on page 160**
- **"IP Address Conflict Commands" on page 164**
- **"Serviceability Packet Tracing Commands" on page 165**
- **"Cable Test Command" on page 179**
- **"Remote Monitoring Commands" on page 180**
- **"Statistics Application Commands" on page 191**



Note: The commands in this chapter consist of four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

AutoInstall Commands

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- Downloading an image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- Automatically downloading an image from a TFTP server in the following situations:
  - When the switch is booted with no saved configuration found.
  - When the switch is booted with a saved configuration that has AutoInstall enabled.

When the switch boots and no configuration file is found, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration flies are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is automatically installed. A downloaded configuration file is saved to non-volatile memory.



Note: AutoInstall from a TFTP server can run on any IP interface, including the network port, service port, and in-band routing interfaces (if supported). To support AutoInstall, the DHCP client is enabled operationally on the service port, if it exists, or the network port, if there is no service port.

boot autoinstall

Use this command to operationally start or stop the AutoInstall process on the switch. The command is non-persistent and is not saved in the startup or running configuration file.

Default	stopped
Format	`boot autoinstall {start | stop}`
Mode	Privileged EXEC

boot host retrycount

Use this command to set the number of attempts to download a configuration file from the TFTP server.

Default	3
Format	`boot host retrycount` *1-3*
Mode	Privileged EXEC

no boot host retrycount

Use this command to set the number of attempts to download a configuration file to the default value.

Format	`no boot host retrycount`
Mode	Privileged EXEC

boot host dhcp

Use this command to enable AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.

Default	enabled
Format	`boot host dhcp`
Mode	Privileged EXEC

no boot host dhcp

Use this command to disable AutoInstall for the next reboot cycle.

Format	`no boot host dhcp`
Mode	Privileged EXEC

boot host autosave

Use this command to automatically save the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory by using the `write memory` or `copy system:running-config nvram:startup-config` command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Default	disabled
Format	`boot host autosave`
Mode	Privileged EXEC

no boot host autosave

Use this command to disable automatically saving the downloaded configuration on the switch.

Format	`no boot host autosave`
Mode	Privileged EXEC

boot host autoreboot

Use this command to allow the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch.

Default	enabled
Format	`boot host autoreboot`
Mode	Privileged EXEC

no boot host autoreboot

Use this command to prevent the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

Format	`no boot host autoreboot`
Mode	Privileged EXEC

erase startup-config

Use this command to erase the text-based configuration file stored in non-volatile memory. If the switch boots and no startup-config file is found, the AutoInstall process automatically begins.

Format	`erase startup-config`
Mode	Privileged EXEC

erase factory-defaults

Use this command to erase the text-based factory-defaults file stored in non-volatile memory.

Default	Disable
Format	`erase factory-defaults`
Mode	Global Config

show autoinstall

This command displays the current status of the AutoInstall process.

Format	`show autoinstall`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show autoinstall

AutoInstall Mode.............................. Stopped
AutoInstall Persistent Mode................... Disabled
AutoSave Mode................................. Disabled
AutoReboot Mode............................... Enabled
AutoInstall Retry Count....................... 3
```

CLI Output Filtering Commands

show *xxx* | include "*string*"

The command *xxx* is executed and the output is filtered to only show lines containing the *string* match. All other non-matching lines in the output are suppressed.

Example: The following shows an example of the CLI command.

```
(UBNT EdgeSwitch) #show running-config | include "spanning-tree"

spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

show *xxx* | include "*string*" exclude "*string2*"

The command *xxx* is executed and the output is filtered to only show lines containing the *string* match and not containing the *string2* match. All other non-matching lines in the output are suppressed. If a line of output contains both the include and exclude strings then the line is not displayed.

Example: The following shows example of the CLI command.

```
(UBNT EdgeSwitch) #show running-config | include "spanning-tree" exclude "configuration"

spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

show *xxx* | exclude "*string*"

The command *xxx* is executed and the output is filtered to show all lines not containing the *string* match. Output lines containing the *string* match are suppressed.

Example: The following shows an example of the CLI command.

```
(UBNT EdgeSwitch) #show interface 0/1

Packets Received Without Error..................... 0
Packets Received With Error........................ 0
Broadcast Packets Received......................... 0
Receive Packets Discarded.......................... 0
Packets Transmitted Without Errors................. 0
Transmit Packets Discarded......................... 0
Transmit Packet Errors............................. 0
Collision Frames................................... 0
Time Since Counters Last Cleared................... 281 day 4 hr 9 min 0 sec

(UBNT EdgeSwitch) #show interface 0/1 | exclude "Packets"

Transmit Packet Errors............................. 0
Collision Frames................................... 0
Time Since Counters Last Cleared................... 20 day 21 hr 30 min 9 sec
```

show *xxx* | begin "*string*"

The command *xxx* is executed and the output is filtered to show all lines beginning with and following the first line containing the *string* match. All prior lines are suppressed.

Example: The following shows an example of the CLI command.

```
(UBNT EdgeSwitch) #show port all | begin “1/1”

1/1           Enable                         Down   Disable N/A    N/A
1/2           Enable                         Down   Disable N/A    N/A
1/3           Enable                         Down   Disable N/A    N/A
1/4           Enable                         Down   Disable N/A    N/A
1/5           Enable                         Down   Disable N/A    N/A
1/6           Enable                         Down   Disable N/A    N/A

(UBNT EdgeSwitch) #
```

show *xxx* | section "*string*"

The command *xxx* is executed and the output is filtered to show only lines included within the section(s) identified by lines containing the *string* match and ending with the first line containing the default end-of-section identifier (i.e. “exit”).

Example: The following shows an example of the CLI command.

```
(UBNT EdgeSwitch) #show running-config | section “interface 0/1”

interface 0/1
no spanning-tree port mode
exit
```

show *xxx* | section "*string*" "*string2*"

The command *xxx* is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the *string* match and ending with the first line containing the *string2* match. If multiple sessions matching the specified string match criteria are part of the base output, then all instances are displayed.

show *xxx* | section "*string*" include "*string2*"

The command *xxx* is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the *string* match and ending with the first line containing the default end-of-section identifier (i.e. “exit”) and that include the *string2* match. This type of filter command could also include “exclude” or user-defined end-of-section identifier parameters as well.

Dual Image Commands

The EdgeSwitch software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

delete

This command deletes the backup image file from the permanent storage.

Format	`delete backup`
Mode	Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image doesn't exist on the system, this command returns an error message.

Format	`boot system {active | backup}`
Mode	Privileged EXEC

show bootvar

This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image. This command displays the switch activation status.

Format	`show bootvar`
Mode	Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced.

Format	`filedescr {active | backup} text-description`
Mode	Privileged EXEC

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.

Format	`update bootcode`
Mode	Privileged EXEC

System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

show arp switch

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces – network or service ports. ARP entries associated with routing interfaces are not listed.

Format `show arp switch`

Mode Privileged EXEC

Term	Definition
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is Management. For a network port, the output is the slot/port of the physical interface.

show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset. The unit is the switch identifier.

Format `show eventlog [unit]`

Mode Privileged EXEC

Term	Definition
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.
Unit	The unit for the event.

Note: Event log information is retained across a switch reset.

show hardware

This command displays inventory information for the switch.

Note: The `show version` command and the `show hardware` command display the same information. In future releases of the software, the `show hardware` command will not be available. For a description of the command output, see the command **"show version" on page 109**.

Format `show hardware`

Mode Privileged EXEC

show version

This command displays inventory information for the switch.



Note: The `show version` command will replace the `show hardware` command in future releases of the software.

Format	`show version`
Mode	Privileged EXEC

Term	Definition
System Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.
Burned in MAC Address	Universally assigned network address.
Software Version	The *release.version.revision* number of the code currently running on the switch.

show platform vpd

This command displays vital product data for the switch.

Format	`show platform vpd`
Mode	User Privileged

The following information is displayed.

Term	Definition
Operational Code Image File Name	Build Signature loaded into the switch
Software Version	Release Version Maintenance Level and Build (RVMB) information of the switch.
Timestamp	Timestamp at which the image is built

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show platform vpd

Operational Code Image File Name.............. ES48.v0.8.0.4697373d
Software Version.............................. v0.8.0.4697373
Timestamp..................................... Thu Aug 28 03:45:53 EDT 2014
```

show interface

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Format	`show interface {`*`slot/port`*` | switchport}`
Mode	Privileged EXEC

The displayed information when the argument is *`slot/port`* is as follows:

Term	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Term	Definition
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffered space.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The displayed information when the argument is `switchport` is as follows:

Term	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interfaces status

Use this command to display interface information, including the description, port state, speed and auto-neg capabilities. The command is similar to `show port all` but displays additional fields like interface description and port-capability.

The description of the interface is configurable through the existing command description <name> which has a maximum length of 64 characters that is truncated to 28 characters in the output. The long form of the description can be displayed using show port description. The interfaces displayed by this command are physical interfaces, LAG interfaces and VLAN routing interfaces.

Format `show interfaces status [slot/port]`

Mode Privileged EXEC

show interfaces traffic

Use this command to display interface traffic information.

Format `show interfaces traffic [slot/port]`

Mode Privileged EXEC

show interface counters

This command reports key summary statistics for all the ports (physical, port-channel, and CPU).

Format `show interface counters`

Mode Privileged EXEC

Term	Definition
Packets Received Successfully:	
Port	Interface (slot/port), port-channel number, or CPU.
InOctets	Total Packets Received Without Error - The total number of packets received that were without errors.
InUcastPkts	Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.
InMcastPkts	Multicast Packets Received - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
InBcastPkts	Broadcast Packets Received - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Successfully:	
Port	Interface (slot/port), port-channel number, or CPU.
OutOctets	Total Packets Transmitted Successfully - The number of frames that have been transmitted by this port to its segment.
OutUcastPkts	Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
OutMcastPkts	Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
OutBcastPkts	Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show interface counters

Port              InOctets      InUcastPkts      InMcastPkts      InBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1                  0                0                0                0
0/2                  0                0                0                0
0/3              15098                0               31               39
0/4                  0                0                0                0
0/5                  0                0                0                0
...
...
ch1                  0                0                0                0
ch2                  0                0                0                0
...
ch64                 0                0                0                0
CPU             359533                0             3044              217

Port             OutOctets     OutUcastPkts     OutMcastPkts     OutBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1                  0                0                0                0
0/2                  0                0                0                0
0/3             131369                0               11               89
0/4                  0                0                0                0
0/5                  0                0                0                0
...
...
ch1                  0                0                0                0
ch2                  0                0                0                0
...
ch64                 0                0                0                0
CPU            4025293                0            32910              120
```

show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

Format	`show interface ethernet {slot/port | switchport | all}`
Mode	Privileged EXEC

When you specify a value for *slot/port*, the command displays the following information.

Term	Definition
Packets Received	• **Total Packets Received (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. • **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Received 65–127 Octets** - The total number of packets (including bad packets) received that were from 65 to 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 128–255 Octets** - The total number of packets (including bad packets) received that were from 128 to 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 256–511 Octets** - The total number of packets (including bad packets) received that were from 256 to 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 512–1023 Octets** - The total number of packets (including bad packets) received that were from 512 to 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 1024–1518 Octets** - The total number of packets (including bad packets) received that were from 1024 to 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received > 1518 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 64 Octets** - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets RX and TX 65–127 Octets** - The total number of packets (including bad packets) received and transmitted that were from 65 to 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 128–255 Octets** - The total number of packets (including bad packets) received and transmitted that were from 128 to 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 256–511 Octets** - The total number of packets (including bad packets) received and transmitted that were from 256 to 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 512–1023 Octets** - The total number of packets (including bad packets) received and transmitted that were from 512 to 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1024–1518 Octets** - The total number of packets (including bad packets) received and transmitted that were from 1024 to 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1519–2047 Octets** - The total number of packets received and transmitted that were from 1519 to 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 2048–4095 Octets** - The total number of packets received that were from 2048 to 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 4096–9216 Octets** - The total number of packets received that were from 4096 to 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	• **Total Packets Received Without Error** - The total number of packets received that were without errors. • **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol. • **Multicast Packets Received** - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. • **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Term	Definition
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Received with MAC Errors	• **Total Packets Received with MAC Errors** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. • **Jabbers Received** - 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). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. • **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). • **Alignment Errors** - 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 a bad Frame Check Sequence (FCS) with a non-integral number of octets. • **FCS Errors** - 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 a bad Frame Check Sequence (FCS) with an integral number of octets. • **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Received Packets Not Forwarded	• **Total Received Packets Not Forwarded** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process • **802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • **Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type.
Packets Transmitted Octets	• **Total Packets Transmitted (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. • **Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Transmitted > 1518 Octets** - The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Max Frame Size** - The maximum size of the Info (non-MAC) field that this port will receive or transmit.
Packets Transmitted Successfully	• **Total Packets Transmitted Successfully** - The number of frames that have been transmitted by this port to its segment. • **Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. • **Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent. • **Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Term	Definition
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Errors	• **Total Transmit Errors** - The sum of Single, Multiple, and Excessive Collisions.
Transmit Discards	• **Total Transmit Packets Discards** - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded. • **Single Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. • **Multiple Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. • **Excessive Collisions** - A count of frames for which transmission on a particular interface fails due to excessive collisions.
Protocol Statistics	• **802.3x Pause Frames Transmitted** - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • **GVRP PDUs Received** - The count of GVRP PDUs received in the GARP layer. • **GVRP PDUs Transmitted** - The count of GVRP PDUs transmitted from the GARP layer. • **GVRP Failed Registrations** - The number of times attempted GVRP registrations could not be completed. • **GMRP PDUs Received** - The count of GMRP PDUs received in the GARP layer. • **GMRP PDUs Transmitted** - The count of GMRP PDUs transmitted from the GARP layer. • **GMRP Failed Registrations** - The number of times attempted GMRP registrations could not be completed. • **STP BPDUs Transmitted** - Spanning Tree Protocol Bridge Protocol Data Units sent. • **STP BPDUs Received** - Spanning Tree Protocol Bridge Protocol Data Units received. • **RST BPDUs Transmitted** - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. • **RSTP BPDUs Received** - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. • **MSTP BPDUs Transmitted** - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. • **MSTP BPDUs Received** - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.
Dot1x Statistics	• **EAPOL Frames Transmitted** - The number of EAPOL frames of any type that have been transmitted by this authenticator. • **EAPOL Frames Received** - The number of valid EAPOL frames of any type that have been received by this authenticator.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

If you use the `switchport` keyword, the following information appears.

Term	Definition
Total Packets Received (Octets)	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received Without Error	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

If you use the `all` keyword, the following information appears for all interfaces on the switch.

Term	Definition
Port	The Interface ID.
Bytes Tx	The total number of bytes transmitted by the interface.
Bytes Rx	The total number of bytes transmitted by the interface.
Packets Tx	The total number of packets transmitted by the interface.
Packets Rx	The total number of packets transmitted by the interface.

show interface ethernet switchport

This command displays the private VLAN mapping information for the switch interfaces.

Format `show interface ethernet interface-id switchport`

Mode Privileged EXEC

Parameter	Definition
interface-id	The slot/port of the switch.

The command displays the following information.

Term	Definition
Private-vlan host-association	The VLAN association for the private-VLAN host ports.
Private-vlan mapping	The VLAN mapping for the private-VLAN promiscuous ports.

show interface lag

Use this command to display configuration information about the specified LAG interface.

Format `show interface lag lag-intf-num`

Mode Privileged EXEC

show fiber-ports optical-transceiver

This command displays the diagnostics information of the SFP like Temp, Voltage, Current, Input Power, Output Power, Tx Fault, and LOS. The values are derived from the SFP's A2 (Diagnostics) table using the I^2C interface.

Format `show fiber-ports optical-transceiver {all | slot/port}`

Mode Privileged EXEC

Term	Description
Temp	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured optical output power relative to 1mW.
Input Power	Measured optical power received relative to 1mW.
TX Fault	Transmitter fault.
LOS	Loss of signal.

Example: The following information shows an example of the command output:

```
(UBNT EdgeSwitch) #show fiber-ports optical-transceiver all

                                    Output    Input
Port      Temp  Voltage  Current     Power     Power    TX     LOS
           [C]   [Volt]     [mA]     [dBm]     [dBm]   Fault
--------  ----  -------  -------   -------   -------   -----  ---
0/49      39.3    3.256      5.0    -2.234    -2.465   No     No
0/50      33.9    3.260      5.3    -2.374   -40.000   No     Yes
0/51      32.2    3.256      5.6    -2.300    -2.897   No     No
```

show fiber-ports optical-transceiver-info

This command displays the SFP vendor-related information such as the vendor name, SFP serial number, and SFP part number. The values are derived from the SFP's A0 table using the I²C interface.

Format `show fiber-ports optical-transceiver-info {all | slot/port}`

Mode Privileged EXEC

Term	Description
Port	The interface (slot/port).
Vendor Name	The vendor name is a 16-character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h). The vendor name is the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.
Link Length (50um, OM2)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500MHz*km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Link Length (62.5um, OM1)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz*km at 850nm, 500 MHz*km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must determined from the transceiver technology
Serial Number	The vendor serial number (vendor SN) is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h), defining the vendor's serial number for the transceiver. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified.
Part Number	The vendor part number (vendor PN) is a 16-byte field that contains ASCII characters, left aligned and added on the right with ASCII spaces (20h), defining the vendor part number or product name. A value of all zero in the 16-byte field indicates that the vendor PN is unspecified.
Nominal Bit Rate (Mbps)	The nominal bit (signaling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal as well as those bits carrying data information. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate will depend on the encoding of the data, as defined by the encoding value.
Rev	The vendor revision number (vendor rev) contains ASCII characters, left aligned and padded on the right with ASCII spaces (20h), defining the vendor's product revision number. A value of all zero in this field indicates that the vendor revision is unspecified.

Example: The following information shows an example of the command output:

```
(UBNT EdgeSwitch) #show fiber-ports optical-transceiver-info all

                        Link Link                                  Nominal
                      Length Length                                   Bit
                        50um 62.5um                                  Rate
Port     Vendor Name      [m] [m]  Serial Number    Part Number     [Mbps] Rev
-------- ---------------- --- ---- ---------------- ---------------- ----- ----
0/49      Ubiquiti         8    3   A7N2018414       AXM761           10300 10
0/51      Ubiquiti         8    3   A7N2018472       AXM761           10300 10
0/52      Ubiquiti         8    3   A7N2018501       AXM761           10300 10
```

show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter `all` or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the `count` parameter to view summary information about the forwarding database table. Use the `interface slot/port` parameter to view MAC addresses on a specific interface.

Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface, where `lag-intf-num` is the LAG port number. Use the `vlan vlan_id` parameter to display information about MAC addresses on a specified VLAN.

Format `show mac-addr-table [{macaddr vlan_id | all | count | interface slot/port | vlan vlan_id}]`

Mode Privileged EXEC

The following information is displayed if you do not enter a parameter, if you enter the keyword `all`, or if you enter the MAC address and VLAN ID.

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is six 2-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: • **Static** The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. • **Learned** The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • **Management** The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. • **Self** The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). • **GMRP Learned** The value of the corresponding was learned via GMRP and applies to Multicast. • **Other** The value of the corresponding instance does not fall into one of the other categories.

If you enter `vlan vlan_id`, only the MAC Address, Interface, and Status fields appear. If you enter the `interface slot/port` parameter, in addition to the MAC Address and Status fields, the VLAN ID field also appears.

The following information displays if you enter the `count` parameter:

Term	Definition
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

process cpu threshold

Use this command to configure the CPU utilization thresholds. The Rising and Falling thresholds are specified as a percentage of CPU resources. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds. The CPU utilization threshold configuration is saved across a switch reboot. Configuring the falling utilization threshold is optional. If the falling CPU utilization parameters are not configured, then they take the same value as the rising CPU utilization parameters.

Format `process cpu threshold type total rising 1-100 interval`

Mode Global Config

Parameter	Description
rising threshold	The percentage of CPU resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
rising interval	The duration of the CPU rising threshold violation, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).
falling threshold	The percentage of CPU resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled). A notification is triggered when the total CPU utilization falls below this level for a configured period of time. The falling utilization threshold notification is made only if a rising threshold notification was previously done. The falling utilization threshold must always be equal or less than the rising threshold value. The CLI does not allow setting the falling threshold to be greater than the rising threshold.
falling interval	The duration of the CPU falling threshold, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).

show process app-list

This command displays the user and system applications.

Note: This command is available in Linux 2.6 only.

Format `show process app-list`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
                          Admin     Auto      Running
ID    Name            PID   Status    Restart   Status
---- ---------------- ----- --------- --------- -------
   1 dataplane        15309 Enabled   Disabled  Running
   2 switchdrvr       15310 Enabled   Disabled  Running
   3 syncdb           15314 Enabled   Disabled  Running
   4 lighttpd         18718 Enabled   Enabled   Running
   5 syncdb-test          0 Disabled  Disabled  Stopped
   6 proctest             0 Disabled  Enabled   Stopped
   7 user.start           0 Enabled   Disabled  Stopped
```

show process app-resource-list

This command displays the configured and in-use resources of each application.

Note: This command is available in Linux 2.6 only.

Format `show process app-resource-list`

Mode Privileged EXEC

show process cpu

This command provides the percentage utilization of the CPU by different tasks.



Note:

- It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.
- This command is available in Linux 2.6 only.

Format	`show process cpu`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command using Linux.

```
(UBNT EdgeSwitch) #show process cpu

Memory Utilization Report
status      bytes
------ ----------
free    106450944
alloc   423227392

 CPU Utilization:

  PID      Name                   5 Secs     60 Secs    300 Secs
-------------------------------------------------------------------
  765    _interrupt_thread          0.00%       0.01%       0.02%
  767    bcmL2X.0                   0.58%       0.35%       0.28%
  768    bcmCNTR.0                  0.77%       0.73%       0.72%
  773    bcmRX                      0.00%       0.04%       0.05%
  786    cpuUtilMonitorTask         0.19%       0.23%       0.23%
  834    dot1s_task                 0.00%       0.01%       0.01%
  810    hapiRxTask                 0.00%       0.01%       0.01%
  805    dtlTask                    0.00%       0.02%       0.02%
  863    spmTask                    0.00%       0.01%       0.00%
  894    ip6MapLocalDataTask        0.00%       0.01%       0.01%
  908    RMONTask                   0.00%       0.11%       0.12%
-------------------------------------------------------------------
 Total CPU Utilization              1.55%       1.58%       1.50%
```

show process proc-list

This application displays the processes started by applications created by the Process Manager.



Note: This command is available in Linux 2.6 only.

Format	`show process proc-list`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show process proc-list

      Process         Application              VM Size  VM Peak
PID   Name            ID-Name             Chld  (KB)     (KB)    FD Count
---- ---------------- -------------------- ---- -------- -------- --------
15260 procmgr          0-procmgr            No       1984     1984        8
15309 dataplane        1-dataplane          No     293556   293560       11
15310 switchdrvr       2-switchdrvr         No     177220   177408       57
15314 syncdb           3-syncdb             No       2060     2080        8
18718 lighttpd         4-lighttpd           No       5508     5644       11
18720 lua_magnet       4-lighttpd           Yes     12112    12112        7
18721 lua_magnet       4-lighttpd           Yes     25704    25708        7
```

show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the `all` option.



Note: The `show running-config` command does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *`scriptname`* is provided with a file name extension of ".scr", the output is redirected to a script file.



Note: If you issue the `show running-config` command from a serial connection, remote access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.



Note: If you use a text-based configuration file, the `show running-config` command only displays configured physical interfaces (i.e., if any interface only contains the default configuration, that interface will be skipped from the show running-config command output). This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the `show running-config` command output (and hence from the startup-config file when the system configuration is saved.)

Use the following keys to navigate the command output.

Key	Action
Enter	Advance one line.
Space Bar	Advance one page.
q	Stop the output and return to the prompt.

Note that `--More--` or `(q)uit` is displayed at the bottom of the output screen until you reach the end of the output.

Format `show running-config [all | scriptname]`

Mode Privileged EXEC

show running-config interface

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, and VLAN interfaces.

Format `show running-config interface {interface | lag {lag-intf-num} | vlan {vlan-id}}`

Mode Privileged EXEC

Parameter	Description
`interface`	Running configuration for the specified interface.
`lag-intf-num`	Running configuration for the LAG interface.
`vlan-id`	Running configuration for the VLAN routing interface.

The following information is displayed for the command.

Term	Description
slot/port	Enter an interface in slot/port format.
lag	Display the running config for a specified lag interface.
vlan	Display the running config for a specified vlan routing interface.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show running-config interface 0/1
!Current Configuration:
!
interface  0/1
addport 3/1
exit
(UBNT EdgeSwitch) #
```

show

This command displays the content of text-based configuration files from the CLI. The text-based configuration files (startup-config, backup-config and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

Format	`show { startup-config | backup-config | factory-defaults }`
Mode	Privileged EXEC

Parameter	Description
`startup-config`	Display the content of the startup-config file.
`backup-config`	Display the content of the backup-config file.
`factory-defaults`	Display the content of the factory-defaults file.

Example: The following shows an example of the output from the command when the `startup-config` parameter is specified.

```
(UBNT EdgeSwitch) #show startup-config

!Current Configuration:
!
!System Description “EdgeSwitch 24-Port 500W, 0.8.0.4712594, Linux 3.6.5-f4a26ed5”
!System Software Version “0.8.0.4712594”
!System Up Time          “1 days 4 hrs 22 mins 0 secs”
!Additional Packages     QOS,IPv6 Management,Routing
!Current SNTP Synchronized Time: SNTP Last Attempt Status Is Not Successful
!
vlan database
exit
configure
stack
member 2 4
exit
slot 2/0 5
set slot power 2/0
no set slot disable 2/0
line console
exit
line telnet
exit
--More-- or (q)uit
line ssh
exit
!
exit

(UBNT EdgeSwitch) #
```

Example: The following shows an example of output from the command when the `backup-config` parameter is specified.

```
(UBNT EdgeSwitch) #show backup-config

!Current Configuration:
!
!System Description "EdgeSwitch 24-Port 500W, 0.8.0.4712594, Linux 3.6.5-f4a26ed5"
!System Software Version "0.8.0.4712594"
!System Up Time          "1 days 4 hrs 22 mins 0 secs"
!Additional Packages     QOS,IPv6 Management,Routing
!Current SNTP Synchronized Time: SNTP Last Attempt Status Is Not Successful
!
vlan database
exit
configure
stack
member 2 4
exit
slot 2/0 5
set slot power 2/0
no set slot disable 2/0
line console
exit
line telnet
exit
line ssh
exit
!
exit

(UBNT EdgeSwitch) #
```

Example: The following shows an example of output from the command when the `factory-defaults` parameter is specified.

```
(UBNT EdgeSwitch) #show factory-defaults

!Current Configuration:
!
!System Description "EdgeSwitch 24-Port 500W, 0.8.0.4712594, Linux 3.6.5-f4a26ed5"
!System Software Version "0.8.0.4712594"
!System Up Time          "1 days 4 hrs 22 mins 0 secs"
!Additional Packages     QOS,IPv6 Management,Routing
!Current SNTP Synchronized Time: SNTP Last Attempt Status Is Not Successful
!
vlan database
exit
configure
stack
member 2 4
exit
slot 2/0 5
set slot power 2/0
no set slot disable 2/0
line console
exit
line telnet
exit
--More-- or (q)uit
```

```
line ssh
exit
!
exit

(UBNT EdgeSwitch) #
```

dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

Format	`dir`
Mode	Privileged EXEC

Example: The following show an example of the output from the `dir` command:

```
(UBNT EdgeSwitch) #dir

    0  drwx                2048 May 09 2002 16:47:30 .
    0  drwx                2048 May 09 2002 16:45:28 ..
    0  -rwx                 592 May 09 2002 14:50:24 slog2.txt
    0  -rwx                  72 May 09 2002 16:45:28 boot.dim
    0  -rwx                   0 May 09 2002 14:46:36 olog2.txt
    0  -rwx            13376020 May 09 2002 14:49:10 image1
    0  -rwx                   0 Apr 06 2001 19:58:28 fsyssize
    0  -rwx                1776 May 09 2002 16:44:38 slog1.txt
    0  -rwx                 356 Jun 17 2001 10:43:18 crashdump.ctl
    0  -rwx                1024 May 09 2002 16:45:44 sslt.rnd
    0  -rwx            14328276 May 09 2002 16:01:06 image2
    0  -rwx                 148 May 09 2002 16:46:06 hpc_broad.cfg
    0  -rwx                   0 May 09 2002 14:51:28 olog1.txt
    0  -rwx                 517 Jul 23 2001 17:24:00 ssh_host_key
    0  -rwx               69040 Jun 17 2001 10:43:04 log_error_crashdump
    0  -rwx                 891 Apr 08 2000 11:14:28 sslt_key1.pem
    0  -rwx                 887 Jul 23 2001 17:24:00 ssh_host_rsa_key
    0  -rwx                 668 Jul 23 2001 17:24:34 ssh_host_dsa_key
    0  -rwx                 156 Apr 26 2001 13:57:46 dh512.pem
    0  -rwx                 245 Apr 26 2001 13:57:46 dh1024.pem
    0  -rwx                   0 May 09 2002 16:45:30 slog0.txt
```

show sysinfo

This command displays switch information.

Format	`show sysinfo`
Mode	Privileged EXEC

Term	Description
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see **"snmp-server" on page 73**.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see **"snmp-server" on page 73**.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see **"snmp-server" on page 73**.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current SNTP Synchronized Time	The system time acquired from a network SNTP server.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the show tech-support command to display system and configuration information when you contact technical support. The output of the `show tech-support` command combines the output of the following commands and includes log history files from previous runs:

- `show version`
- `show sysinfo`
- `show port all`
- `show isdp neighbors`
- `show logging`
- `show event log`
- `show logging buffered`
- `show trap log`
- `show running-config`

Format `show tech-support`
Mode Privileged EXEC

length

Use this command to set the pagination length to *value* number of lines for the sessions specified by configuring on different Line Config modes (telnet/ssh) and is persistent.

Example: The `length` command in Line Console mode applies for Serial Console session.

Default 24
Format `length` *value*
Mode Line Config

no length

Use this command to set the pagination length to the default *value* number of lines.

Format `no length` *value*
Mode Line Config

terminal length

Use this command to set the pagination length to *value* number of lines for the current session. This command configuration takes an immediate effect on the current session and is nonpersistent.

Default 24 lines per page
Format `terminal length` *value*
Mode Privileged EXEC

no terminal length

Use this command to set the *value* to the length value configured on Line Config mode depending on the type of session.

Format `no terminal length` *value*
Mode Privileged EXEC

show terminal length

Use this command to display all the configured terminal length values.

Format `show terminal length`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show terminal length
Terminal Length:
----------------------
For Current Session..... 24
For Serial Console..... 24
For Telnet Sessions..... 24
For SSH Sessions..... 24
```

memory free low-watermark processor

Use this command to get notifications when the CPU free memory falls below the configured threshold. A notification is generated when the free memory falls below the threshold. Another notification is generated once the available free memory rises to 10 percent above the specified threshold. To prevent generation of excessive notifications when the CPU free memory fluctuates around the configured threshold, only one Rising or Falling memory notification is generated over a period of 60 seconds. The threshold is specified in kilobytes. The CPU free memory threshold configuration is saved across a switch reboot.

Format `memory free low-watermark processor` *`1-256392`*

Mode Global Config

Parameter	Description
1-256392	The CPU free memory threshold value. When CPU free memory falls below this threshold, a notification message is triggered. The range is 1 to 256392. The default is 0 (disabled).

Logging Commands

This section describes the commands used to configure system logging, and to view logs and logging settings.

logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

Default	disabled; critical when enabled
Format	`logging buffered`
Mode	Global Config

no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default	enabled
Format	`logging buffered wrap`
Mode	Privileged EXEC

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format	`no logging buffered wrap`
Mode	Privileged EXEC

logging cli-command

This command enables the CLI command logging feature, which enables the EdgeSwitch software to log all CLI commands issued on the system.

Default	enabled
Format	`logging cli-command`
Mode	Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format	`no logging cli-command`
Mode	Global Config

logging console

This command enables logging to the console. You can specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Default	disabled; critical when enabled
Format	`logging console [`*severitylevel*`]`
Mode	Global Config

no logging console

This command disables logging to the console.

Format	`no logging console`
Mode	Global Config

logging host

This command configures the logging host parameters. You can configure up to eight hosts.

Default	*port*: 514 *severitylevel*: critical (2)
Format	`logging host {`*hostaddress*`|`*hostname*`} `*addresstype*` {`*port*` `*severitylevel*`}`
Mode	Global Config

Parameter	Description
hostaddress	The IP address of the logging host.
hostname	The hostname of the logging host.
addresstype	Indicates the type of address ipv4 or ipv6 or dns being passed.
port	A port number from 1 to 65535.
severitylevel	Specify this value as either an integer from 0 to 7, or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# logging host google.com dns 214
(UBNT EdgeSwitch) (Config)# logging host 10.130.64.88 ipv4 214 6
(UBNT EdgeSwitch) (Config)# logging host 2000::150 ipv6 214 7
```

logging host reconfigure

This command enables logging host reconfiguration. The *hostindex* is the logging host index for which to change the IP address.

Format	`logging host reconfigure` *hostindex*
Mode	Global Config

logging host remove

This command disables logging to host. See **"show logging hosts" on page 130** for a list of host indexes.

Format	`logging host remove` *hostindex*
Mode	Global Config

logging port

This command sets the local port number of the LOG client for logging messages. The *portid* can be in the range from 1 to 65535.

Default	514
Format	`logging port` *portid*
Mode	Global Config

no logging port

This command resets the local logging port to the default.

Format	`no logging port`
Mode	Global Config

logging syslog

This command enables syslog logging.

Format `logging syslog`

Mode Global Config

no logging syslog

This command disables syslog logging.

Format `no logging syslog`

Mode Global Config

logging syslog port

This command enables syslog logging. The *portid* parameter is an integer with a range of 1-65535.

Default disabled

Format `logging syslog port portid`

Mode Global Config

no logging syslog port

This command disables syslog logging.

Format `no logging syslog port`

Mode Global Config

logging syslog source-interface

This command configures the syslog source-interface (source IP address) for syslog server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format `logging syslog source-interface {slot/port | {vlan vlan-id}}`

Mode Global Config

Parameter	Description
slot/port	VLAN or port-based routing interface.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

Example: The following shows examples of the command.

```
(config)#logging syslog source-interface 4/1
(config)#logging syslog source-interface 0/1
```

no logging syslog source-interface

This command disables syslog logging.

Format `no logging syslog source-interface`

Mode Global Config

show logging

This command displays logging configuration information.

Format `show logging`

Mode Privileged EXEC

Term	Description
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client Source Interface	Shows the configured syslog source-interface (source IP address).
CLI Command Logging	Shows whether CLI Command logging is enabled.
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity at which the logging entries are retained after a system reboot.
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show logging

Logging Client Local Port           : 514
Logging Client Source Interface     : (not configured)
CLI Command Logging                 : disabled
Console Logging                     : enabled
Console Logging Severity Filter     : error
Buffered Logging                    : enabled
Persistent Logging                  : disabled
Persistent Logging Severity Filter  : alert

Syslog Logging                      : disabled

Log Messages Received               : 1010
Log Messages Dropped                : 0
Log Messages Relayed                : 0
```

show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format `show logging buffered`

Mode Privileged EXEC

Term	Description
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In-Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts. Use the "|" character to display the output filter options.

Format `show logging hosts`

Mode Privileged EXEC

Term	Description
Index	Used for deleting hosts.
IP Address / Hostname	IP address or hostname of the logging host.
Severity	The minimum severity to log to the specified address. The possible values are `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Status	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show logging hosts ?

<cr>                    Press enter to execute the command.
|                       Output filter options.

(UBNT EdgeSwitch) #show logging hosts

Index    IP Address/Hostname     Severity    Port   Status
-------- ---------------------- -----------  ------ ---------
1         10.130.64.88           critical     514    Active
2         2000::150              critical     514    Active
```

show logging persistent

Use the `show logging persistent` command to display persistent log entries.

Format `show logging persistent`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show logging persistent

Persistent Logging    : disabled
Persistent Log Count  : 0
```

show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

Mode Privileged EXEC

Term	Definition
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

clear logging buffered

This command clears buffered logging (system startup and system operation logs).

Format	`clear logging buffered`
Mode	Privileged EXEC

Email Alerting and Mail Server Commands

logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. The *severitylevel* value is specified either as an integer from 0 to 7 or symbolically using one of these keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Default	disabled; when enabled, log messages at or above severity Warning (4) are emailed
Format	logging email [*severitylevel*]
Mode	Global Config

no logging email

This command disables email alerting.

Format	no logging email
Mode	Global Config

logging email urgent

This command sets the lowest severity level at which log messages are emailed immediately in a single email message. Specify the *severitylevel* value either an as integer (0-7) or symbolically using these keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7). Specify none to indicate that log messages are collected and sent in a batch email at a specified interval.

Default	Alert (1) and emergency (0) messages are sent immediately.
Format	logging email urgent {*severitylevel* | none}
Mode	Global Config

no logging email urgent

This command resets the urgent severity level to the default value.

Format	no logging email urgent
Mode	Global Config

logging email message-type to-addr

This command configures the email address to which messages are sent. The message types supported are urgent, non-urgent, and both. For each supported severity level, multiple email addresses can be configured. The *to-email-addr* variable is a standard email address, such as *admin@yourcompany.com*.

Format	logging email message-type {urgent|non-urgent|both} to-addr *to-email-addr*
Mode	Global Config

no logging email message-type to-addr

This command removes the configured to-addr field of email.

Format	no logging email message-type {urgent|non-urgent|both} to-addr *to-email-addr*
Mode	Global Config

logging email from-addr

This command configures the email address of the sender (the switch).

Default	switch@company.com
Format	logging email from-addr *from-email-addr*
Mode	Global Config

no logging email from-addr

This command removes the configured email source address.

Format	`no logging email from-addr` *`from-email-addr`*
Mode	Global Config

logging email message-type subject

This command configures the subject line of the email for the specified type.

Default	For urgent messages: Urgent Log Message For non-urgent messages: Non Urgent Log Messages
Format	`logging email message-type {urgent |non-urgent |both} subject` *`subject`*
Mode	Global Config

no logging email message-type subject

This command removes the configured email subject for the specified message type and restores it to the default email subject.

Format	`no logging email message-type {urgent|non-urgent|both} subject`
Mode	Global Config

logging email logtime

This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The valid range is every 30-1440 minutes.

Default	30 minutes
Format	`logging email logtime` *`minutes`*
Mode	Global Config

no logging email logtime

This command resets the non-urgent log time to the default value.

Format	`no logging email logtime`
Mode	Global Config

logging traps

This command sets the severity at which SNMP traps are logged and sent in an email. Specify the *`severitylevel`* value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Default	Info (6) messages and higher are logged.
Format	`logging traps` *`severitylevel`*
Mode	Global Config

no logging traps

This command resets the SNMP trap logging severity level to the default value.

Format	`no logging traps`
Mode	Global Config

logging email test message-type

This command sends an email to the SMTP server to test the email alerting function.

Format `logging email test message-type {urgent |non-urgent |both} message-body message-body`

Mode Global Config

show logging email config

This command displays information about the email alert configuration.

Format `show logging email config`

Mode Privileged EXEC

Term	Definition
Email Alert Logging	The administrative status of the feature: enabled or disabled
Email Alert From Address	The email address of the sender (the switch).
Email Alert Urgent Severity Level	The lowest severity level that is considered urgent. Messages of this type are sent immediately.
Email Alert Non Urgent Severity Level	The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.
Email Alert Trap Severity Level	The lowest severity level at which traps are logged.
Email Alert Notification Period	The amount of time to wait between non-urgent messages.
Email Alert To Address Table	The configured email recipients.
Email Alert Subject Table	The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages. For Msg Type urgent, subject is: The configured email subject for sending urgent messages. For Msg Type non-urgent, subject is: The configured email subject for sending non-urgent messages.

show logging email statistics

This command displays email alerting statistics.

Format `show logging email statistics`

Mode Privileged EXEC

Term	Definition
Email Alert Operation Status	The operational status of the email alerting feature.
No of Email Failures	The number of email messages that have attempted to be sent but were unsuccessful.
No of Email Sent	The number of email messages that were sent from the switch since the counter was cleared.
Time Since Last Email Sent	The amount of time that has passed since the last email was sent from the switch.

clear logging email statistics

This command resets the email alerting statistics.

Format `clear logging email statistics`

Mode Privileged EXEC

mail-server

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4, IPv6, or DNS name format.

Format `mail-server {ip-address | ipv6-address | hostname}`

Mode Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format `no mail-server {ip-address | ipv6-address | hostname}`

Mode Global Config

security

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP sever does not support TLS mode, no email is sent to the SMTP server.

Default none

Format `security {tlsv1 | none}`

Mode Mail Server Config

port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security (i.e. none) it is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

Default 25

Format `port {465 | 25 | 1–65535}`

Mode Mail Server Config

username (Mail Server Config)

This command configures the login ID the switch uses to authenticate with the SMTP server.

Default admin

Format `username name`

Mode Mail Server Config

password

This command configures the password the switch uses to authenticate with the SMTP server.

Default admin

Format `password password`

Mode Mail Server Config

show mail-server config

This command displays information about the email alert configuration.

Format `show mail-server {ip-address | hostname | all} config`

Mode Privileged EXEC

Term	Definition
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4/IPv6 address or DNS hostname of the configured SMTP server.
Email Alert Mail Server Port	The TCP port the switch uses to send email to the SMTP server
Email Alert Security Protocol	The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.
Email Alert Username	The username the switch uses to authenticate with the SMTP server.
Email Alert Password	The password the switch uses to authenticate with the SMTP server.

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

Use the `traceroute` command to discover the routes that IPv4 or IPv6 packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

The user may specify the source IP address of the traceroute probes. Recall that traceroute works by sending packets that are expected not to reach their final destination, but instead trigger ICMP error messages back to the source address from each hop along the forward path to the destination. By specifying the source address, the user can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric.) It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router.

In the CLI, the user may specify the source either as an IPv4 address, IPv6 address, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the primary IPv4 address on the source interface. With SNMP, the source must be specified as an address. The source cannot be specified in the web UI.

The EdgeSwitch software will not accept an incoming packet, such as a traceroute response, that arrives on a routing interface if the packet's destination address is on one of the out-of-band management interfaces (service port or network port). Similarly, the EdgeSwitch software will not accept a packet that arrives on a management interface if the packet's destination is an address on a routing interface. Thus, it would be futile to send a traceroute on a management interface using a routing interface address as source, or to send a traceroute on a routing interface using a management interface as source. When sending a traceroute on a routing interface, the source must be that routing interface or another routing interface. When sending a traceroute on a management interface, the source must be on that management interface. For this reason, the user cannot specify the source as a management interface or management interface address. When sending a traceroute on a management interface, the user should not specify a source address, but instead let the system select the source address from the outgoing interface.

Default

- *count*: 3 probes
- *interval*: 3 seconds
- *size*: 0 bytes
- *port*: 33434
- *maxTtl*: 30 hops
- *maxFail*: 5 probes
- *initTtl*: 1 hop

Format

```
traceroute {ip-address | [ipv6] {ipv6-address | hostname}}
[initTtl initTtl] [maxTtl maxTtl] [maxFail maxFail]
[interval interval] [count count] [port port] [size size]
[source {ip-address | ipv6-address | slot/port}]
```

Mode Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	Description
ip-address	The IP address value should be a valid IP address.
ipv6-address	The IPv6 address value should be a valid IPv6 address.
hostname	The hostname value should be a valid hostname.
ipv6	The optional `ipv6` keyword can be used before *ipv6-address* or *hostname*. Giving the `ipv6` keyword before the hostname tries it to resolve to an IPv6 address.

Parameter	Description
initTtl	Use *initTtl* to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 1 to 255.
maxTtl	Use *maxTtle* to specify the maximum TTL. Range is 1 to 255.
maxFail	Use *maxFail* to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 1 to 255.
interval	Use the optional *interval* parameter to specify the time between probes, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
count	Use the optional *count* parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional *port* parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional *size* parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the optional *source* parameter to specify the source IP address or interface for the traceroute.

The following are examples of the CLI command.

Example: traceroute success:

```
(UBNT EdgeSwitch) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3
port 33434 size 43
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

Example: traceroute IPv6 success:

```
(UBNT EdgeSwitch) # traceroute 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port
33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1      2001::2   708 msec     41 msec     11 msec

The above command can also be execute with the optional ipv6 parameter as follows:

(UBNT EdgeSwitch) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port
33434 size 43
```

Example: traceroute failure:

```
(UBNT EdgeSwitch) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3 port 33434 size
43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

Example: traceroute IPv6 Failure:

```
(UBNT EdgeSwitch)# traceroute 2001::2 initTtl 1 maxFail 0 interval 1 count 3 port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1       3001::1   708 msec     41 msec     11 msec
2       4001::2   250 msec     200 msec    193 msec
3       5001::3   289 msec     313 msec    278 msec
4       6001::4   651 msec     41 msec     270 msec
5          0             0 msec *
Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0
```

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **y**, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format	`clear config`
Mode	Privileged EXEC

clear counters

This command clears the statistics for a specified *slot/port*, for `all` ports, or for the entire switch (if no parameter is specified).

Format	`clear counters [`*slot/port* `|` `all]`
Mode	Privileged EXEC

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format	`clear igmpsnooping`
Mode	Privileged EXEC

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format	`clear pass`
Mode	Privileged EXEC

clear traplog

This command clears the trap log.

Format	`clear traplog`
Mode	Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults. When the VLAN configuration is reset to the factory defaults, there are some scenarios regarding GVRP and MVRP that happen due to this:

1. Static VLANs are deleted.
2. GVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since GVRP is disabled by default, this means that GVRP should be disabled and all of its dynamic VLANs should be deleted.

Format	`clear vlan`
Mode	Privileged EXEC

logout

This command closes the current telnet connection or resets the current serial connection.



Note: Save configuration changes before logging out.

Format `logout`

Modes
- Privileged EXEC
- User EXEC

ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and web interfaces.

Default
- The default count is **1**.
- The default interval is **3** seconds.
- The default size is **0** bytes.

Format `ping {address | hostname | {ipv6 {interface {slot/port | vlan 1-4093 | network} link-local-address} | ipv6-address | hostname} [count count] [interval 1-60] [size size] [source ip-address | ipv6-address | {slot/port | vlan 1-4093 | network}]`

Modes Privileged EXEC, User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Description
address	The IPv4 or IPv6 address to ping.
hostname	The hostname of the host to ping.
ipv6	The optional keyword **ipv6** can be used before the *ipv6-address* or *hostname* argument. Using the ipv6 optional keyword before hostname tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
count	Use the count parameter to specify the number of ping packets (ICMP Echo Requests) that are sent to the destination address specified by the *address* field. The range for count is 1 to 15 requests.
interval	Use the interval parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the source keyword to specify the source IP/IPv6 address or interface to use when sending the Echo Request packets.
interface	Use the interface keyword to ping a link-local IPv6 address over an interface.
link-local-address	The link-local IPv6 address to ping over an interface.

The following are examples of the CLI command.

Example: IPv4 ping success:

```
(UBNT EdgeSwitch) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

Example: IPv6 ping success

```
(UBNT EdgeSwitch) #ping 2001::1
 Pinging 2001::1 with 64 bytes of data:

Send count=3, Receive count=3 from 2001::1
Average round trip time = 3.00 ms
```

Example: IPv4 ping failure:

In Case of Unreachable Destination:

```
(UBNT EdgeSwitch) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0
```

In Case Of Request Timed Out:

```
(UBNT EdgeSwitch) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0
```

Example: IPv6 ping failure

```
(UBNT EdgeSwitch) #ping ipv6 2001::4
 Pinging 2001::4 with 64 bytes of data:

Send count=3, Receive count=0 from 2001::4
Average round trip time = 0.00 ms
```

quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	`quit`
Modes	• Privileged EXEC • User EXEC

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format	`reload`
Mode	Privileged EXEC

copy

The `copy` command uploads and downloads files to and from the switch. You can also use the `copy` command to manage the dual images (active and backup) on the file system. To upload and download files from a server you can use FTP, TFTP, Xmodem, Ymodem, or Zmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

Format	`copy` *`source destination`* `{verify | noverify}`
Mode	Privileged EXEC

Replace the source and destination parameters with the options in **"Table 11. Copy Parameters" on page 141**. For the *url* source or destination, use one of the following values:

```
{xmodem | tftp://ipaddr|hostname | ip6address|hostname/filepath/filename
[noval] |  ftp://user@ipaddress | hostname/filepath/filename}
```

The verify|noverify parameters are only available if the image/configuration verify options feature is enabled (see **"file verify" on page 143**). The verify parameter specifies that digital signature verification will be performed for the specified downloaded image or configuration file. The noverify parameter specifies that no verification will be performed.

The keyword ias-users supports the downloading of the IAS user database file. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and its attributes available in the downloaded file. In the command copy *url* ias-users, for *url* one of the following is used for the IAS users file:

```
{ { tftp://ipaddr|hostname | ipv6address|hostname/filepath/filename } |
{ sftp | scp://username@ipaddress/filepath/filename} }
```

Note: The maximum length for the file path is 160 characters, and the maximum length for the file name is 31 characters.

For FTP, TFTP, SFTP, and SCP, the *ipaddr|hostname* parameter is the IP address or host name of the server, *filepath* is the path to the file, and *filename* is the name of the file you want to upload or download. For SFTP and SCP, the *username* parameter is the username for logging into the remote server via SSH.

Note: *ip6address* is also a valid parameter for routing packages that support IPv6.

CAUTION: Remember to upload the existing fastpath.cfg file off the switch prior to loading a new release image in order to make a backup.

Table 11. Copy Parameters

Source	Destination	Description
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration.
nvram:clibanner	*url*	Copies the CLI banner to a server.
nvram:cpupktcapture.pcap	*url*	Uploads CPU packets capture file.
nvram:crash-log	*url*	Copies the crash log to a server.
nvram:errorlog	*url*	Copies the error log file to a server.
nvram:factory-defaults	*url*	Uploads factory defaults file.
nvram:fastpath.cfg	*url*	Uploads the binary config file to a server.
nvram:log	*url*	Copies the log file to a server.
nvram:operational-log	*url*	Copies the operational log file to a server.
nvram:script scriptname	*url*	Copies a specified configuration script file to a server.
nvram:startup-config	nvram:backup-config	Copies the startup configuration to the backup configuration.
nvram:startup-config	*url*	Copies the startup configuration to a server.
nvram:startup-log	*url*	Uploads the startup log file.
nvram:traplog	*url*	Copies the trap log file to a server.
system:running-config	nvram:startup-config	Saves the running configuration to NVRAM.

Table 11. Copy Parameters (Continued)

Source	Destination	Description
system:running-config	nvram:factory-defaults	Saves the running configuration to NVRAM to the factory-defaults file.
system:image	*url*	Saves the system image to a server.
url	nvram:clibanner	Downloads the CLI banner to the system.
url	nvram:fastpath.cfg	Downloads the binary config file to the system.
url	nvram:publickey-config	Downloads the Public Key for Configuration Script validation.
url	nvram:publickey-image	Downloads Public Key for Image validation.
url	nvram:script *destfilename*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
url	nvram:script *destfilename* noval	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows: `#copy tftp://1.1.1.1/file.scr nvram:script file.scr noval`
url	nvram:sshkey-dsa	Downloads an SSH key file. For more information, see **"Secure Shell Commands" on page 46**.
url	nvram:sshkey-rsa1	Downloads an SSH key file.
url	nvram:sshkey-rsa2	Downloads an SSH key file.
url	nvram:sslpem-dhweak	Downloads an HTTP secure-server certificate.
url	nvram:sslpem-dhstrong	Downloads an HTTP secure-server certificate.
url	nvram:sslpem-root	Downloads an HTTP secure-server certificate. For more information, see **"Hypertext Transfer Protocol Commands" on page 49**.
url	nvram:sslpem-server	Downloads an HTTP secure-server certificate.
url	nvram:startup-config	Downloads the startup configuration file to the system.
url	ias-users	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and their attributes available in the downloaded file.
url	{active | backup}	Download an image from the remote server to either image.
{active | backup}	*url*	Upload either image to the remote server.
active	backup	Copy the active image to the backup image.
backup	active	Copy the backup image to the active image.

Example: The following shows an example of downloading and applying the IAS users file.

```
(UBNT EdgeSwitch) #copy tftp://10.131.17.104/aaa_users.txt ias-users

Mode..................................... TFTP
Set Server IP............................ 10.131.17.104
Path..................................... ./
Filename................................. aaa_users.txt
Data Type................................ IAS Users

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer operation completed successfully.

Validating and updating the users to the IAS users database.

Updated IAS users database successfully.

(UBNT EdgeSwitch) #
```

file verify

This command enables digital signature verification while an image and/or configuration file is downloaded to the switch.

Format `file verify {all | image | none | script}`

Mode Global Config

Parameter	Description
`all`	Verifies the digital signature of both image and configuration files.
`image`	Verifies the digital signature of image files only.
`none`	Disables digital signature verification for both images and configuration files.
`script`	Verifies the digital signature of configuration files.

no file verify

Resets the configured digital signature verification value to the factory default value.

Format `no file verify`

Mode Global Config

Simple Network Time Protocol Commands

This section describes the commands you use to automatically configure the system time and date using Simple Network Time Protocol (SNTP).

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *poll-interval* can be a value from 6-10.

Default	6
Format	`sntp broadcast client poll-interval poll-interval`
Mode	Global Config

no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format	`no sntp broadcast client poll-interval`
Mode	Global Config

sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default	disabled
Format	`sntp client mode [broadcast | unicast]`
Mode	Global Config

no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format	`no sntp client mode`
Mode	Global Config

sntp client port

This command sets the SNTP client port ID to a value from 1-65535. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default	0
Format	`sntp client port portid`
Mode	Global Config

no sntp client port

This command resets the SNTP client port back to its default value.

Format	`no sntp client port`
Mode	Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *poll-interval* can be a value from 6-10.

Default	6
Format	`sntp unicast client poll-interval poll-interval`
Mode	Global Config

no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-interval`
Mode	Global Config

sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1 to 30.

Default	5
Format	`sntp unicast client poll-timeout` *`poll-timeout`*
Mode	Global Config

no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-timeout`
Mode	Global Config

sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

Default	1
Format	`sntp unicast client poll-retry` *`poll-retry`*
Mode	Global Config

no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-retry`
Mode	Global Config

sntp server

This command configures an SNTP server (a maximum of three). The server address can be either an IPv4 address or an IPv6 address. The optional *`priority`* can be a value of 1-3, the *`version`* a value of 1-4, and the *`port-id`* a value of 1-65535.

Format	`sntp server {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`} [`*`priority`* `[`*`version`* `[`*`port-id`*`]]]`
Mode	Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format	`no sntp server remove {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`}`
Mode	Global Config

sntp source-interface

Use this command to specify the physical or logical interface to use as the source interface (source IP address) for SNTP unicast server configuration. If configured, the address of source Interface is used for all SNTP communications between the SNTP server and the SNTP client. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the SNTP client falls back to its default behavior.

Format `sntp source-interface {slot/port | vlan vlan-id}`

Mode Global Config

Parameter	Description
slot/port	The unit identifier assigned to the switch.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

no sntp source-interface

Use this command to reset the SNTP source interface to the default settings.

Format `no sntp source-interface`

Mode Global Config

show sntp

This command is used to display SNTP settings and status.

Format `show sntp`

Mode Privileged EXEC

Term	Definition
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
Multicast Count	Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

This command is used to display SNTP client settings.

Format `show sntp client`

Mode Privileged EXEC

Term	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port. The field displays the value 0 if it is default value. When the client port value is 0, if the client is in broadcast mode, it binds to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying OS.
Client Mode	Configured SNTP Client Mode.

show sntp server

This command is used to display SNTP server settings and configured servers.

Format `show sntp server`

Mode Privileged EXEC

Term	Definition
Server IP Address / Hostname	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4, IPv6, or DNS).
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Term	Definition
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4, IPv6, or DNS).
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

Format `show sntp source-interface`

Mode Privileged EXEC

Term	Description
SNTP Client Source Interface	The interface ID of the physical or logical interface configured as the SNTP client source interface.
SNTP Client Source IPv4 Address	The IP address of the interface configured as the SNTP client source interface.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show sntp source-interface

SNTP Client Source Interface.................. (not configured)

(UBNT EdgeSwitch) #
```

Time Zone Commands

Use the Time Zone commands to configure system time and date, time zone and summer time (daylight saving time). Summer time can be recurring or non-recurring.

clock set

This command sets the system time and date.

Format `clock set hh:mm:ss`
`clock set mm/dd/yyyy`

Mode Global Config

Parameter	Description
hh:mm:ss	Enter the current system time in 24-hour format in hours (0-23), minutes (0-59), and seconds (0-59).
mm/dd/yyyy	Enter the current system date the format month, day, year: • The range for month is 1 to 12. • The range for the day of the month is 1 to 31. • The range for year is 2010 to 2079.

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# clock set 03:17:00
(UBNT EdgeSwitch) (Config)# clock set 11/01/2011
```

clock summer-time date

Use the clock summer-time date command to set the summer-time offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they are read as either 0 or \0, as appropriate.

Format `clock summer-time date {date month year hh:mm date month year hh:mm}`
`[offset offset] [zone acronym]`

Mode Global Config

Parameter	Description
date	Day of the month. Range is 1 to 31.
month	Month. Range is the first three letters by name; for example, “jan” for January.
year	Year. The range is 2010 to 2079.
hh:mm	Time in 24-hour format in hours and minutes: • The range for hours is 0 to 23. • The range for minutes is 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The time zone acronym to display when summer-time is in effect. Up to four characters are allowed.

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
(UBNT EdgeSwitch) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18 offset 120
zone INDA
```

clock summer-time recurring

This command sets the summer-time recurring parameters.

Format `clock summer-time recurring {week day month hh:mm week day month hh:mm} [offset offset] [zone acronym]`

Mode Global Config

Parameter	Description
week	Week of the month. The range is 1 to 5, first, last.
day	Day of the week. The range is the first three letters by name; sun, for example.
month	Month. The range is the first three letters by name; jan, for example.
hh:mm	Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
offset	The number of minutes to add during summer-time. The range is 1 to 1440.
acronym	The time zone acronym to display when summer-time is in effect. Up to four characters are allowed.

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18
(UBNT EdgeSwitch) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18 offset 120
zone INDA
```

no clock summer-time

This command disables the summer-time settings.

Format `no clock summer-time`

Mode Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# no clock summer-time
```

clock timezone

Use this command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either 0 or \0 as appropriate.

Format `clock timezone {hours} [minutes minutes] [zone acronym]`

Mode Global Config

Parameter	Description
hours	Hours difference from UTC. The range is -12 to 13.
minutes	Minutes difference from UTC. The range is 0 to 59.
acronym	The acronym for the time zone. Up to four characters are allowed.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# clock timezone 5 minutes 30 zone INDA
```

no clock timezone

Use this command to reset the time zone settings.

Format `no clock timezone`

Mode Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# no clock timezone
```

show clock

Use this command to display the time and date from the system clock.

Format	`show clock`
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) # show clock

15:02:09 (UTC+0:00) Nov 1 2011
No time source
```

Example: The following shows example CLI display output for the command.

With the above configuration the output appears as below:

```
(UBNT EdgeSwitch) # show clock

10:55:40 INDA(UTC+7:30) Nov 1 2011
No time source
```

show clock detail

Use this command to display the detailed system time along with the time zone and the summer-time configuration.

Format	`show clock detail`
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) # show clock detail

15:05:24 (UTC+0:00) Nov 1 2011
No time source

Time zone:
Acronym not configured
Offset is UTC+0:00

Summertime:
Summer-time is disabled
```

Example: The following shows example CLI display output for the command.

With the above configuration the output appears as below:

```
(UBNT EdgeSwitch) # show clock detail

10:57:57 INDA(UTC+7:30) Nov 1 2011
No time source

Time zone:
Acronym is INDA
Offset is UTC+5:30

Summertime:
Acronym is INDA
Recurring every year
Begins on second Sunday of Nov at 03:18
Ends on second Monday of Nov at 03:18
Offset is 120 minutes
Summer-time is in effect.
```

DHCP Server Commands

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

ip dhcp pool

This command configures a DHCP address pool *name* on a DHCP server and enters DHCP pool configuration mode.

Default	none
Format	`ip dhcp pool name`
Mode	Global Config

no ip dhcp pool

This command removes the DHCP address pool. The *name* should be a previously configured pool name.

Format	`no ip dhcp pool name`
Mode	Global Config

client-identifier

This command specifies the unique identifier for a DHCP client. The *unique-identifier* is a valid notation in hexadecimal format. Some systems, such as Microsoft® DHCP clients, require the client identifier instead of hardware addresses. The *unique-identifier* is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, Assigned Numbers for a list of media type codes.

Default	none
Format	`client-identifier unique-identifier`
Mode	DHCP Pool Config

no client-identifier

This command deletes the client identifier.

Format	`no client-identifier`
Mode	DHCP Pool Config

client-name

This command specifies the *name* for a DHCP client. Name is a string consisting of standard ASCII characters.

Default	none
Format	`client-name name`
Mode	DHCP Pool Config

no client-name

This command removes the client name.

Format	`no client-name`
Mode	DHCP Pool Config

default-router

This command specifies the default router list for a DHCP client. The *address1 address2...address8* parameters are valid IP addresses, each containing four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	`default-router address1 [address2....address8]`
Mode	DHCP Pool Config

no default-router

This command removes the default router list.

Format	`no default-router`
Mode	DHCP Pool Config

dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	`dns-server address1 [address2....address8]`
Mode	DHCP Pool Config

no dns-server

This command removes the DNS Server list.

Format	`no dns-server`
Mode	DHCP Pool Config

hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default	ethernet
Format	`hardware-address hardwareaddress type`
Mode	DHCP Pool Config

no hardware-address

This command removes the hardware address of the DHCP client.

Format	`no hardware-address`
Mode	DHCP Pool Config

host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32.

Default	none
Format	`host address [{mask | prefix-length}]`
Mode	DHCP Pool Config

no host

This command removes the IP address of the DHCP client.

Format	`no host`
Mode	DHCP Pool Config

lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify `infinite`, the lease is set for 60 days. You can also specify a lease duration in *`days`* (0-59), *`hours`* (0-23), and *`minutes`* (0-59).

Default	1 (day)
Format	`lease [{`*`days`* `[`*`hours`*`] [`*`minutes`*`] | infinite}]`
Mode	DHCP Pool Config

no lease

This command restores the default value of the lease time for DHCP Server.

Format	`no lease`
Mode	DHCP Pool Config

network (DHCP Pool Config)

This command configures the subnet number and mask for a DHCP address pool on the server. The *`networknumber`* is a valid IP address, made up of four decimal bytes ranging from 0-255. IP address 0.0.0.0 is invalid. The *`mask`* is the IP subnet mask for the specified address pool. The *`prefixlength`* is an integer from 0 to 32.

Default	none
Format	`network` *`networknumber`* `[{`*`mask`* `|` *`prefixlength`*`}]`
Mode	DHCP Pool Config

no network

This command removes the subnet number and mask.

Format	`no network`
Mode	DHCP Pool Config

bootfile

This command specifies the name (*`filename`* parameter) of the default boot image for a DHCP client.

Format	`bootfile` *`filename`*
Mode	DHCP Pool Config

no bootfile

This command deletes the boot image name.

Format	`no bootfile`
Mode	DHCP Pool Config

domain-name

This command specifies the domain name (*`domain`* parameter) for a DHCP client.

Default	none
Format	`domain-name` *`domain`*
Mode	DHCP Pool Config

no domain-name

This command removes the domain name.

Format	`no domain-name`
Mode	DHCP Pool Config

domain-name enable

This command enables the domain name functionality.

Format	`domain-name enable [name name]`
Mode	Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)#domain-name enable
(UBNT EdgeSwitch) (Config)#exit
```

no domain-name enable

This command disables the domain name functionality.

Format	`no domain-name enable`
Mode	Global Config

netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients. One IP address is required; you can specify up to eight addresses in one command line. Servers are listed in order of preference (*address1* is the most preferred server, *address2* the next most preferred, etc.).

Default	none
Format	`netbios-name-server address [address2...address8]`
Mode	DHCP Pool Config

no netbios-name-server

This command removes the NetBIOS name server list.

Format	`no netbios-name-server`
Mode	DHCP Pool Config

netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. The *type* specifies the NetBIOS node type. Valid types are:

- b-node – Broadcast
- p-node – Peer-to-peer
- m-node – Mixed
- h-node – Hybrid (recommended)

Default	none
Format	`netbios-node-type type`
Mode	DHCP Pool Config

no netbios-node-type

This command removes the NetBIOS node Type.

Format	`no netbios-node-type`
Mode	DHCP Pool Config

next-server

This command configures the next server in the boot process of a DHCP client.The *address* parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

Default	inbound interface helper addresses
Format	`next-server address`
Mode	DHCP Pool Config

no next-server

This command removes the boot server list.

Format	`no next-server`
Mode	DHCP Pool Config

option

The option command configures DHCP Server options. The *code* parameter specifies the DHCP option code and ranges from 1-254. The `ascii` *string* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The `hex` *string* parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, a3.4f.22.0c), colon (for example, a3:4f:22:0c), or white space (for example, a3 4f 22 0c).

Default	none
Format	`option code {ascii string | hex string1 [string2...string8] | ip address1 [address2...address8]}`
Mode	DHCP Pool Config

no option

This command removes the DHCP Server options. The *code* parameter specifies the DHCP option code.

Format	`no option code`
Mode	DHCP Pool Config

ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. The parameters *low-address* and *high-address* are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	`ip dhcp excluded-address low-address [high-address]`
Mode	Global Config

no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. The parameters *low-address* and *high-address* are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format	`no ip dhcp excluded-address low-address [high-address]`
Mode	Global Config

ip dhcp ping packets

Use this command to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

Default	2
Format	`ip dhcp ping packets` *`0,2-10`*
Mode	Global Config

no ip dhcp ping packets

This command restores the number of ping packets to the default value.

Format	`no ip dhcp ping packets`
Mode	Global Config

service dhcp

This command enables the DHCP server.

Default	disabled
Format	`service dhcp`
Mode	Global Config

no service dhcp

This command disables the DHCP server.

Format	`no service dhcp`
Mode	Global Config

ip dhcp bootp automatic

This command enables allocation of addresses to the bootp client from the automatic address pool.

Default	disabled
Format	`ip dhcp bootp automatic`
Mode	Global Config

no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Format	`no ip dhcp bootp automatic`
Mode	Global Config

ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default	enabled
Format	`ip dhcp conflict logging`
Mode	Global Config

no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format	`no ip dhcp conflict logging`
Mode	Global Config

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If an asterisk (*) is specified for the *address* parameter, the bindings corresponding to all the addresses are deleted. The *address* is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format `clear ip dhcp binding {address | *}`

Mode Privileged EXEC

clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format `clear ip dhcp server statistics`

Mode Privileged EXEC

clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. The DHCP server clears all conflicts if an asterisk (*) is used as the *address* parameter.

Default none

Format `clear ip dhcp conflict {address | *}`

Mode Privileged EXEC

show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format `show ip dhcp binding [address]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.
Lease expiration	The lease expiration time of the IP address assigned to the client.
Type	The manner in which IP address was assigned to the client.

show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format `show ip dhcp global configuration`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Service DHCP	The field to display the status of dhcp protocol.
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.
Conflict Logging	Shows whether conflict logging is enabled or disabled.
BootP Automatic	Shows whether BootP for dynamic pools is enabled or disabled.

show ip dhcp pool configuration

This command displays pool configuration. If all is specified, configuration for all the pools is displayed.

Format `show ip dhcp pool configuration {name | all}`

Modes Privileged EXEC, User EXEC

Field	Definition
Pool Name	The name of the configured pool.
Pool Type	The pool type.
Lease Time	The lease expiration time of the IP address assigned to the client.
DNS Servers	The list of DNS servers available to the DHCP client.
Default Routers	The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Field	Definition
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Field	Definition
Client Name	The name of a DHCP client.
Client Identifier	The unique identifier of a DHCP client.
Hardware Address	The hardware address of a DHCP client.
Hardware Address Type	The protocol of the hardware platform.
Host	The IP address and the mask for a manual binding to a DHCP client.

show ip dhcp server statistics

This command displays DHCP server statistics.

Format `show ip dhcp server statistics`

Modes Privileged EXEC, User EXEC

Field	Definition
Automatic Bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.

Message	Definition
Message Received:	
DHCP DISCOVER	The number of DHCPDISCOVER messages the server has received.
DHCP REQUEST	The number of DHCPREQUEST messages the server has received.
DHCP DECLINE	The number of DHCPDECLINE messages the server has received.
DHCP RELEASE	The number of DHCPRELEASE messages the server has received.
DHCP INFORM	The number of DHCPINFORM messages the server has received.
Message Sent:	
DHCP OFFER	The number of DHCPOFFER messages the server sent.
DHCP ACK	The number of DHCPACK messages the server sent.
DHCP NACK	The number of DHCPNACK messages the server sent.

show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Format `show ip dhcp conflict [ip-address]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP Server.
Detection time	The time when the conflict was found.

DNS Client Commands

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components of the EdgeSwitch software.

ip domain lookup

Use this command to enable the DNS client.

Default	enabled
Format	`ip domain lookup`
Mode	Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format	`no ip domain lookup`
Mode	Global Config

ip domain name

Use this command to define a default domain name that EdgeSwitch software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. The *name* may not be longer than 255 characters and should not include an initial period. This *name* should be used only when the default domain name list, configured using the `ip domain list` command, is empty.

Default	none
Format	`ip domain name` *name*
Mode	Global Config

Example: The CLI command `ip domain name yahoo.com` will configure yahoo.com as a default domain name. For an unqualified hostname *xxx*, a DNS query is made to find the IP address corresponding to *xxx*.yahoo.com.

no ip domain name

Use this command to remove the default domain name configured using the `ip domain name` command.

Format	`no ip domain name`
Mode	Global Config

ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the `ip domain name` command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default	none
Format	`ip domain list` *name*
Mode	Global Config

no ip domain list

Use this command to delete a name from a list.

Format	`no ip domain list` *name*
Mode	Global Config

ip name-server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter *server-address* is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they are entered.

Format	`ip name-server server-address1 [server-address2...server-address8]`
Mode	Global Config

no ip name-server

Use this command to remove a name server.

Format	`no ip name-server [server-address1...server-address8]`
Mode	Global Config

ip name source-interface

Use this command to specify the physical or logical interface to use as the DNS client (IP name) source interface (source IP address) for DNS client management application. If configured, the source interface address is used for all DNS communications between the DNS server and the DNS client. The selected `source-interface` IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the DNS client falls back to its default behavior.

Format	`ip name source-interface {slot/port | vlan vlan-id}`
Mode	Global Config

no ip name source-interface

Use this command to reset the DNS source interface to the default settings.

Format	`no ip name source-interface`
Mode	Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. The parameter *name* is the host name and *ipaddress* is the IP address of the host. The host name can include 1-158 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	none
Format	`ip host name ipaddress`
Mode	Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format	`no ip host name`
Mode	Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. The *name* is the host name and *v6address* is the IPv6 address of the host. The hostname can include 1-158 alphanumeric characters, periods, hyphens, and spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example "lab-pc 45".

Default none

Format `ipv6 host name v6address`

Mode Global Config

no ipv6 host

Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format `no ipv6 host name`

Mode Global Config

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The *number* indicates the number of times to retry sending a DNS query to the DNS server, and ranges from 0-100.

Default 2

Format `ip domain retry number`

Mode Global Config

no ip domain retry

Use this command to return to the default.

Format `no ip domain retry number`

Mode Global Config

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The *seconds* specifies the time, in seconds, to wait for a response to a DNS query, and ranges from 0-3600.

Default 3

Format `ip domain timeout seconds`

Mode Global Config

no ip domain timeout

Use this command to return to the default setting.

Format `no ip domain timeout seconds`

Mode Global Config

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format `clear host {name | all}`

Mode Privileged EXEC

Parameter	Description
name	A particular host entry to remove. The parameter name ranges from 1-255 characters.
all	Removes all entries.

show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. The parameter name ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

Format `show hosts [name]`

Mode User EXEC

Term	Description
Host name	Domain host name.
Default domain	Default domain name.
Default domain list	Default domain list.
Domain Name lookup	DNS client enabled/disabled.
Number of retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry timeout period	Amount of time to wait for a response to a DNS query.
Name servers	Configured name servers.
DNS Client Source Interface	Shows the configured source interface (source IP address) used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) # show hosts

Host name..................... Device
Default domain................ gm.com
Default domain list........... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup............ Enabled
Number of retries............. 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19
DNS Client Source Interface.......    (not configured)

Configured host name-to-address mapping:

Host                          Addresses
----------------------------- -------------------------------
accounting.gm.com             176.16.8.8

Host              Total       Elapsed     Type          Addresses
--------------- --------      ------    --------     --------------
www.stanford.edu   72            3         IP         171.64.14.203
```

show ip name source-interface

Use this command to display the configured source interface details used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

Format `show ip name source-interface`

Mode Privileged Exec

IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

ip address-conflict-detect run

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format `ip address-conflict-detect run`

Mode Global Config

show ip address-conflict

This command displays the status information corresponding to the last detected address conflict.

Format `show ip address-conflict`

Modes
- Privileged EXEC
- User EXEC

Term	Description
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP Address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC Address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes and seconds since the last address conflict was detected.

clear ip address-conflict-detect

This command clears the detected address conflict status information.

Format `clear ip address-conflict-detect`

Modes
- Privileged EXEC
- User EXEC

Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting the EdgeSwitch.

⚠ **CAUTION:** The output of "debug" commands can be long and may adversely affect system performance.

capture start

Use the command capture start to manually start capturing CPU packets for packet trace. The packet capture operates in three modes: capture file, remote capture, and capture line.

The command is not persistent across a reboot cycle.

Format `capture start [{all|receive|transmit}]`

Mode Privileged EXEC

Parameter	Description
`all`	Capture all traffic.
`receive`	Capture only received traffic.
`transmit`	Capture only transmitted traffic.

capture stop

Use the command capture stop to manually stop capturing CPU packets for packet trace.

Format `capture stop`

Mode Privileged EXEC

capture file|remote|line

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format `capture {file|remote|line}`

Mode Global Config

Parameter	Description
`file`	In the capture file mode, the captured packets are stored in a file on NVRAM. The maximum file size defaults to 524288 bytes. The switch can transfer the file to a TFTP server via TFTP, SFTP, SCP via CLI, and SNMP. The file is formatted in pcap format, is named cpuPktCapture.pcap, and can be examined using network analyzer tools such as Wireshark® or Ethereal®. Starting a file capture automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reaches its maximum size, or until the capture is stopped manually using the CLI command `capture stop`.
`remote`	In the remote capture mode, the captured packets are redirected in real time to an external PC running the Wireshark tool for Microsoft® Windows®. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disabled using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not store any captured data locally on its file system. You can configure the IP port number for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, then these ports must be allowed to pass through the firewall. You must configure the firewall to allow the Wireshark PC to initiate TCP connections to the switch. If the client successfully connects to the switch, the CPU packets are sent to the client PC, then Wireshark receives the packets and displays them. This continues until the session is terminated by either end. Starting a remote capture session automatically terminates the file capture and line capturing.
`line`	In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture session and capturing into a file. There is a maximum 128 packets of maximum 128 bytes that can be captured and displayed in line mode.

capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format `capture remote port id`

Mode Global Config

capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format `capture file size max-file-size`

Mode Global Config

capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reach full capacity.

Format `capture line wrap`

Mode Global Config

no capture line wrap

This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Format `no capture line wrap`

Mode Global Config

show capture packets

Use this command to display packets captured and saved to RAM. It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format `show capture packets`

Mode Privileged EXEC

debug aaa accounting

This command is useful to debug accounting configuration and functionality in User Manager.

Format `debug aaa accounting`

Mode Privileged EXEC

no debug aaa accounting

Use this command to turn off debugging of User Manager accounting functionality.

Format `no debug aaa accounting`

Mode Privileged EXEC

debug aaa authorization

Use this command to enable the tracing for AAA in User Manager. This is useful to debug authorization configuration and functionality in the User Manager. Each of the parameters are used to configure authorization debug flags.

Format `debug aaa authorization commands|exec`

Mode Privileged EXEC

no debug aaa authorization

Use this command to turn off debugging of the User Manager authorization functionality.

Format	`no debug aaa authorization`
Mode	Privileged EXEC

Example: The following is an example of the command.

```
(UBNT EdgeSwitch) #debug aaa authorization
Tacacs authorization receive packet tracing enabled.

(UBNT EdgeSwitch) #debug tacacs authorization packet transmit
authorization tracing enabled.

(UBNT EdgeSwitch) #no debug aaa authorization
AAA authorization tracing enabled

(UBNT EdgeSwitch) #
```

debug arp

Use this command to enable ARP debug protocol messages.

Default	disabled
Format	`debug arp`
Mode	Privileged EXEC

no debug arp

Use this command to disable ARP debug protocol messages.

Format	`no debug arp`
Mode	Privileged EXEC

debug authentication

This command displays either the debug trace for either a single event or all events for an interface

Default	none
Format	`debug authentication packet {all | event} interface`
Mode	Privileged EXEC

debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default	disabled
Format	`debug auto-voip [H323|SCCP|SIP|oui]`
Mode	Privileged EXEC

no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format	`no debug auto-voip`
Mode	Privileged EXEC

debug clear

This command disables all previously enabled "debug" traces.

Default	disabled
Format	`debug clear`
Mode	Privileged EXEC

debug console

This command enables the display of "debug" trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default	disabled
Format	`debug console`
Mode	Privileged EXEC

no debug console

This command disables the display of "debug" trace output on the login session in which it is executed.

Format	`no debug console`
Mode	Privileged EXEC

debug crashlog

Use this command to view information contained in the crash log file that the system maintains when it experiences an unexpected reset. The crash log file contains the following information:

Call stack information in both primitive and verbose forms

- Log Status
- Buffered logging
- Event logging
- Persistent logging
- System Information (output of sysapiMbufDump)
- Message Queue Debug Information
- Memory Debug Information
- Memory Debug Status
- OS Information (output of osapiShowTasks)
- /proc information (meminfo, cpuinfo, interrupts, version and net/sockstat)

Default	disabled
Format	`debug crashlog {[kernel] crashlog-number [upload url] | proc | verbose | deleteall}`
Mode	Privileged EXEC

Parameter	Description
`kernel`	View the crash log file for the kernel
`crashlog-number`	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1 – 4.
`upload` *`url`*	To upload the crash log to a TFTP server, use the `upload` keyword and specify the required TFTP server information.
`proc`	View the application process crashlog.
`verbose`	Enable the verbose crashlog.
`deleteall`	Delete all crash log files on the system.

debug debug-config

Use this command to download or upload the debug-config.ini file. The debug-config. ini file executes CLI commands (including devshell and drivshell commands) on specific predefined events. The debug config file is created manually and downloaded to the switch.

Default	disabled
Format	`debug debug-config {download` *`url`* `| upload` *`url`*`}`
Mode	Privileged EXEC

debug dhcp packet

This command displays "debug" information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Default	disabled
Format	`debug dhcp packet [transmit | receive]`
Mode	Privileged EXEC

no debug dhcp

This command disables the display of "debug" trace output for DHCPv4 client activity.

Format	`no debug dhcp packet [transmit | receive]`
Mode	Privileged EXEC

debug dot1x packet

Use this command to enable 802.1X packet debug trace.

Default	disabled
Format	`debug dot1x`
Mode	Privileged EXEC

no debug dot1x packet

Use this command to disable 802.1X packet debug trace.

Format	`no debug dot1x`
Mode	Privileged EXEC

debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default	disabled
Format	`debug igmpsnooping packet`
Mode	Privileged EXEC

no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format	`no debug igmpsnooping packet`
Mode	Privileged EXEC

debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug igmpsnooping packet transmit`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt
TX - Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01 Src_IP:
9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

Parameter	Description
`TX`	A packet transmitted by the device.
`Intf`	The interface that the packet went out on. Format used is slot/port (internal interface number).
`Src_Mac`	Source MAC address of the packet.
`Dest_Mac`	Destination multicast MAC address of the packet.
`Src_IP`	The source IP address in the IP header in the packet.
`Dest_IP`	The destination multicast IP address in the packet.
`Type`	The type of IGMP packet. Type can be one of the following: • **Membership Query** IGMP Membership Query • **V1_Membership_Report** IGMP Version 1 Membership Report • **V2_Membership_Report** IGMP Version 2 Membership Report • **V3_Membership_Report** IGMP Version 3 Membership Report • **V2_Leave_Group** IGMP Version 2 Leave Group
`Group`	Multicast group address in the IGMP header.

no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format	`no debug igmpsnooping transmit`
Mode	Privileged EXEC

debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug igmpsnooping packet receive`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt
RX - Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05 Src_IP:
11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group: 225.0.0.5
```

The following information is displayed in the trace message:

Term	Description
`RX`	A packet received by the device.
`Intf`	The interface that the packet went out on. Format used is slot/port (internal interface number).
`Src_Mac`	Source MAC address of the packet.
`Dest_Mac`	Destination multicast MAC address of the packet.

Term	Description
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • **Membership_Query** IGMP Membership Query • **V1_Membership_Report** IGMP Version 1 Membership Report • **V2_Membership_Report** IGMP Version 2 Membership Report • **V3_Membership_Report** IGMP Version 3 Membership Report • **V2_Leave_Group** IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format `no debug igmpsnooping receive`

Mode Privileged EXEC

debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default disabled

Format `debug ip acl acl-number`

Mode Privileged EXEC

no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Format `no debug ip acl acl-number`

Mode Privileged EXEC

debug ipv6 dhcp

This command displays "debug" information about DHCPv6 client activities and traces DHCPv6 packets to and from the local DHCPv6 client.

Default disabled

Format `debug ipv6 dhcp`

Mode Privileged EXEC

no debug ipv6 dhcp

This command disables the display of "debug" trace output for DHCPv6 client activity.

Format `no debug ipv6 dhcp`

Mode Privileged EXEC

debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default disabled

Format `debug lacp packet`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
 Pkt TX - Intf: 0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key: 0x36
```

no debug lacp packet

This command disables tracing of LACP packets.

Format	`no debug lacp packet`
Mode	Privileged EXEC

debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port or service port for switching packages. For routing packages, pings are traced on the routing ports as well.

Default	disabled
Format	`debug ping packet`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX - Intf:
0/1(1), SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST
```

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX - Intf: 0/1(1),
SRC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following information is displayed in the trace message:

Term	Definition
`TX/RX`	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
`Intf`	The interface that the packet came in or went out on. Format used is slot/port (internal interface number).
`SRC_IP`	The source IP address in the IP header in the packet.
`DEST_IP`	The destination IP address in the IP header in the packet.
`Type`	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format	`no debug ping packet`
Mode	Privileged EXEC

debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default	disabled
Format	`debug spanning-tree bpdu`
Mode	Privileged EXEC

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format	`no debug spanning-tree bpdu`
Mode	Privileged EXEC

debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug spanning-tree bpdu receive`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX - Intf:
0/9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root Priority:
0x8000 Path Cost: 0
```

The following information is displayed in the trace message:

Term	Definition
RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number).
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is from 0 to 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format `no debug spanning-tree bpdu receive`

Mode Privileged EXEC

debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default disabled

Format `debug spanning-tree bpdu transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX - Intf:
0/7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00, Root_Priority:
0x8000 Path_Cost: 0
```

The following information is displayed in the trace message:

Term	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is port/slot (internal interface number).
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 refers to RSTP, and 3 refers to MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is from 0-61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format `no debug spanning-tree bpdu transmit`

Mode Privileged EXEC

debug tacacs

Use the `debug tacacs packet` command to turn on TACACS+ debugging.

Format	`debug tacacs {packet {receive | transmit}} | accounting | authentication`
Mode	Global Config

Parameter	Description
`packet receive`	Turn on TACACS+ receive packet debugs.
`packet transmit`	Turn on TACACS+ transmit packet debugs.
`accounting`	Turn on TACACS+ authentication debugging.
`authentication`	Turn on TACACS+ authorization debugging.

debug transfer

This command enables debugging for file transfers.

Format	`debug transfer`
Mode	Privileged EXEC

no debug transfer

This command disables debugging for file transfers.

Format	`no debug transfer`
Mode	Privileged EXEC

show debugging

Use the `show debugging` command to display enabled packet tracing configurations.

Format	`show debugging`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)# debug arp
Arp packet tracing enabled.
(UBNT EdgeSwitch)# show debugging
Arp packet tracing enabled.
```

no show debugging

Use the `no show debugging` command to disable packet tracing configurations.

Format	`no show debugging`
Mode	Privileged EXEC

exception protocol

Use this command to specify the protocol used to store the core dump file.

Default	None
Format	`exception protocol {nfs | tftp | none}`
Mode	Global Config

no exception protocol

Use this command to reset the exception protocol configuration to its factory default value.

Default	None
Format	`no exception protocol`
Mode	Global Config

exception dump tftp-server

Use this command to configure the IP address of a remote TFTP server in order to dump core files to an external server.

Default	None
Format	`exception dump tftp-server {`*`ip-address`*`}`
Mode	Global Config

no exception dump tftp-server

Use this command to reset the exception dump remote server configuration to its factory default value.

Default	None
Format	`no exception dump tftp-server`
Mode	Global Config

exception dump nfs

Use this command to configure an NFS mount point in order to dump core file to the NFS file system.

Default	None
Format	`exception dump nfs` *`ip-address/dir`*
Mode	Global Config

no exception dump nfs

Use this command to reset the exception dump NFS mount point configuration to its factory default value.

Default	None
Format	`no exception dump nfs`
Mode	Global Config

exception dump filepath

Use this command to configure a file-path to dump core file to a TFTP server, NFS mount or USB device subdirectory.

Default	None
Format	`exception dump filepath` *`dir`*
Mode	Global Config

no exception dump filepath

Use this command to reset the exception dump filepath configuration to its factory default value.

Default	None
Format	`exception dump filepath`
Mode	Global Config

exception core-file

Use this command to configure a prefix for a core-file name. The core file name is generated with the prefix as follows:

- If `hostname` is selected: `file-name-prefix_hostname_Time_Stamp.bin`
- If `hostname` is not selected: `file-name-prefix_MAC_Address_Time_Stamp.bin`

If `hostname` is configured the core file name takes the `hostname`, otherwise the core-file names uses the MAC address when generating a core dump file. The prefix length is 15 characters.

Default	Core
Format	`exception core-file {file-name-prefix | [hostname] | [time-stamp]}`
Mode	Global Config

no exception core-file

Use this command to reset the exception core file prefix configuration to its factory default value. The hostname and time-stamp are disabled.

Default	Core
Format	`no exception core-file`
Mode	Global Config

exception switch-chip-register

This command enables or disables the switch-chip-register dump in case of an exception. The switch-chip-register dump is taken only for a master unit and not for member units

Default	Disable
Format	`exception switch-chip-register {enable | disable}`
Mode	Global Config

write core

Use the `write core` command to generate a core dump file on demand. The `write core test` command is helpful when testing the core dump setup. For example, if the TFTP protocol is configured, `write core test` communicates with the TFTP server and informs the user if the TFTP server can be contacted. Similarly, if protocol is configured as `nfs`, this command mounts and unmounts the file system and informs the user of the status.

Note: `write core` reloads the switch which is useful when the device malfunctions, but has not crashed.

For `write core test`, the destination file name is used for the TFTP test. Optionally, you can specify the destination file name when the protocol is configured as TFTP.

Default	None
Format	`write core [test [dest_file_name]]`
Mode	Privileged EXEC

show exception

Use this command to display the configuration parameters for generating a core dump file.

Default	None
Format	`show exception`
Mode	Privileged EXEC

Example: The following shows an example of this command.

```
Protocol                    exception protocol configuration
TFTP Server Address         TFTP server configuration
NFS Mount point             NFS mount point configuration
Core File name prefix       Core file prefix configuration.
Hostname                    Core file name contains hostname if enabled.
Timestamp                   Core file name contains timestamp if enabled.
Switch Chip Register Dump   Switch chip register dump configuration
```

logging persistent

Use this command to configure persistent logging for the switch. The severity level of logging messages is specified by *severity-level*.

Possible values for *severity level* are emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, and debug|7.

Default	Disable
Format	logging persistent *severity-level*
Mode	Global Config

no logging persistent

Use this command to disable the persistent logging in the switch.

Format	no logging persistent
Mode	Global Config

mbuf

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format	mbuf {*falling-threshold* | *rising-threshold* | *severity*}
Mode	Global Config

Parameter	Description
falling-threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
rising-threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
severity	The severity level at which Mbuf logs messages. The range is 1-7; default is 5 (L7_LOG_SEVERITY_NOTICE).

show mbuf

Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Format	show mbuf
Mode	Privileged EXEC

Term	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level.

show mbuf total

Use this command to display memory buffer (MBUF) information.

Format `show mbuf total`

Mode Privileged EXEC

Field	Description
`Mbufs Total`	Total number of message buffers in the system.
`Mbufs Free`	Number of message buffers currently available.
`Mbufs Rx Used`	Number of message buffers currently in use.
`Total Rx Norm Alloc Attempts`	Number of times the system tried to allocate a message buffer allocation of class RX Norm.
`Total Rx Mid2 Alloc Attempts`	Number of times the system tried to allocate a message buffer allocation of class RX Mid2.
`Total Rx Mid1 Alloc Attempts`	Number of times the system tried to allocate a message buffer allocation of class RX Mid1.
`Total Rx Mid0 Alloc Attempts`	Number of times the system tried to allocate a message buffer allocation of class RX Mid0.
`Total Rx High Alloc Attempts`	Number of times the system tried to allocate a message buffer allocation of class RX High.
`Total Tx Alloc Attempts`	Number of times the system tried to allocate a message buffer allocation of class TX.
`Total Rx Norm Alloc Failures`	Number of message buffer allocation failures for RX Norm class of message buffer.
`Total Rx Mid2 Alloc Failures`	Number of message buffer allocation failures for RX Mid2 class of message buffer.
`Total Rx Mid1 Alloc Failures`	Number of message buffer allocation failures for RX Mid1 class of message buffer.
`Total Rx Mid0 Alloc Failures`	Number of message buffer allocation failures for RX Mid0 class of message buffer.
`Total Rx High Alloc Failures`	Number of message buffer allocation failures for RX High class of message buffer.
`Total Tx Alloc Failures`	Number of message buffer allocation failures for TX class of message buffer.

Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.



Note: The cable test feature is supported only for copper cable. It is not supported for optical fiber cable. If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

This command returns the status of the specified port.

Format `cablestatus slot/port`

Mode Privileged EXEC

Term	Description
`Cable Status`	One of the following statuses is returned: • **Normal** The cable is working correctly. • **Open** The cable is disconnected or there is a faulty connector. • **Short** There is an electrical short in the cable. • **Cable Test Failed** The cable status could not be determined. The cable may in fact be working.
`Cable Length`	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

Remote Monitoring Commands

Remote Monitoring (RMON) is a method of collecting a variety of data about network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).



Note: There is no configuration command for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.

rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format `rmon alarm alarm-number variable sample-interval {absolute|delta} rising-threshold value [rising-event-index] falling-threshold value [falling-event-index] [startup {rising|falling|rising-falling}] [owner string]`

Mode Global Config

Parameter	Description
alarm-number	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
sample-interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 3600.
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
rising-threshold *value*	The rising threshold for the sample statistics. The range is -2147483648 to 2147483647. The default is 1.
rising-event-index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
falling-threshold *value*	The falling threshold for the sample statistics. The range is -2147483648 to 2147483647. The default is 1.
falling-event-index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
startup	The alarm that may be sent. Possible values are rising, falling, or both rising-falling. The default is rising-falling.
owner *string*	The owner string associated with the alarm entry. The default is monitorAlarm.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100 1
falling-threshold 10 2 startup rising owner myOwner
```

no rmon alarm

This command deletes the RMON alarm entry.

Format `no rmon alarm alarm-number`

Mode Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# no rmon alarm 1
```

rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Format `rmon hcalarm alarm-number variable sample-interval {absolute|delta} rising-threshold high value low value status {positive|negative} [rising-event-index] falling-threshold high value low value status {positive|negative} [falling-event-index] [startup {rising|falling|rising-falling}] [owner string]`

Mode Global Config

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are Absolute Value or Delta Value. The default is Absolute Value.
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are valueNotAvailable, valuePositive, or valueNegative. The default is valueNotAvailable.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are rising, falling, or rising-falling. The default is rising-falling.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of the hcAlarmEntry (while in the active state) and the value was not available. This object is a read-only 32-bit counter value.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is monitorHCAlarm.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is volatile.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# rmon hcalarm 1 ifInOctets.1 30 absolute rising-threshold high 1 low
100 status positive 1 falling-threshold high 1 low 10 status positive startup rising owner myOwner
```

no rmon hcalarm

This command deletes the rmon hcalarm entry.

Format `no rmon hcalarm alarm-number`

Mode Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# no rmon hcalarm 1
```

rmon event

This command sets the RMON event entry in the RMON event MIB group.

Format `rmon event event-number [description string|log|owner string|trap community]`

Mode Global Config

Parameter	Description
`Event Index`	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
`Event Description`	A comment describing the event entry. The default is alarmEvent.
`Event Type`	The type of notification that the probe makes about the event. Possible values are None, Log, SNMP Trap, Log and SNMP Trap. The default is None.
`Event Owner`	Owner string associated with the entry. The default is monitorEvent.
`Event Community`	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# rmon event 1 log description test
```

no rmon event

This command deletes the rmon event entry.

Format `no rmon event event-number`

Mode Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)# no rmon event 1
```

rmon collection history

This command sets the history control parameters of the RMON historyControl MIB group.

Note: This command is not supported on interface range. Each RMON history control collection entry can be configured on only one interface. If you try to configure on multiple interfaces, DUT displays an error.

Format `rmon collection history index-number [buckets number | interval interval-in-sec | owner string]`

Mode Interface Config

Parameter	Description
`History Control Index`	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
`History Control Data Source`	The source interface for which historical data is collected.
`History Control Buckets Requested`	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
`History Control Buckets Granted`	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
`History Control Interval`	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
`History Control Owner`	The owner string associated with the history control entry. The default is monitorHistoryControl.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Interface 0/1)# rmon collection history 1 buckets 10 interval 30 owner myOwner
```

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Interface 0/1-0/10)#rmon collection history 1 buckets 10 interval 30 owner
myOwner

Error: 'rmon collection history' is not supported on range of interfaces.
```

no rmon collection history

This command will delete the history control group entry with the specified index number.

Format	`no rmon collection history` *`index-number`*
Mode	Interface Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Interface 0/1-0/10)# no rmon collection history 1
```

show rmon

This command displays the entries in the RMON alarm table.

Format	`show rmon {alarms | alarm` *`alarm-index`*`}`
Mode	Privileged Exec

Parameter	Description
`Alarm Index`	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
`Alarm Variable`	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
`Alarm Interval`	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
`Alarm Absolute Value`	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
`Alarm Rising Threshold`	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
`Alarm Rising Event Index`	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
`Alarm Falling Threshold`	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
`Alarm Falling Event Index`	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
`Alarm Startup Alarm`	The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising-falling.
`Alarm Owner`	The owner string associated with the alarm entry. The default is monitorAlarm.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon alarms

Index    OID                      Owner
-----------------------------------------------
1      alarmInterval.1            MibBrowser
2      alarmInterval.1            MibBrowser
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon alarm 1

Alarm 1
----------
OID: alarmInterval.1
Last Sample Value: 1
```

```
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold: 1
Falling Threshold: 1
Rising Event: 1
Falling Event: 2
Owner: MibBrowser
```

show rmon collection history

This command displays the entries in the RMON history control table.

Format `show rmon collection history [interfaces slot/port]`

Mode Privileged Exec

Parameter	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon collection history

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
---------------------------------------------------------------------
1         0/1        30         10          10          myowner
2         0/1        1800       50          10          monitorHistoryControl
3         0/2        30         50          10          monitorHistoryControl
4         0/2        1800       50          10          monitorHistoryControl
5         0/3        30         50          10          monitorHistoryControl
6         0/3        1800       50          10          monitorHistoryControl
7         0/4        30         50          10          monitorHistoryControl
8         0/4        1800       50          10          monitorHistoryControl
9         0/5        30         50          10          monitorHistoryControl
10        0/5        1800       50          10          monitorHistoryControl
11        0/6        30         50          10          monitorHistoryControl
12        0/6        1800       50          10          monitorHistoryControl
13        0/7        30         50          10          monitorHistoryControl
14        0/7        1800       50          10          monitorHistoryControl
15        0/8        30         50          10          monitorHistoryControl
16        0/8        1800       50          10          monitorHistoryControl
17        0/9        30         50          10          monitorHistoryControl
18        0/9        1800       50          10          monitorHistoryControl
19        0/10       30         50          10          monitorHistoryControl
--More-- or (q)uit
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon collection history interfaces 0/1

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-------------------------------------------------------------------
1         0/1        30         10          10          myowner
2         0/1        1800       50          10          monitorHistoryControl
```

show rmon events

This command displays the entries in the RMON event table.

Format `show rmon events`

Mode Privileged Exec

Parameter	Description
`Event Index`	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
`Event Description`	A comment describing the event entry. The default is alarmEvent.
`Event Type`	The type of notification that the probe makes about the event. Possible values are None, Log, SNMP Trap, Log and SNMP Trap. The default is None.
`Event Owner`	Owner string associated with the entry. The default is monitorEvent.
`Event Community`	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.
`Owner`	Event owner. The owner string associated with the entry.
`Last time sent`	The last time over which a log or a SNMP trap message is generated.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) # show rmon events

Index  Description       Type      Community   Owner      Last time sent
-------------------------------------------------------------------------------
1      test              log       public      MIB        0 days 0 h:0 m:0 s
```

show rmon history

This command displays the specified entry in the RMON history table.

Format `show rmon history` *`index`* `{errors [period` *`seconds`*`] | other [period` *`seconds`*`] | throughput [period` *`seconds`*`]}`

Mode Privileged Exec

Parameter	Description
`History Control Index`	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
`History Control Data Source`	The source interface for which historical data is collected.
`History Control Buckets Requested`	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
`History Control Buckets Granted`	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
`History Control Interval`	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
`History Control Owner`	The owner string associated with the history control entry. The default is monitorHistoryControl.
`Maximum Table Size`	Maximum number of entries that the history table can hold.

Parameter	Description
Time	Time at which the sample is collected, displayed as period seconds.
CRC Align	Number of CRC align errors.
Undersize Packets	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good Broadcast packets received on the interface.
Multicast	Total number of good Multicast packets received on the interface.
Util	Port utilization of the interface associated with the history index specified.
Dropped Collisions	Total number of dropped collisions.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon history 1 errors

Sample set: 1   Owner: myowner
Interface: 0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                 CRC Align  Undersize Oversize  Fragments  Jabbers
-------------------- ---------- --------- --------- ---------- -------
Jan 01 1970 21:41:43  0          0         0         0          0
Jan 01 1970 21:42:14  0          0         0         0          0
Jan 01 1970 21:42:44  0          0         0         0          0
Jan 01 1970 21:43:14  0          0         0         0          0
Jan 01 1970 21:43:44  0          0         0         0          0
Jan 01 1970 21:44:14  0          0         0         0          0
Jan 01 1970 21:44:45  0          0         0         0          0
Jan 01 1970 21:45:15  0          0         0         0          0
Jan 01 1970 21:45:45  0          0         0         0          0
Jan 01 1970 21:46:15  0          0         0         0          0
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon history 1 throughput

Sample set: 1   Owner: myowner
Interface: 0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                 Octets     Packets   Broadcast Multicast  Util
-------------------- ---------- --------- --------- ---------- --------
Jan 01 1970 21:41:43 0          0         0         0          1
Jan 01 1970 21:42:14 0          0         0         0          1
Jan 01 1970 21:42:44 0          0         0         0          1
Jan 01 1970 21:43:14 0          0         0         0          1
Jan 01 1970 21:43:44 0          0         0         0          1
```

```
Jan 01 1970 21:44:14 0          0         0         0          1
Jan 01 1970 21:44:45 0          0         0         0          1
Jan 01 1970 21:45:15 0          0         0         0          1
Jan 01 1970 21:45:45 0          0         0         0          1
Jan 01 1970 21:46:15 0          0         0         0          1

(UBNT EdgeSwitch) #show rmon history 1 other

Sample set: 1   Owner: myowner
Interface: 0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                 Dropped Collisions
-------------------- ------- ----------
Jan 01 1970 21:41:43 0       0
Jan 01 1970 21:42:14 0       0
Jan 01 1970 21:42:44 0       0
Jan 01 1970 21:43:14 0       0
Jan 01 1970 21:43:44 0       0
Jan 01 1970 21:44:14 0       0
Jan 01 1970 21:44:45 0       0
Jan 01 1970 21:45:15 0       0
Jan 01 1970 21:45:45 0       0
Jan 01 1970 21:46:15 0       0
```

show rmon log

This command displays the entries in the RMON log table.

Format `show rmon log [event-index]`

Mode Privileged Exec

Parameter	Description
`Maximum table size`	Maximum number of entries that the log table can hold.
`Event`	Event index for which the log is generated.
`Description`	A comment describing the event entry for which the log is generated.
`Time`	Time at which the event is generated.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon log

Event   Description                   Time
----------------------------------------------
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon log 1

Maximum table size: 10

Event   Description                   Time
----------------------------------------------
```

show rmon statistics interfaces

This command displays the RMON statistics for the given interfaces.

Format `show rmon statistics interfaces slot/port`

Mode Privileged Exec

Parameter	Description
Port	slot/port
Dropped	Total number of dropped events on the interface.
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good broadcast packets received on the interface.
Multicast	Total number of good multicast packets received on the interface.
CRC Align Errors	Total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.
Collisions	Total number of collisions on the interface.
Undersize Pkts	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Pkts	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
64 Octets	Total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	Total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).
128-255 Octets	Total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	Total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).
512-1023 Octets	Total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	Total number of packets which are between 1024 and 1518 octets in length (excluding framing bits, including FCS octets).
HC Overflow Pkts	Total number of HC overflow packets.
HC Overflow Octets	Total number of HC overflow octets.
HC Overflow Pkts 64 Octets	Total number of HC overflow packets which are 64 octets in length
HC Overflow Pkts 65 - 127 Octets	Total number of HC overflow packets which are between 65 and 127 octets in length.
HC Overflow Pkts 128 - 255 Octets	Total number of HC overflow packets which are between 128 and 255 octets in length.
HC Overflow Pkts 256 - 511 Octets	Total number of HC overflow packets which are between 256 and 511 octets in length.
HC Overflow Pkts 512 - 1023 Octets	Total number of HC overflow packets which are between 512 and 1023 octets in length.
HC Overflow Pkts 1024 - 1518 Octets	Total number of HC overflow packets which are between 1024 and 1518 octets in length.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) # show rmon statistics interfaces 0/1
Port: 0/1
Dropped: 0
Octets: 0  Packets: 0
Broadcast: 0  Multicast: 0
CRC Align Errors: 0  Collisions: 0
Undersize Pkts: 0  Oversize Pkts: 0
Fragments: 0  Jabbers: 0
64 Octets: 0  65 - 127 Octets: 0
128 - 255 Octets: 0  256 - 511 Octets: 0
512 - 1023 Octets: 0  1024 - 1518 Octets: 0
HC Overflow Pkts: 0  HC Pkts: 0
HC Overflow Octets: 0  HC Octets: 0
HC Overflow Pkts 64 Octets: 0  HC Pkts 64 Octets: 0
HC Overflow Pkts 65 - 127 Octets: 0  HC Pkts 65 - 127 Octets: 0
HC Overflow Pkts 128 - 255 Octets: 0  HC Pkts 128 - 255 Octets: 0
HC Overflow Pkts 256 - 511 Octets: 0  HC Pkts 256 - 511 Octets: 0
HC Overflow Pkts 512 - 1023 Octets: 0  HC Pkts 512 - 1023 Octets: 0
HC Overflow Pkts 1024 - 1518 Octets: 0  HC Pkts 1024 - 1518 Octets: 0
```

show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Format `show rmon {hcalarms | hcalarm alarm-index}`

Mode Privileged Exec

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are Absolute Value or Delta Value. The default is Absolute Value.
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are valueNotAvailable, valuePositive, or valueNegative. The default is valueNotAvailable.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are rising, falling, or rising-falling. The default is rising-falling.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.

Parameter	Description
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of thie hcAlarmEntry (while in the active state) and the value was not available. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is monitorHCAlarm.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is volatile.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show rmon hcalarms

Index    OID                       Owner
-----------------------------------------------
1      alarmInterval.1             MibBrowser
2      alarmInterval.1             MibBrowser

(UBNT EdgeSwitch) #show rmon hcalarm 1

Alarm 1
----------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold High: 0
Rising Threshold Low: 1
Rising Threshold Status: Positive
Falling Threshold High: 0
Falling Threshold Low: 1
Falling Threshold Status: Positive
Rising Event: 1
Falling Event: 2
Startup Alarm: Rising-Falling
Owner: MibBrowser
```

Statistics Application Commands

The statistics application gives you the ability to query for statistics on port utilization, flow-based and packet reception on programmable time slots. The statistics application collects the statistics at a configurable time range. You can specify the port number(s) or a range of ports for statistics to be displayed. The configured time range applies to all ports. Detailed statistics are collected between a specified time range in date and time format. You can define the time range as having an absolute time entry and/or a periodic time. For example, you can specify the statistics to be collected and displayed between 9:00 12 NOV 2011 (START) and 21:00 12 NOV 2012 (END) or schedule it on every Mon, Wed, and Fri 9:00 (START) to 21:00 (END).

You can receive the statistics in the following ways:

- User requests through the CLI for a set of counters.
- Configuring the device to display statistics using syslog or email alert. The syslog or email alert messages are sent by the statistics application at END time.

You can configure the device to display statistics on the console. The collected statistics are presented on the console at END time.

stats group

This command creates a new group with the specified id or name and configures the time range and the reporting mechanism for that group.

Format `stats group group-id|name timerange time-range-name reporting list-of-reporting-methods`

Mode Global Config

Parameter	Description
group-id|name	Name of the group of statistics or its identifier to apply on the interface. The range is: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.
time-range-name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
list-of-reporting-methods	Report the statistics to the configured method. The range is: 0. none 1. console 2. syslog 3. e-mail The default is None.

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# stats group received timerange test reporting console email syslog
(UBNT EdgeSwitch) (Config)# stats group received-errors timerange test reporting email syslog
(UBNT EdgeSwitch) (Config)# stats group received-transmitted timerange test reporting none
```

no stats group

This command deletes the configured group.

Format `no stats group group id|name`

Mode Global Config

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# no stats group received
(UBNT EdgeSwitch) (Config)# no stats group received-errors
(UBNT EdgeSwitch) (Config)# no stats group received-transmitted
```

stats flow-based

This command configures flow based statistics rules for the given parameters over the specified time range. Only an IPv4 address is allowed as source and destination IP address.

Format `stats flow-based rule-id timerange time-range-name [{srcip ip-address} {dstip ip-address} {srcmac mac-address} {dstmac mac-address} {srctcpport portid} {dsttcpport portid} {srcudpport portid} {dstudpport portid}]`

Mode Global Config

Parameter	Description
rule-id	The flow-based rule ID. The range is 1 to 16. The default is None.
time-range-name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
srcip *ip-address*	The source IP address.
dstip *ip-address*	The destination IP address.
srcmac *mac-address*	The source MAC address.
dstmac *mac-address*	The destination MAC address.
srctcpport *portid*	The source TCP port number.
dsttcpport *portid*	The destination TCP port number.
srcudpport *portid*	The source UDP port number.
dstudpport *portid*	The destination UDP port number.

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)#stats flow-based 1 timerange test srcip 1.1.1.1 dstip 2.2.2.2 srcmac
1234 dstmac 1234 srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport  123

(UBNT EdgeSwitch) (Config)#stats flow-based 2 timerange test srcip 1.1.1.1 dstip 2.2.2.2
srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport 123
```

no stats flow-based

This command deletes flow-based statistics.

Format `stats flow-based rule-id`

Mode Global Config

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# no stats flow-based 1
(UBNT EdgeSwitch) (Config)# no stats flow-based 2
```

stats flow-based reporting

This command configures the reporting mechanism for all the flow-based rules configured on the system. There is no per flow-based rule reporting mechanism. Setting the reporting method to `none` resets all the reporting methods.

Format `stats flow-based reporting list-of-reporting-methods`

Mode Global Config

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Config)# stats flow-based reporting console email syslog
(UBNT EdgeSwitch) (Config)# stats flow-based reporting email syslog
(UBNT EdgeSwitch) (Config)# stats flow-based reporting none
```

stats group

This command applies the group specified on an interface or interface-range.

Format `stats group group-id|name`

Mode Interface Config

Parameter	Description
group-id	The unique identifier for the group.
name	The name of the group.

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Interface 0/1-0/10)# stats group 1
(UBNT EdgeSwitch) (Interface 0/1-0/10)# stats group 2
```

no stats group

This command deletes the interface or interface-range from the group specified.

Format `no stats group group-id|name`

Mode Interface Config

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Interface 0/1-0/10)# no stats group 1
(UBNT EdgeSwitch) (Interface 0/1-0/10)# no stats group 2
```

stats flow-based

This command applies the flow-based rule specified by the ID on an interface or interface-range.

Format `stats flow-based rule-id`

Mode Interface Config

Parameter	Description
rule-id	The unique identifier for the flow-based rule.

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Interface 0/1-0/10)# stats flow-based 1
(UBNT EdgeSwitch) (Interface 0/1-0/10)# stats flow-based 2
```

no stats flow-based

This command deletes the interface or interface-range from the flow-based rule specified.

Format `no stats flow-based rule-id`

Mode Interface Config

Example: The following shows examples of the command.

```
(UBNT EdgeSwitch) (Interface 0/1-0/10)# no stats flow-based 1
(UBNT EdgeSwitch) (Interface 0/1-0/10)# no stats flow-based 2
```

show stats group

This command displays the configured time range and the interface list for the group specified and shows collected statistics for the specified time-range name on the interface list after the time-range expiry.

Format `show stats group group-id|name`

Mode Privileged EXEC

Parameter	Description
group-id	The unique identifier for the group.
name	The name of the group.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show stats group received

Group: received
Time Range: test
Interface List
-----------------
0/2, 0/4, lag 1

Counter ID                 Interface  Counter Value
-------------------------  ---------  -------------
Rx Total                     0/2        951600
Rx Total                     0/4        304512
Rx Total                    lag 1       0
Rx 64                        0/2        0
Rx 64                        0/4        4758
Rx 64                       lag 1       0
Rx 65to128                   0/2        0
Rx 65to128                   0/4        0
Rx 65to128                  lag 1       0
Rx 128to255                  0/2        4758
Rx 128to255                  0/4        0
Rx 128to255                 lag 1       0
Rx 256to511                  0/2        0
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show stats group port-utilization

Group: port-utilization
Time Range: test
Interface List
--------------
0/2, 0/4, lag 1
Interface  Utilization (%)
---------  ---------------
0/2        0
0/4        0
lag 1      0
```

show stats flow-based

This command displays the configured time range, flow-based rule parameters, and the interface list for the flow specified.

Format `show stats flow-based rule-id|all`

Mode Privileged EXEC

Parameter	Description
rule-id	The unique identifier for the flow-based rule.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show stats flow-based all

Flow based rule Id.............................. 1
Time Range...................................... test
Source IP....................................... 1.1.1.1
Source MAC...................................... 1234
Source TCP Port................................. 123
Source UDP Port................................. 123
Destination IP.................................. 2.2.2.2
Destination MAC................................. 1234
Destination TCP Port............................ 123
Destination UDP Port............................ 123
Interface List
--------------
0/1 - 0/2

Interface  Hit Count
---------  ---------
0/1        100
0/2        0

Flow based rule Id.............................. 2
Time Range...................................... test
Source IP....................................... 1.1.1.1
Source TCP Port................................. 123
Source UDP Port................................. 123
Destination IP.................................. 2.2.2.2
Destination TCP Port............................ 123
Destination UDP Port............................ 123

Interface List
--------------
0/1 - 0/2

Interface  Hit Count
---------  ---------
0/1        100
0/2        0
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show stats flow-based 2

Flow based rule Id.............................. 2
Time Range...................................... test
Source IP....................................... 1.1.1.1
Source TCP Port................................. 123
Source UDP Port................................. 123
Destination IP.................................. 2.2.2.2
Destination TCP Port............................ 123
Destination UDP Port............................ 123
Interface List
--------------
0/1 - 0/2

Interface  Hit Count
---------  ---------
0/1        100
0/2        0
```

Chapter 4: Switching Commands

This chapter describes the switching commands available in the EdgeSwitch CLI.

The chapter contains the following sections:

- **"Port Configuration Commands" on page 197**
- **"Spanning Tree Protocol Commands" on page 203**
- **"VLAN Commands" on page 217**
- **"Private VLAN Commands" on page 224**
- **"Voice VLAN Commands" on page 226**
- **"Provisioning (IEEE 802.1p) Commands" on page 228**
- **"Protected Ports Commands" on page 229**
- **"GARP Commands" on page 231**
- **"GVRP Commands" on page 233**
- **"GMRP Commands" on page 235**
- **"Port-Based Network Access Control Commands" on page 237**
- **"802.1X Supplicant Commands" on page 248**
- **"Storm-Control Commands" on page 251**
- **"Port-Channel/LAG (802.3ad) Commands" on page 256**
- **"Port Mirroring Commands" on page 269**
- **"Static MAC Filtering Commands" on page 271**
- **"DHCP Client Commands" on page 274**
- **"DHCP Snooping Configuration Commands" on page 275**
- **"IGMP Snooping Configuration Commands" on page 281**
- **"IGMP Snooping Querier Commands" on page 287**
- **"Port Security Commands" on page 290**
- **"LLDP (802.1AB) Commands" on page 294**
- **"LLDP-MED Commands" on page 300**
- **"Denial of Service Commands" on page 306**
- **"MAC Database Commands" on page 313**

Note: The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Port Configuration Commands

This section describes the commands you use to view and configure port settings.

interface

This command gives access to Interface Config mode, which lets you enable or modify the operation of an interface (port). You can also specify a range of ports to configure by specifying a starting *slot/port* and an ending *slot/port*, separated by a hyphen.

Format	`interface {slot/port | slot/port-slot/port}`
Mode	Global Config

Example: The following example enters Interface Config mode for port 0/1:

```
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (config)#interface 0/1
(UBNT EdgeSwitch) (interface 0/1)#
```

Example: The following example enters Interface Config mode for ports 0/1 through 0/4:

```
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (config)#interface 0/1-0/4
(UBNT EdgeSwitch) (interface 0/1-0/4)#
```

auto-negotiate

This command enables automatic negotiation on a port or range of ports.

Default	enabled
Format	`auto-negotiate`
Mode	Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Note: Automatic sensing is disabled when automatic negotiation is disabled.

Format	`no auto-negotiate`
Mode	Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports.

Default	enabled
Format	`auto-negotiate all`
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	`no auto-negotiate all`
Mode	Global Config

description

Use this command to create an alphanumeric description of an interface or range of interfaces.

Format	`description description`
Mode	Interface Config

media-type

Use this command to change between fiber and copper mode on the Combo port.

- Combo Port: A port or an interface that can operate in either copper or in fiber mode.
- Copper and Fiber port: A port that uses copper a medium for communication (for example, RJ45 ports). A fiber port uses the fiber optics as a medium for communication (for example, example SFP ports).

Default	Auto-select, SFP preferred
Format	`media-type {auto-select | rj45 | sfp }`
Mode	Interface Config

The following modes are supported by the `media-type` command.

- Auto-select, SFP preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the fiber link takes precedence and the fiber link is up.
- Auto-select, RJ45 preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the copper link takes precedence and the copper link is up.
- SFP: Only the fiber medium works. The copper medium is always down.
- RJ45: Only the copper medium works. The fiber medium is always down.

no media-type

Use this command to revert the `media-type` configuration and configure the default value on the interface.

Format	`no media-type`
Mode	Interface Config

mtu

Use the `mtu` command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the `mtu` command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard EdgeSwitch implementation, the MTU size is a valid integer between 1522–9216 for tagged packets and a valid integer between 1518–9216 for untagged packets.



Note: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see **"ip mtu" on page 324**.

Default	1518 (untagged)
Format	`mtu 1518-12288`
Mode	Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	`no mtu`
Mode	Interface Config

shutdown

This command disables a port or range of ports.



Note: You can use the `shutdown` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown`
Mode	Interface Config

no shutdown

This command enables a port.

Format	`no shutdown`
Mode	Interface Config

shutdown all

This command disables all ports.



Note: You can use the `shutdown all` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown all`
Mode	Global Config

no shutdown all

This command enables all ports.

Format	`no shutdown all`
Mode	Global Config

speed

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The `half-duplex` and `full-duplex` parameters allow you to set the advertised speed for half-duplex and full-duplex modes.

Use the `auto` keyword to enable auto-negotiation on the port. Use the command without the `auto` keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default	Auto-negotiation is enabled.
Format	`speed {auto {40G | 10G | 1000 | 100 | 10} [40G | 10G | 1000 | 100 | 10] [half-duplex | full-duplex] | {40G | 10G | 1000 | 100 | 10} {half-duplex | full-duplex}}`
Mode	Interface Config

speed all

This command sets the speed and duplex setting for all interfaces.

Format	`speed all {100 | 10} {half-duplex | full-duplex}`
Mode	Global Config

show interface media-type

Use this command to display the media-type configuration of the interface.

Format `show interface media-type`

Mode Privileged Exec

The following information is displayed for the command.

Term	Definition
Port	Interface in slot/port format.
Configured Media Type	The media type for the interface. • **auto-select** The media type is automatically selected. The preferred media type is displayed. • **RJ45** RJ45 • **SFP** SFP
Active	Displays the current operational state of the combo port.

Example: The following command shows the command output:

```
(UBNT EdgeSwitch) #show interface media-type

Port       Configured Media Type        Active
---------  ---------------------------  ------
0/21       SFP                          RJ45
0/22       auto-select, SFP preferred   Down
0/23       auto-select, SFP preferred   RJ45
0/24       auto-select, SFP preferred   Down
```

show port

This command displays port information.

Format `show port {intf-range | all}`

Mode Privileged EXEC

Term	Definition
Intf	Interface in slot/port format
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • **Mirror** This port is a monitoring port. For more information, see **"Port Mirroring Commands" on page 269**. • **PC Mbr** This port is a member of a port-channel (LAG). • **Probe** This port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

Example: The following command shows an example of the command output for all ports.

```
(UBNT EdgeSwitch) #show port all

                 Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type   Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
0/1              Enable    Auto       100 Full   Up     Enable  Enable long
0/2              Enable    Auto       100 Full   Up     Enable  Enable long
0/3              Enable    Auto                  Down   Enable  Enable long
0/4              Enable    Auto       100 Full   Up     Enable  Enable long
0/5              Enable    Auto       100 Full   Up     Enable  Enable long
0/6              Enable    Auto       100 Full   Up     Enable  Enable long
0/7              Enable    Auto       100 Full   Up     Enable  Enable long
0/8              Enable    Auto       100 Full   Up     Enable  Enable long
1/1              Enable                          Down   Disable N/A    N/A
1/2              Enable                          Down   Disable N/A    N/A
1/3              Enable                          Down   Disable N/A    N/A
1/4              Enable                          Down   Disable N/A    N/A
1/5              Enable                          Down   Disable N/A    N/A
1/6              Enable                          Down   Disable N/A    N/A
```

Example: The following command shows an example of the command output for a range of ports.

```
(UBNT EdgeSwitch) #show port 0/1-1/6

                 Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type   Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
0/1              Enable    Auto       100 Full   Up     Enable  Enable long
0/2              Enable    Auto       100 Full   Up     Enable  Enable long
0/3              Enable    Auto                  Down   Enable  Enable long
0/4              Enable    Auto       100 Full   Up     Enable  Enable long
0/5              Enable    Auto       100 Full   Up     Enable  Enable long
0/6              Enable    Auto       100 Full   Up     Enable  Enable long
0/7              Enable    Auto       100 Full   Up     Enable  Enable long
0/8              Enable    Auto       100 Full   Up     Enable  Enable long
1/1              Enable                          Down   Disable N/A    N/A
1/2              Enable                          Down   Disable N/A    N/A
1/3              Enable                          Down   Disable N/A    N/A
1/4              Enable                          Down   Disable N/A    N/A
1/5              Enable                          Down   Disable N/A    N/A
1/6              Enable                          Down   Disable N/A    N/A
```

show port advertise

Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface. It also displays priority Resolution for speed and duplex as per 802.3 Annex 28B.3. It displays the Auto negotiation state, Phy Master/Slave Clock configuration, and Link state of the port.

If the link is down, the Clock is displayed as `No Link`, and a dash is displayed against the Oper Peer advertisement, and Priority Resolution. If Auto negotiation is disabled, then the admin Local Link advertisement, operational local link advertisement, operational peer advertisement, and Priority resolution fields are not displayed.

If this command is executed without the optional *`slot/port`* parameter, then it displays the Auto-negotiation state and operational Local link advertisement for all the ports. Operational link advertisement will display speed only if it is supported by both local as well as link partner. If auto-negotiation is disabled, then operational local link advertisement is not displayed.

Format	`show port advertise [`*`slot`*`/`*`port`*`]`
Mode	Privileged EXEC

Example: The following commands show the command output with and without the optional parameter:

```
(UBNT EdgeSwitch) #show port advertise 0/1

Port: 0/1
Type: Gigabit - Level
Link State: Down
Auto Negotiation: Enabled
Clock: Auto
                              1000f 1000h 100f 100h 10f 10h
                              ----- ----- ---- ---- --- ---
Admin Local Link Advertisement no    no    yes  no   yes no
Oper Local Link Advertisement  no    no    yes  no   yes no
Oper Peer Advertisement              no      no     yes    yes    yes yes
Priority Resolution            -     -     yes  -    -   -

(UBNT EdgeSwitch) #show port advertise

Port      Type                                Neg      Operational Link Advertisement
--------- ------------------------------ ----------- ------------------------------
0/1   Gigabit - Level                    Enabled  1000f, 100f, 100h, 10f, 10h
0/2   Gigabit - Level                    Enabled  1000f, 100f, 100h, 10f, 10h
0/3   Gigabit - Level                    Enabled  1000f, 100f, 100h, 10f, 10h
```

show port description

This command displays the interface description. Instead of `slot/port`, you can use `lag lag-intf-num` as an alternate way to specify the LAG interface, where `lag-intf-num` is the LAG port number.

Format	`show port description slot/port`
Mode	Privileged EXEC

Term	Definition
Interface	Interface in slot/port format.
ifIndex	The interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the command **"description" on page 197**.
MAC address	The MAC address of the port. The format is six 2-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show port description 0/1

Interface...........0/1
ifIndex.............1
Description.........
MAC address.........00:10:18:82:0C:10
Bit Offset Val......1
```

Spanning Tree Protocol Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.



Notes:

- STP is enabled on the switch and on all ports and LAGs by default.
- If STP is disabled, the system does not forward BPDU messages.

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	enabled
Format	`spanning-tree`
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	`no spanning-tree`
Mode	Global Config

spanning-tree auto-edge

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

Default	Enabled
Format	`spanning-tree auto-edge`
Mode	Interface Config

no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree auto-edge`
Mode	Interface Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *slot*/*port* parameter to transmit a BPDU from a specified interface, or use the `all` keyword to transmit RST or MST BPDUs from all interfaces. Because this command forces the BPDU transmission when executed, the command does not change the system configuration, and does not have a corresponding `no` form.

Format	`spanning-tree bpdumigrationcheck {`*slot*`/`*port*` | all}`
Mode	Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *name* is a string of up to 32 characters.

Default	base MAC address in hexadecimal notation
Format	`spanning-tree configuration name` *name*
Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	`no spanning-tree configuration name`
Mode	Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default	0
Format	`spanning-tree configuration revision` *`0-65535`*
Mode	Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format	`no spanning-tree configuration revision`
Mode	Global Config

spanning-tree cost

Use this command to configure the external path cost for port used by a MST instance. When the `auto` keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a *`cost`* value from 1–200000000.

Default	auto
Format	`spanning-tree cost {`*`cost`*` | auto}`
Mode	Interface Config

no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree cost`
Mode	Interface Config

spanning-tree edgeport

This command specifies that an interface (or range of interfaces) is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format	`spanning-tree edgeport`
Mode	Interface Config

no spanning-tree edgeport

This command specifies that this port is not an edge port within the common and internal spanning tree.

Format	`no spanning-tree edgeport`
Mode	Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default	802.1s
Format	`spanning-tree forceversion {802.1d | 802.1s | 802.1w}`
Mode	Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Format	`no spanning-tree forceversion`
Mode	Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The value in seconds ranges from 4 to 30, with the value being greater than or equal to *(Bridge Max Age / 2) + 1*.

Default	15
Format	`spanning-tree forward-time 4-30`
Mode	Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree forward-time`
Mode	Global Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The value is in seconds range from 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

Default	20
Format	`spanning-tree max-age 6-40`
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-age`
Mode	Global Config

spanning-tree max-hops

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree.

Default	20
Format	`spanning-tree max-hops 6-40`
Mode	Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-hops`
Mode	Global Config

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *mstid* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, the configurations are done for the common and internal spanning tree instance.

If you specify the `cost` option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter. You can set the path cost as a number in the range of 1 to 200000000 or `auto`. If you select `auto` the path cost value is set based on Link Speed.

If you specify the `port-priority` option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default	• `cost`: auto • `port-priority`: 128
Format	`spanning-tree mst` *`mstid`* `{{cost` *`1-200000000`* `| auto} | port-priority` *`0-240`*`}`
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an *mstid* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, you are configuring the common and internal spanning tree instance.

If you specify `cost`, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value, i.e., a path cost value based on the Link Speed.

If you specify `port-priority`, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value.

Format	`no spanning-tree mst` *`mstid`* `{cost | port-priority}`
Mode	Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter *mstid* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default	none
Format	`spanning-tree mst instance` *`mstid`*
Mode	Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format	`no spanning-tree mst instance mstid`
Mode	Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 4094.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 4094. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default	32768
Format	`spanning-tree mst priority mstid 0-4094`
Mode	Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the mstid, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree mst priority mstid`
Mode	Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter *mstid* is a multiple spanning tree instance identifier, in the range of 0 to 4094, that corresponds to the desired existing multiple spanning tree instance. The *vlanid* can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs in the range 1 to 4093, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). Spaces and zeros are not permitted. The VLAN IDs may or may not exist in the system.

Format	`spanning-tree mst vlan mstid vlanid`
Mode	Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format	`no spanning-tree mst vlan mstid vlanid`
Mode	Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled for use by spanning tree.

Default enabled

Format `spanning-tree port mode`

Mode Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled, disabling the port for use by spanning tree.

Format `no spanning-tree port mode`

Mode Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default enabled

Format `spanning-tree port mode all`

Mode Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format `no spanning-tree port mode all`

Mode Global Config

spanning-tree tcnguard

Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Default Enabled

Format `spanning-tree tcnguard`

Mode Interface Config

no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format `no spanning-tree tcnguard`

Mode Interface Config

spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter.

Default 6

Format `spanning-tree transmit` *`hold-count`*

Mode Global Config

Parameter	Description
`hold-count`	The Bridge Tx hold-count parameter. The value is an integer between 1 and 10.

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format `show spanning-tree`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It consists of the bridge priority and the bridge's base MAC address.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change in Progress	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge, consisting of the bridge priority and the bridge's base MAC address.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST.
Bridge Max Age	Derived value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Forwarding Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
CST Regional Root	Bridge Identifier of the CST Regional Root, consisting of the bridge priority and the bridge's base MAC address.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show spanning-tree

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:00:10:18:48:FC:07
Time Since Topology Change................... 8 day 3 hr 22 min 37 sec
Topology Change Count........................ 0
Topology Change in progress.................. FALSE
Designated Root.............................. 80:00:00:10:18:48:FC:07
Root Path Cost............................... 0
Root Port Identifier......................... 00:00
Bridge Max Age............................... 20
Bridge Max Hops.............................. 20
Bridge Tx Hold Count......................... 6
Bridge Forwarding Delay...................... 15
Hello Time................................... 2
Bridge Hold Time............................. 6
CST Regional Root............................ 80:00:00:10:18:48:FC:07
Regional Root Path Cost...................... 0

     Associated FIDs          Associated VLANs
     ---------------          ----------------

(UBNT EdgeSwitch) #
```

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format `show spanning-tree brief`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It consists of the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show spanning-tree brief

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:00:10:18:48:FC:07
Bridge Max Age............................... 20
Bridge Max Hops.............................. 20
Bridge Hello Time............................ 2
Bridge Forward Delay......................... 15
Bridge Hold Time............................. 6

(UBNT EdgeSwitch) #
```

show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *slot/port* is the desired switch port. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface, where *lag-intf-num* is the LAG port number. The following details are displayed on execution of the command.

Format `show spanning-tree interface` *slot/port*|`lag` *lag-intf-num*

Mode Privileged EXEC, User EXEC

Term	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for edge delay time, to become an edge port and transition to forwarding faster.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) >show spanning-tree interface 0/1

Hello Time..................................... Not Configured
Port Mode...................................... Enabled
BPDU Guard Effect.............................. Disabled
Root Guard..................................... FALSE
Loop Guard..................................... FALSE
TCN Guard...................................... FALSE
BPDU Filter Mode............................... Disabled
BPDU Flood Mode................................ Disabled
Auto Edge...................................... TRUE
Port Up Time Since Counters Last Cleared....... 8 day 3 hr 39 min 58 sec
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0

(UBNT EdgeSwitch) >
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) >show spanning-tree interface lag 1

Hello Time..................................... Not Configured
Port Mode...................................... Enabled
BPDU Guard Effect.............................. Disabled
Root Guard..................................... FALSE
Loop Guard..................................... FALSE
TCN Guard...................................... FALSE
BPDU Filter Mode............................... Disabled
BPDU Flood Mode................................ Disabled
Auto Edge...................................... TRUE
Port Up Time Since Counters Last Cleared....... 8 day 3 hr 42 min 5 sec
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0

(UBNT EdgeSwitch) >
```

show spanning-tree mst detailed

This command displays the detailed settings for an MST instance.

Format `show spanning-tree mst detailed` *`mstid`*

Mode
- Privileged EXEC
- User EXEC

Parameter	Description
`mstid`	A multiple spanning tree instance identifier. The value is 0–4094.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) >show spanning-tree mst detailed 0

MST Instance ID.............................. 0
MST Bridge Priority.......................... 32768
MST Bridge Identifier........................ 80:00:00:10:18:48:FC:07
Time Since Topology Change................... 8 day 3 hr 47 min 7 sec
Topology Change Count........................ 0
Topology Change in progress.................. FALSE
Designated Root.............................. 80:00:00:10:18:48:FC:07
Root Path Cost............................... 0
Root Port Identifier......................... 00:00

     Associated FIDs           Associated VLANs
     ---------------           ----------------
```

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The *slot/port* is the desired switch port. Instead of *slot/port*, you can use lag *lag-intf-num* as an alternate way to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format show spanning-tree mst port detailed *mstid slot/port* | lag *lag-intf-num*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID	The ID of the existing multiple spanning tree (MST) instance identifier. The value is 0-4094.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *slot/port* is the desired switch port. In this case, the following are displayed.

Term	Definition
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.

Term	Definition
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.

Example: The following shows example CLI display output for the command in slot/port format.

```
(UBNT EdgeSwitch) >show spanning-tree mst port detailed 0 0/1

Port Identifier.............................. 80:01
Port Priority................................ 128
Port Forwarding State........................ Disabled
Port Role.................................... Disabled
Auto-calculate Port Path Cost................ Enabled
Port Path Cost............................... 0
Auto-Calculate External Port Path Cost....... Enabled
External Port Path Cost...................... 0
Designated Root.............................. 80:00:00:10:18:48:FC:07
Root Path Cost............................... 0
Designated Bridge............................ 80:00:00:10:18:48:FC:07
Designated Port Identifier................... 00:00
Topology Change Acknowledge.................. FALSE
Hello Time................................... 2
Edge Port.................................... FALSE
Edge Port Status............................. FALSE
Point to Point MAC Status.................... TRUE
CST Regional Root............................ 80:00:00:10:18:48:FC:07
CST Internal Root Path Cost.................. 0
Loop Inconsistent State...................... FALSE
Transitions Into Loop Inconsistent State..... 0
Transitions Out Of Loop Inconsistent State.... 0
```

Example: The following shows example CLI display output for the command using a LAG interface number.

```
(UBNT EdgeSwitch) >show spanning-tree mst port detailed 0 lag 1

Port Identifier.............................. 60:42
Port Priority................................ 96
Port Forwarding State........................ Disabled
Port Role.................................... Disabled
```

```
Auto-calculate Port Path Cost..................... Enabled
Port Path Cost.................................... 0
Auto-Calculate External Port Path Cost......... Enabled
External Port Path Cost........................... 0
Designated Root................................... 80:00:00:10:18:48:FC:07
Root Path Cost.................................... 0
Designated Bridge................................. 80:00:00:10:18:48:FC:07
Designated Port Identifier........................ 00:00
Topology Change Acknowledge....................... FALSE
Hello Time........................................ 2
Edge Port......................................... FALSE
Edge Port Status.................................. FALSE
Point to Point MAC Status......................... TRUE
CST Regional Root................................. 80:00:00:10:18:48:FC:07
CST Internal Root Path Cost....................... 0
Loop Inconsistent State........................... FALSE
Transitions Into Loop Inconsistent State....... 0
Transitions Out Of Loop Inconsistent State..... 0
--More-- or (q)uit
```

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *mstid* indicates a particular MST instance. The parameter {*slot/port*|all} indicates the desired switch port or all ports. Instead of *slot/port*, you can use lag *lag-intf-num* as an alternate way to specify the LAG interface, where *lag-intf-num* is the LAG port number.

If you specify 0 (defined as the default CIST ID) as the *mstid*, the status summary displays for one or all ports within the common and internal spanning tree.

Format show spanning-tree mst port summary *mstid* {*slot/port* | lag *lag-intf-num* | all}

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID	The MST instance associated with this port.
Interface	The interface in slot/port format.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

Example: The following shows example CLI display output for the command in slot/port format.

```
(UBNT EdgeSwitch) >show spanning-tree mst port summary 0 0/1

MST Instance ID.............................. CST

           STP                 STP           Port
Interface  Mode   Type         State         Role       Desc
---------- -------- ------- ----------------- ---------- ----------
0/1       Enabled          Disabled          Disabled
```

Example: The following shows example CLI display output for the command using a LAG interface number.

```
(UBNT EdgeSwitch) >show spanning-tree mst port summary 0 lag 1

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type         State           Role       Desc
--------- -------- ------- ----------------- ---------- ----------
3/1       Enabled          Disabled          Disabled
```

show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format `show spanning-tree mst port summary mstid active`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID	The ID of the existing MST instance.
Interface	The interface in slot/port format.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) >show spanning-tree mst port summary 0 active

            STP                  STP            Port
Interface   Mode   Type         State           Role       Desc
--------- -------- ------- ----------------- ---------- ---------
```

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format `show spanning-tree mst summary`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • Associated FIDs • Associated VLANs	 • List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format `show spanning-tree summary`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) >show spanning-tree summary

Spanning Tree Adminmode........... Enabled
Spanning Tree Version............. IEEE 802.1s
BPDU Guard Mode................... Disabled
BPDU Filter Mode.................. Disabled
Configuration Name................ ****
Configuration Revision Level...... ****
Configuration Digest Key.......... ****
Configuration Format Selector..... 0
No MST instances to display.
```

show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The *vlanid* corresponds to an existing VLAN ID.

Format `show spanning-tree vlan vlanid`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
VLAN Identifier	The VLANs associated with the selected MST instance.
Associated Instance	Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) >show spanning-tree vlan 1

VLAN Identifier.............................. 1
Associated Instance.......................... CST
```

VLAN Commands

This section describes the commands you use to configure VLAN settings.

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format	`vlan database`
Mode	Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default	1
Format	`network mgmt_vlan` *`1-4093`*
Mode	Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format	`no network mgmt_vlan`
Mode	Privileged EXEC

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4093.

Format	`vlan` *`2-4093`*
Mode	VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2-4093.

Format	`no vlan` *`2-4093`*
Mode	VLAN Config

vlan acceptframe

This command sets the frame acceptance mode on an interface or range of interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. For Admit Untagged Only mode, only untagged frames are accepted on this interface; tagged frames are discarded. With any option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all
Format	`vlan acceptframe {admituntaggedonly | vlanonly | all}`
Mode	Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format	`no vlan acceptframe`
Mode	Interface Config

vlan ingressfilter

This command enables ingress filtering on an interface or range of interfaces. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	`vlan ingressfilter`
Mode	Interface Config

no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	`no vlan ingressfilter`
Mode	Interface Config

vlan internal allocation

Use this command to configure which VLAN IDs to use for port-based routing interfaces. When a port-based routing interface is created, an unused VLAN ID is assigned internally.

Format	`vlan internal allocation {base` *`vlan-id`* `| policy ascending | policy descending}`
Mode	Global Config

Parameter	Description
`base` *`vlan-id`*	The first VLAN ID to be assigned to a port-based routing interface.
`policy ascending`	VLAN IDs assigned to port-based routing interfaces start at the base and increase in value
`policy descending`	VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value

vlan makestatic

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Format	`vlan makestatic` *`2-4093`*
Mode	VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

Default	VLAN ID 1 - default other VLANS - blank string
Format	`vlan name` *`1-4093 name`*
Mode	VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format	`no vlan name` *`1-4093`*
Mode	VLAN Config

vlan participation

This command configures the degree of participation for a specific interface or range of interfaces in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format `vlan participation {exclude | include | auto} 1-4093`

Mode Interface Config

Participation options are:

Option	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format `vlan participation all {exclude | include | auto} 1-4093`

Mode Global Config

You can use the following participation options:

Option	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default all

Format `vlan port acceptframe all {vlanonly | admituntaggedonly |all}`

Mode Global Config

The modes are defined as follows:

Mode	Definition
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit Untagged Only mode	VLAN-tagged and priority tagged frames received on this interface are discarded.
Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN specification.

Format `no vlan port acceptframe all`

Mode Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	`vlan port ingressfilter all`
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	`no vlan port ingressfilter all`
Mode	Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Format	`vlan port pvid all` *`1-4093`*
Mode	Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format	`no vlan port pvid all`
Mode	Global Config

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`vlan port tagging all` *`1-4093`*
Mode	Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`no vlan port tagging all`
Mode	Global Config

vlan pvid

This command changes the VLAN ID on an interface or range of interfaces.

Default	1
Format	`vlan pvid` *`1-4093`*
Mode	• Interface Config • Interface Range Config

no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Format `no vlan pvid`

Mode Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `vlan tagging 1-4093`

Mode Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan tagging 1-4093`

Mode Interface Config

vlan association mac

This command associates a MAC address to a VLAN.

Format `vlan association mac macaddr vlanid`

Mode VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format `no vlan association mac macaddr`

Mode VLAN database

show vlan

This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format `show vlan {vlanid|private-vlan [type]}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Primary	Primary VLAN identifier. The range of the VLAN ID is 1 to 4093.
Secondary	Secondary VLAN identifier.
Type	Secondary VLAN type (community, isolated, or primary).
Ports	Ports which are associated with a private VLAN.
VLAN ID	The VLAN identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has the name `Default`. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.
Interface	Interface in slot/port format. It is possible to set the parameters for all ports by using the selectors on the top line.

Term	Definition
Current	The degree of participation of this port in this VLAN. The permissible values are: • **Include** This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • **Include** This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. • **Tagged** Transmit traffic for this VLAN as tagged frames. • **Untagged** Transmit traffic for this VLAN as untagged frames.

show vlan internal usage

This command displays information about the VLAN ID allocation on the switch.

Format `show vlan internal usage`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Base VLAN ID	Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.
Allocation policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.

show vlan brief

This command displays a list of all configured VLANs.

Format `show vlan brief`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has the name "Default". This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format `show vlan port {slot/port | all}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface in slot/port format. It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.

Private VLAN Commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer-2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer-2 network.

switchport private-vlan

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format `switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list}`

Mode Interface Config

Parameter	Description
`host-association`	Defines the VLAN association for community or host ports.
`primary-vlan-id`	Primary VLAN ID of a private VLAN.
`secondary-vlan-id`	Secondary (isolated or community) VLAN ID of a private VLAN.
`mapping`	Defines the private VLAN mapping for promiscuous ports.
`add`	Associates the secondary VLAN with the primary one.
`remove`	Deletes the secondary VLANs from the primary VLAN association.
`secondary-vlan-list`	A list of secondary VLANs to be mapped to a primary VLAN.

no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format `no switchport private-vlan {host-association|mapping}`

Mode Interface Config

switchport mode private-vlan

This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Default general

Format `switchport mode private-vlan {host|promiscuous}`

Mode Interface Config

Term	Definition
host	Configures an interface as a private VLAN host port. It can be either isolated or community port depending on the secondary VLAN it is associated with.
promiscuous	Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.

no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Format `no switchport mode private-vlan`

Mode Interface Config

private-vlan

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format `private-vlan {association [add|remove] community | isolated | primary}`

Mode VLAN Config

Parameter	Description
`association`	Associates the primary and secondary VLAN.
`community`	Designates a VLAN as a community VLAN.
`isolated`	Designates a VLAN as the isolated VLAN.
`primary`	Designates a VLAN as the primary VLAN.

no private-vlan

This command restores normal VLAN configuration.

Format `no private-vlan {association}`

Mode VLAN Config

Voice VLAN Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default disabled

Format `voice vlan`

Mode Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format `no voice vlan`

Mode Global Config

voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default disabled

Format `voice vlan {vlan-id` *`id`* `| dot1p` *`priority`* `| none | untagged}`

Mode Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	Description
`vlan-id` *`id`*	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID range is 1-4093 (the maximum supported by the platform).
`dot1p` *`priority`*	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid priority range is 0 to 7.
`none`	Allow the IP phone to use its own configuration to send untagged voice traffic.
`untagged`	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format `no voice vlan`

Mode Interface Config

voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default trust

Format `voice vlan data priority {untrust | trust}`

Mode Interface Config

show voice vlan

Format `show voice vlan [interface {slot/port | all}]`

Mode Privileged EXEC

When the `interface` parameter is not specified, only the global mode of the Voice VLAN is displayed.

Term	Definition
Administrative Mode	The Global Voice VLAN mode.

When the `interface` parameter is specified, the following information is displayed:

Term	Definition
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID.
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format	`vlan port priority all` *priority*
Mode	Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default	0
Format	`vlan priority` *priority*
Mode	Interface Config

Protected Ports Commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

Use this command to create a protected port group. The *groupid* parameter identifies the set of protected ports. Use the `name` *name* pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Note: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	`switchport protected` *groupid* `name` *name*
Mode	Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The *groupid* parameter identifies the set of protected ports.

Format	`no switchport protected` *groupid*
Mode	Global Config

switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

Note: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	`switchport protected` *groupid*
Mode	Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format	`no switchport protected` *groupid*
Mode	Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format `show switchport protected groupid`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with groupid. If no port is configured as protected for this group, this field is blank.

show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the group ID.

Format `show interfaces switchport slot/port groupid`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates whether the interface is protected or not (TRUE or FALSE). If the group is multiple groups then it shows TRUE in Group `groupid`.

GARP Commands

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or reregistering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default	20
Format	`set garp timer join` *`10-100`*
Mode	• Interface Config • Global Config

no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer join`
Mode	• Interface Config • Global Config

set garp timer leave

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds. The leave time must be greater than or equal to three times the join time.

Default	60
Format	`set garp timer leave` *`20-600`*
Mode	• Interface Config • Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leave`
Mode	• Interface Config • Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode), or on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

Default	1000
Format	`set garp timer leaveall 200-6000`
Mode	• Interface Config • Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leaveall`
Mode	• Interface Config • Global Config

show garp

This command displays GARP information.

Format	`show garp`
Mode	• Privileged EXEC • User EXEC

Term	Definition
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP Commands

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.



Note: If GVRP is disabled, the system does not forward GVRP messages.

set gvrp adminmode

This command enables GVRP on the system.

Default	disabled
Format	`set gvrp adminmode`
Mode	Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format	`no set gvrp adminmode`
Mode	Privileged EXEC

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode), a range of ports (Interface Range mode), or all ports (Global Config mode).

Default	disabled
Format	`set gvrp interfacemode`
Mode	• Interface Config • Interface Range • Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format	`no set gvrp interfacemode`
Mode	• Interface Config • Global Config

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gvrp configuration {`*`slot/port`*` | all}`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	Interface in slot/port format.
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).

Term	Definition
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP Commands

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP Snooping, GMRP helps control the flooding of multicast packets. GMRP-enabled switches dynamically register and deregister group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.



Note: If GMRP is disabled, the system does not forward GMRP messages.

set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default	disabled
Format	`set gmrp adminmode`
Mode	Privileged EXEC

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format	`no set gmrp adminmode`
Mode	Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode), a range of interfaces, or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default	disabled
Format	`set gmrp interfacemode`
Mode	• Interface Config • Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format	`no set gmrp interfacemode`
Mode	• Interface Config • Global Config

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gmrp configuration {`*`slot/port`*` | all}`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	The slot/port of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

This command displays the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table gmrp`

Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is six 2-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (IEEE 802.1X). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- **ias** Uses the internal authentication server users database for authentication. This method can be used in conjunction with any one of the existing methods like `local`, `radius`, etc.
- **local** Uses the local username database for authentication.
- **none** Uses no authentication.
- **radius** Uses the list of all RADIUS servers for authentication.

Format	`aaa authentication dot1x default {[ias]|[method1 [method2 [method3]]]}`
Mode	Global Config

Example: The following is an example of the command.

```
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure
(UBNT EdgeSwitch) (Config)#aaa authentication dot1x default ias none
(UBNT EdgeSwitch) (Config)#aaa authentication dot1x default ias local radius none
```

clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format	`clear dot1x statistics {slot/port | all}`
Mode	Privileged EXEC

clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format	`clear dot1x authentication-history [slot/port]`
Mode	Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format	`clear radius statistics`
Mode	Privileged EXEC

dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Default	disabled
Format	`dot1x eapolflood`
Mode	Global Config

no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format	`no dot1x eapolflood`
Mode	Global Config

dot1x guest-vlan

This command configures VLAN as guest vlan on an interface or a range of interfaces. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Default	disabled
Format	`dot1x guest-vlan` *`vlan-id`*
Mode	Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default	disabled
Format	`no dot1x guest-vlan`
Mode	Interface Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or MAC-based. If the control mode is not auto or MAC-based, an error will be returned.

Format	`dot1x initialize` *`slot/port`*
Mode	Privileged EXEC

dot1x max-req

This command sets the maximum number of times the authenticator state machine on an interface or range of interfaces will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The *`count`* value must be in the range 1–10.

Default	2
Format	`dot1x max-req` *`count`*
Mode	Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format	`no dot1x max-req`
Mode	Interface Config

dot1x max-users

Use this command to set the maximum number of clients supported on an interface or range of interfaces when MAC-based 802.1X authentication is enabled on the port. The maximum users supported per port is dependent on the product. The *`count`* value is in the range 1–48.

Default	16
Format	`dot1x max-users count`
Mode	Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format	`no dot1x max-users`
Mode	Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the `force-unauthorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the `force-authorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the `auto` parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based 802.1X authentication is enabled on the port.

Default	auto
Format	`dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format	`no dot1x port-control`
Mode	Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select `force-unauthorized` to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select `force-authorized` to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select `auto` to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based 802.1X authentication is enabled on the port.

Default	auto
Format	`dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format	`no dot1x port-control all`
Mode	Global Config

dot1x mac-auth-bypass

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones – to authenticate to the network using the client MAC address as an identifier.

Default	disabled
Format	`dot1x mac-auth-bypass`
Mode	Interface Config

no dot1x mac-auth-bypass

This command sets the MAB mode on the ports to the default value.

Format	`no dot1x mac-auth-bypass`
Mode	Interface Config

dot1x re-authenticate

This command begins the reauthentication sequence on the specified port. This command is only valid if the control mode for the specified port is `auto` or `mac-based`. If the control mode is not `auto` or `mac-based`, an error will be returned.

Format	`dot1x re-authenticate` *`slot/port`*
Mode	Privileged EXEC

dot1x re-authentication

This command enables reauthentication of the supplicant for the specified interface or range of interfaces.

Default	disabled
Format	`dot1x re-authentication`
Mode	Interface Config

no dot1x re-authentication

This command disables reauthentication of the supplicant for the specified port.

Format	`no dot1x re-authentication`
Mode	Interface Config

dot1x system-auth-control

Use this command to enable the 802.1X authentication support on the switch. While disabled, the 802.1X configuration is retained and can be changed, but is not activated.

Default	disabled
Format	`dot1x system-auth-control`
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the 802.1X authentication support on the switch.

Format	`no dot1x system-auth-control`
Mode	Global Config

dot1x system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default	disabled
Format	`dot1x system-auth-control monitor`
Mode	Global Config

no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Format `no dot1x system-auth-control monitor`

Mode Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on an interface or range of interfaces. Depending on the parameter used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Parameter	Definition
`guest-vlan-period`	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
`reauth-period`	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The `reauth-period` valid range is 1–65535.
`quiet-period`	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The valid range is 0–65535.
`tx-period`	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The `quiet-period` valid range is 1–65535.
`supp-timeout`	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The `supp-timeout` valid range is 1–65535.
`server-timeout`	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The `server-timeout` valid range is 1–65535.

Default
- `guest-vlan-period`: 90 seconds
- `reauth-period`: 3600 seconds
- `quiet-period`: 60 seconds
- `tx-period`: 30 seconds
- `supp-timeout`: 30 seconds
- `server-timeout`: 30 seconds

Format `dot1x timeout {{guest-vlan-period` *`seconds`*`} | {reauth-period` *`seconds`*`} | {quiet-period` *`seconds`*`} | {tx-period` *`seconds`*`} | {supp-timeout` *`seconds`*`} | {server-timeout` *`seconds`*`}}`

Mode Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format `no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}`

Mode Interface Config

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface or range of interfaces. The unauthenticated VLAN ID can be a valid VLAN ID from 0 to the maximum supported VLAN ID (4093 for EdgeSwitch). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0; i.e., invalid and not operational.

Default 0

Format `dot1x unauthenticated-vlan` *`vlan-id`*

Mode Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated VLAN associated with the port to its default value.

Format	`no dot1x unauthenticated-vlan`
Mode	Interface Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The user parameter must be a configured user.

Format	`dot1x user user {slot/port | all}`
Mode	Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format	`no dot1x user user {slot/port | all}`
Mode	Global Config

show authentication methods

Use this command to display information about the authentication methods.

Format	`show authentication methods`
Mode	Privileged EXEC

Term	Definition
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.
Method 3	The third method in the specified authentication login list, if any.

Example: The following example displays the authentication configuration.

```
(UBNT EdgeSwitch)#show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local
networkList         :  local

Enable Authentication Method Lists
----------------------------------
enableList          :  enable   none
enableNetList       :  enable   deny

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableNetList
SSH      networkList          enableNetList

HTTPS       :local
HTTP        :local
DOT1X       :
```

show dot1x

This command is used to show a summary of the global 802.1X configuration, summary information of the 802.1X configuration for a specified port or all ports, the detailed 802.1X configuration for a specified port and the 802.1X statistics for a specified port, depending on the tokens used.

Format	`show dot1x [{summary {slot/port | all} | detail slot/port | statistics slot/port]`
Mode	Privileged EXEC

If you do not use the optional parameters *slot/port* or *vlanid*, the command displays the global 802.1X mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Term	Definition
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the 802.1X Monitor mode on the switch is enabled or disabled.

If you use the optional parameter `summary {slot/port | all}`, the 802.1X configuration for the specified port or all ports are displayed.

Term	Definition
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Indicates whether reauthentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

Example: The following shows example CLI display output for the command `show dot1x summary 0/1`.

```
                              Operating
Interface     Control Mode    Control Mode     Port Status
---------     ------------    ------------     ------------
0/1           auto            auto             Authorized
```

If you use the optional parameter `detail slot/port`, the detailed 802.1X configuration for the specified port is displayed.

Term	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the 802.1X specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized, force-authorized, auto, and mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.

Term	Definition
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Configured MAB Mode	The administrative mode of the MAC authentication bypass feature on the switch.
Operational MAB Mode	The operational mode of the MAC authentication bypass feature on the switch. MAB might be administratively enabled but not operational if the control mode is not MAC based.
Vlan-ID	The VLAN assigned to the port by the RADIUS server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by 802.1X. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are 'True" or "False".
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
EAPOL Flood Mode Enabled	Indicates whether the EAPOL flood support is enabled on the switch. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based 802.1X authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show dot1x detail 0/3

Port..................................... 0/1
Protocol Version......................... 1
PAE Capabilities......................... Authenticator
Control Mode............................. auto
Authenticator PAE State.................. Initialize
Backend Authentication State............. Initialize
Quiet Period (secs)...................... 60
Transmit Period (secs)................... 30
Guest VLAN ID............................ 0
Guest VLAN Period (secs)................. 90
Supplicant Timeout (secs)................ 30
```

```
Server Timeout (secs)..... 30
Maximum Requests..... 2
Configured MAB Mode..... Enabled
Operational MAB Mode..... Disabled
VLAN Id..... 0
VLAN Assigned Reason..... Not Assigned
Reauthentication Period (secs)..... 3600
Reauthentication Enabled..... FALSE
Key Transmission Enabled..... FALSE
EAPOL flood Mode Enabled..... FALSE
Control Direction..... both
Maximum Users..... 16
Unauthenticated VLAN ID..... 0
Session Timeout..... 0
Session Termination Action..... Default
```

For each client authenticated on the port, the `show dot1x detail slot/port` command will display the following MAC-based 802.1X parameters if the port-control mode for that specific port is MAC-based.

Term	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the RADIUS server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter `statistics slot/port`, the following 802.1X statistics for the specified port appear.

Term	Definition
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful 802.1X authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format `show dot1x authentication-history {slot/port | all} [failed-auth-only] [detail]`

Mode Privileged EXEC

Term	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
Mac-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Montior Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

Format `show dot1x clients {slot/port | all}`

Mode Privileged EXEC

Term	Definition
Clients Authenticated using Monitor Mode	Indicates the number of the 802.1X clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of 802.1X clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format `show dot1x users slot/port`

Mode Privileged EXEC

Term	Definition
Users	Users configured locally to have access to the specified port.

802.1X Supplicant Commands

EdgeSwitch supports 802.1X ("dot1x") supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port's 802.1X role. The port can serve as either a supplicant or an authenticator.

Format `dot1x pae {supplicant | authenticator}`

Mode Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port's attribute needs to be moved from authenticator to supplicant or from supplicant to authenticator, use this command.

Format `dot1x supplicant port-control {auto | force-authorized | force_unauthorized}`

Mode Interface Config

Parameter	Description
`auto`	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
`force-authorized`	Sets the authorization state of the port to Authorized, bypassing the authentication process.
`force-unauthorized`	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default auto

Format `no dot1x supplicant port-control`

Mode Interface Config

dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

Default 3

Format `dot1x supplicant max-start` *`1-10`*

Mode Interface Config

no dot1x supplicant max-start

This command sets the max-start value to the default.

Format `no dot1x supplicant max-start`

Mode Interface Config

dot1x supplicant timeout start-period

This command configures the `start-period` timer interval to wait for the EAP identity request from the authenticator.

Default 30 seconds

Format `dot1x supplicant timeout start-period` *`1-65535`*

Mode Interface Config

no dot1x supplicant timeout start-period

This command sets the `start-period` value to the default.

Format	`no dot1x supplicant timeout start-period`
Mode	Interface Config

dot1x supplicant timeout held-period

This command configures the held period timer interval to wait for the next authentication on previous authentication fail.

Default	60 seconds
Format	`dot1x supplicant timeout held-period` *1-65535*
Mode	Interface Config

no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Format	`no dot1x supplicant timeout held-period`
Mode	Interface Config

dot1x supplicant timeout auth-period

This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator.

Default	30 seconds
Format	`dot1x supplicant timeout auth-period` *1-65535*
Mode	Interface Config

no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Format	`no dot1x supplicant timeout auth-period`
Mode	Interface Config

dot1x supplicant user

Use this command to map the given user to the port.

Format	`dot1x supplicant user`
Mode	Interface Config

show dot1x statistics

This command displays the 802.1X port statistics in detail.

Format	`show dot1x statistics` *slot/port*
Mode	• Privileged EXEC • User EXEC

Term	Definition
EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.
EAPOL Start Frames Transmitted	Displays the number of EAPOL Start frames transmitted via the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.

Term	Definition
EAP Resp/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.
EAP Req/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Req Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAP Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to the most recently received EAPOL frame.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show dot1x statistics 0/1

Port..................................... 0/1
EAPOL Frames Received.................... 0
EAPOL Frames Transmitted................. 0
EAPOL Start Frames Transmitted........... 3
EAPOL Logoff Frames Received............. 0
EAP Resp/Id frames transmitted........... 0
EAP Response frames transmitted.......... 0
EAP Req/Id frames transmitted............ 0
EAP Req frames transmitted............... 0
Invalid EAPOL frames received............ 0
EAP length error frames received......... 0
Last EAPOL Frame Version................. 0
Last EAPOL Frame Source.................. 00:00:00:00:02:01
```

Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

The EdgeSwitch provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the `no` form of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the `no` form of the storm-control command (not stating a "level") disables that form of storm-control but maintains the configured "level" (to be active the next time that form of storm-control is enabled.)



Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes – used to calculate a packet-per-second (pps) rate – as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512-byte packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control broadcast`
Mode	• Global Config • Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control broadcast`
Mode	• Global Config • Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	5
Format	`storm-control broadcast level` *`0-100`*
Mode	• Global Config • Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format `no storm-control broadcast level`

Mode
- Global Config
- Interface Config

storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 0

Format `storm-control broadcast rate` *`0-33554431`*

Mode
- Global Config
- Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format `no storm-control broadcast rate`

Mode
- Global Config
- Interface Config

storm-control multicast

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control multicast`

Mode
- Global Config
- Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control multicast`

Mode
- Global Config
- Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	`storm-control multicast level` *`0-100`*
Mode	• Global Config • Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	`no storm-control multicast level` *`0-100`*
Mode	• Global Config • Interface Config

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control multicast rate` *`0-33554431`*
Mode	• Global Config • Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	`no storm-control multicast rate`
Mode	• Global Config • Interface Config

storm-control unicast

This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control unicast`
Mode	• Global Config • Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control unicast`

Mode
- Global Config
- Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default 5

Format `storm-control unicast level` *`0-100`*

Mode
- Global Config
- Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format `no storm-control unicast level`

Mode
- Global Config
- Interface Config

storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0

Format `storm-control unicast rate` *`0-33554431`*

Mode
- Global Config
- Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format `no storm-control unicast rate`

Mode
- Global Config
- Interface Config

show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the `all` keyword to display the per-port configuration parameters for all interfaces, or specify the *`slot/port`* to display information about a specific interface.

Format	`show storm-control [all | slot/port]`
Mode	• Privileged EXEC

Term	Definition
Broadcast Storm Control Mode / Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Broadcast Storm Control Level / Bcast Level	The broadcast storm control level.
Multicast Storm Control Mode / Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Multicast Storm Control Level / Mcast Level	The multicast storm control level.
Unicast Storm Control Mode / Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Unicast Storm Control Level / Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show storm-control

(UBNT EdgeSwitch) #show storm-control

Broadcast Storm Control Mode................... Disable
Broadcast Storm Control Level.................. 5 percent
Multicast Storm Control Mode................... Disable
Multicast Storm Control Level.................. 5 percent
Unicast Storm Control Mode..................... Disable
Unicast Storm Control Level.................... 5 percent
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show storm-control 0/1

        Bcast   Bcast    Mcast   Mcast    Ucast   Ucast
 Intf   Mode    Level    Mode    Level    Mode    Level
------ ------- -------- ------- -------- ------- --------
0/1    Disable     5%   Disable     5%   Disable     5%
```

Example: The following shows an example of part of the CLI display output for the command.

```
(UBNT EdgeSwitch) #show storm-control all

        Bcast   Bcast    Mcast   Mcast    Ucast   Ucast
 Intf   Mode    Level    Mode    Level    Mode    Level
------ ------- -------- ------- -------- ------- --------
0/1    Disable     5%   Disable     5%   Disable     5%
0/2    Disable     5%   Disable     5%   Disable     5%
0/3    Disable     5%   Disable     5%   Disable     5%
0/4    Disable     5%   Disable     5%   Disable     5%
0/5    Disable     5%   Disable     5%   Disable     5%
```

Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.



Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

port-channel

This command configures a new port-channel (LAG) and generates a logical slot/port number for the port-channel. The *name* field is a character string which can contain alphanumeric characters and "-" (dash character). Use the `show port channel` command to display the slot/port number for the logical interface. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface where *lag-intf-num* is the LAG port number.



Note: Before you include a port in a port-channel, set the port physical mode. For more information, see **"speed" on page 199**.

Format	`port-channel` *name*
Mode	Global Config

addport

This command adds one port to the port-channel (LAG). The first interface is a logical slot/port number of a configured port-channel. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example: interface 0/1-0/4. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface, where *lag-intf-num* is the LAG port number.



Note: Before adding a port to a port-channel, set the physical mode of the port. For more information, see **"speed" on page 199**.

Format	`addport {`*slot/port* `|` `lag` *lag-intf_num*`}`
Mode	Interface Config

deleteport (Interface Config)

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical *slot/port* number of a configured port-channel (or range of port-channels). Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format	`deleteport {`*slot/port* `|` `lag` *lag-intf_num*`}`
Mode	Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical *slot/port* number of a configured port-channel.

Format	`deleteport` *slot/port* `all`
Mode	Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of *key* is 0–65535.

Default	0x8000
Format	`lacp admin key` *key*
Mode	Interface Config



Note: This command is applicable only to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format	`no lacp admin key`
Mode	Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces.The valid range of *delay* is 0–65535.

Default	0x8000
Format	`lacp collector max delay` *delay*
Mode	Interface Config



Note: This command is applicable only to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format	`no lacp collector max delay`
Mode	Interface Config

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for *key* is 0–65535.

Default	Internal Interface Number of this Physical Port
Format	`lacp actor admin key` *key*
Mode	Interface Config



Note: This command is applicable only to port-channel interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format	`no lacp actor admin key`
Mode	Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format	`lacp actor admin state individual`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format	`no lacp actor admin state individual`
Mode	Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format	`lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format	`no lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format	`lacp actor admin state passive`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format	`no lacp actor admin state passive`
Mode	Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. This command can be used to configure a single interfaces or a range of interfaces.

Default	0x07
Format	`lacp actor admin state {individual | longtimeout | passive}`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Note: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

Format	`no lacp actor admin state {individual | longtimeout | passive}`
Mode	Interface Config

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for `priority` is 0 to 65535.

Default	0x80
Format	`lacp actor port priority` *`0-65535`*
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format	`no lacp actor port priority`
Mode	Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for *`key`* is 0 to 65535.

Default	0x0
Format	`lacp partner admin key` *`key`*
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin key

Use this command to set the administrative value of the Key for the protocol partner to the default.

Format `no lacp partner admin key`

Mode Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format `lacp partner admin state individual`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format `no lacp partner admin state individual`

Mode Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to long timeout.

Format `lacp partner admin state longtimeout`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format `no lacp partner admin state longtimeout`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format `lacp partner admin state passive`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format `no lacp partner admin state passive`

Mode Interface Config

lacp partner port id

Use this command to configure the LACP partner port ID. This command can be used to configure a single interface or a range of interfaces. The valid range for *port-id* is 0 to 65535.

Default	0x80
Format	`lacp partner port-id port-id`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port ID to the default.

Format	`no lacp partner port-id`
Mode	Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range for *priority* is 0 to 65535.

Default	0x0
Format	`lacp partner port priority priority`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner port priority

Use this command to set the LACP partner port priority to the default.

Format	`no lacp partner port priority`
Mode	Interface Config

lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of *system-id* is 00:00:00:00:00:00 to FF:FF:FF:FF:FF:FF.

Default	00:00:00:00:00:00
Format	`lacp partner system-id system-id`
Mode	Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner system-id

Use this command to set the administrative value of the Aggregation Port's protocol Partner's System ID to the default.

Format	`no lacp partner system-id`
Mode	Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range for `priority` is 0 to 65535.

Default	0x0
Format	`lacp partner system priority` *`0-65535`*
Mode	Interface Config



Note: This command is applicable only to physical interfaces.

no lacp partner system priority

Use this command to set the administrative value of priority associated with the Partner's System ID to the default.

Format	`no lacp partner system priority`
Mode	Interface Config

interface lag

Use this command to enter Interface configuration mode for the specified LAG.

Format	`interface lag` *`lag-interface-number`*
Mode	Global Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface or range of interfaces. By default the static mode for a new port-channel is enabled, which means the port-channel is static. If the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel is enabled, which means the port-channel is static. You can only use this command on port-channel interfaces.

Default	enabled
Format	`port-channel static`
Mode	Interface Config

no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format	`no port-channel static`
Mode	Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	enabled
Format	`port lacpmode`
Mode	Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	`no port lacpmode`
Mode	Interface Config

port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	`port lacpmode enable all`
Mode	Global Config

no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	`no port lacpmode enable all`
Mode	Global Config

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner).

Format	`no port lacptimeout {actor | partner}`
Mode	Interface Config



Note: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

Format	`no port lacptimeout {actor | partner}`
Mode	Global Config



Note: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to the default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

port-channel adminmode

This command enables all configured port-channels with the same administrative mode setting.

Format `port-channel adminmode all`

Mode Global Config

no port-channel adminmode

This command disables all configured port-channels with the same administrative mode setting.

Format `no port-channel adminmode all`

Mode Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical *slot/port* for a configured port-channel. The option `all` sets every configured port-channel to the same administrative mode setting. Instead of *slot/port*, `lag` *lag-intf-num* can also be used to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Default enabled

Format `port-channel linktrap {logical` *slot/port* `| all}`

Mode Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Format `no port-channel linktrap {logical` *slot/port* `| all}`

Mode Global Config

port-channel load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link. Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of *slot/port*, `lag` *lag-intf-num* can also be used to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Default 3

Format `port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {`*slot/port* `| all}`

Mode Interface Config, Global Config

Parameter	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
7	Enhanced hashing mode
slot/port `|` `all`	Global Config Mode only: The interface is a logical *slot/port* number of a configured port-channel; `all` applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format `no port-channel load-balance {slot/port | all}`

Mode
- Interface Config
- Global Config

Term	Definition
`slot/port | all`	Global Config Mode only: The interface is a logical `slot/port` number of a configured port-channel; `all` applies the command to all currently configured port-channels.

port-channel local-preference

This command enables the local-preference mode on a port-channel (LAG) interface or range of interfaces. By default, the local-preference mode for a port-channel is disabled. This command can be used only on port-channel interfaces.

Default disable

Format `port-channel local-preference`

Mode Interface Config

no port-channel local-preference

This command disables the local-preference mode on a port-channel.

Format `no port-channel local-preference`

Mode Interface Config

port-channel min-links

This command configures the port-channel's minimum links for lag interfaces.

Default 1

Format `port-channel min-links 1-8`

Mode Interface Config

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical `slot/port` for a configured port-channel, and `name` is an alphanumeric string up to 15 characters. Instead of `slot/port`, `lag lag-intf-num` can also be used to specify the LAG interface, where `lag-intf-num` is the LAG port number.

Format `port-channel name {logical slot/port} name`

Mode Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of `priority` is 0-65535.

Default 0x8000

Format `port-channel system priority priority`

Mode Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format `no port-channel system priority`

Mode Global Config

show lacp actor

Use this command to display LACP actor attributes. Instead of *slot/port*, lag *lag-intf-num* can also be used to specify the LAG interface where, *lag-intf-num* is the LAG port number.

Format show lacp actor {*slot/port* | all}

Mode Global Config

The following information is displayed.

Term	Description
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes. Instead of *slot/port*, lag *lag-intf-num* can also be used to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format show lacp partner {*slot/port* | all}

Mode Privileged EXEC

The following information is displayed.

Term	Description
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces. Instead of *slot/port*, lag *lag-intf-num* can also be used to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format show port-channel brief

Mode User EXEC

For each port-channel the following information is displayed:

Term	Definition
Logical Interface	The slot/port of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch. Instead of *slot/port*, `lag` *lag-intf-num* can also be used to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format `show port-channel {slot/port | lag lag-intf-num}`

Mode Privileged EXEC

Term	Definition
Local Interface	The valid slot/port number.
Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • **Static** The port-channel is statically maintained. • **Dynamic** The port-channel is dynamically maintained.
Load Balance Option	The load balance option associated with this LAG. See **"port-channel load-balance" on page 264**.
Local Preference Mode	Indicates whether the local preference mode is enabled or disabled.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device/Timeout	For each port, lists the timeout (long or short) for Device Type (actor or partner).
Port Speed	Speed of the port-channel port.
Port Active	This field indicates if the port is actively participating in the port-channel (LAG).

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show port-channel 3/1

Local Interface.............................. 3/1
Channel Name................................. ch1
Link State................................... Up
Admin Mode................................... Enabled
Type......................................... Static
Load Balance Option.......................... 3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode........................ Enabled

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/1    actor/long    Auto      True
       partner/long
0/2    actor/long    Auto      True
       partner/long
0/3    actor/long    Auto      False
       partner/long
0/4    actor/long    Auto      False
       partner/long
```

show port-channel system priority

Use this command to display the port-channel system priority.

Format `show port-channel system priority`

Mode Privileged EXEC

show port-channel counters

Use this command to display port-channel counters for the specified port.

Format `show port-channel slot/port counters`

Mode Privileged EXEC

Term	Definition
Local Interface	The valid slot/port number.
Channel Name	The name of this port-channel (LAG).
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Port Channel Flap Count	The number of times the port-channel was inactive.
Mbr Ports	The slot/port for the port member.
Mbr Flap Counters	The number of times a port member is inactive, either because the link is down, or the admin state is disabled.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show port-channel 3/1 counters

Local Interface.............................. 3/1
Channel Name................................. ch1
Link State................................... Down
Admin Mode................................... Enabled
Port Channel Flap Count...................... 0

Mbr    Mbr Flap
Ports  Counters
------ ---------
0/1    0
0/2    0
0/3    1
0/4    0
0/5    0
0/6    0
0/7    0
0/8    0
```

clear port-channel counters

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Format `clear port-channel {lag-intf-num | slot/port} counters`

Mode Privileged EXEC

clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format `clear port-channel all counters`

Mode Privileged EXEC

Port Mirroring Commands

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the `source interface slot/port` parameter to specify the interface to monitor. Use `rx` to monitor only ingress packets, or use `tx` to monitor only egress packets. If you do not specify an `{rx|tx}` option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.



Note: The source and destination cannot be configured as remote on the same device.

The `reflector-port` is configured at the source switch. The `reflector-port` forwards the mirrored traffic towards the destination switch.



Note: This port must be configured with RSPAN VLAN membership.

An IP/MAC ACL can be attached to a session by giving the access list number/name.

Use `destination interface slot/port` to specify the interface to receive the monitored traffic.

Use the `mode` parameter to enable the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Use the `filter` parameter to filter a specified access group either by IP address or MAC address.

Format	`monitor session session-id {`
	`source {interface slot/port | vlan vlan-id | remote vlan vlan-id} [rx|tx] |`
	`destination {interface slot/port | remote vlan vlan-id reflector-port slot/port} |`
	`mode | filter {ip access-group {acl-id|acl-name} | mac access-group acl-name} }`

Mode	Global Config

Example: To configure the RSPAN VLAN source:

```
monitor session session-id source {interface slot/port | vlan vlan-id | remote vlan vlan-id}
[rx|tx]
```

Example: To the configure RSPAN VLAN destination:

```
monitor session session-id destination {interface slot/port | remote vlan vlan-id reflector-port
slot/port}
```

Example: To attach an ACL:

```
monitor session session-id filter {ip access-group acl-id/acl-name | mac access-group acl-name}
```

no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the `source interface slot/port` parameter or `destination interface` to remove the specified interface from the port monitoring session. Use the `mode` parameter to disable the administrative mode of the session.

Note: Since the current version of the software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the `no monitor` command.

Format	`no monitor session session-id [{source interface slot/port | destination interface | mode | filter {ip access-group | mac access-group}}]`
Mode	Global Config

no monitor

This command removes all the source ports and a destination port for the {} and restores the default value for mirroring session mode for all the configured sessions.

This is a standalone `no` command; i.e., there is no corresponding `monitor` command.

Default	enabled
Format	`no monitor`
Mode	Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session. The `session-id` parameter is an integer value used to identify the session. In the current version of the software, the `session-id` parameter's value is always 1.

Format	`show monitor session session-id`
Mode	Privileged EXEC

Term	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with `session-id`. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with `session-id`. If probe port is not set then this field is blank.
Source Port	The port which is configured as mirrored port (source port) for the session identified with `session-id`. If no source port is configured for the session then this field is blank.
Type	Direction in which source port configured for port mirroring. Types are "tx" for transmitted packets and "rx" for received packets.

show vlan remote-span

This command displays the configured RSPAN VLAN.

Format	`show vlan remote-span`
Mode	Privileged EXEC

Example: The following shows example output for the command.

```
(UBNT EdgeSwitch)# show vlan remote-span

Remote SPAN VLAN
-----------------------------------------------------------------------
100
```

Static MAC Filtering Commands

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

This command adds a static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The value of the *macaddr* parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The *vlanid* parameter must identify a valid VLAN.

The number of static MAC filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured:

- For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

You can configure the following combinations:

- Unicast MAC and source port (max = 20)
- Multicast MAC and source port (max = 20)
- Multicast MAC and destination port (only) (max = 256)
- Multicast MAC and source ports and destination ports (max = 20)

Format	`macfilter macaddr vlanid`
Mode	Global Config

no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter macaddr vlanid`
Mode	Global Config

macfilter adddest

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest macaddr`
Mode	Interface Config

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter adddest macaddr`
Mode	Interface Config

macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.



Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest all macaddr`
Mode	Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter adddest all macaddr`
Mode	Global Config

macfilter addsrc

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`macfilter addsrc macaddr vlanid`
Mode	Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter addsrc macaddr vlanid`
Mode	Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and *vlanid*. You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`macfilter addsrc all macaddr vlanid`
Mode	Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter addsrc all macaddr vlanid`
Mode	Global Config

show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you specify all, all the Static MAC Filters in the system are displayed. If you supply a value for macaddr, you must also enter a value for vlanid, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format `show mac-address-table static {macaddr vlanid | all}`

Mode Privileged EXEC

Term	Definition
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).



Note: Only multicast address filters will have destination port lists.

show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table staticfiltering`

Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is six 2-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

DHCP Client Commands

The EdgeSwitch can include vendor and configuration information in DHCP client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the EdgeSwitch.

Format	`dhcp client vendor-id-option` *`string`*
Mode	Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the EdgeSwitch.

Format	`no dhcp client vendor-id-option`
Mode	Global Config

dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the EdgeSwitch.

Format	`dhcp client vendor-id-option-string` *`string`*
Mode	Global Config

no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format	`no dhcp client vendor-id-option-string`
Mode	Global Config

show dhcp client vendor-id-option

This command displays the configured administration mode of the `vendor-id-option` and the vendor-id string to be included in Option-43 in DHCP requests.

Format	`show dhcp client vendor-id-option`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option is Enabled
DHCP Client Vendor Identifier Option string is EdgeSwitchClient.
```

DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default	disabled
Format	`ip dhcp snooping`
Mode	Global Config

no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format	`no ip dhcp snooping`
Mode	Global Config

ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	`ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	`no ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	enabled
Format	`ip dhcp snooping verify mac-address`
Mode	Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	`no ip dhcp snooping verify mac-address`
Mode	Global Config

ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default	local
Format	`ip dhcp snooping database {local|tftp://`*`hostIP/filename`*`}`
Mode	Global Config

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The *interval* value ranges from 15 to 86400 seconds.

Default	300 seconds
Format	`ip dhcp snooping database write-delay interval`
Mode	Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format	`no ip dhcp snooping database write-delay`
Mode	Global Config

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format	`ip dhcp snooping binding mac-address vlan vlan-id ip address interface interface-id`
Mode	Global Config

no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format	`no ip dhcp snooping binding mac-address`
Mode	Global Config

ip dhcp filtering trust

Use this command to enable trusted mode on the interface if the previously saved configuration or applied script contains this command.

Format	`ip dhcp filtering trust interface-id`
Mode	Global Config

no ip dhcp filtering trust

Use this command to disable trusted mode on the interface.

Format	`no ip dhcp filtering trust interface-id`
Mode	Global Config

ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds.

Default	disabled (no limit)
Format	`ip dhcp snooping limit {rate pps [burst interval seconds]}`
Mode	Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format	`no ip dhcp snooping limit`
Mode	Interface Config

ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default disabled

Format `ip dhcp snooping log-invalid`

Mode Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format `no ip dhcp snooping log-invalid`

Mode Interface Config

ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default disabled

Format `ip dhcp snooping trust`

Mode Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format `no ip dhcp snooping trust`

Mode Interface Config

show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format `show ip dhcp snooping`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40

Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
0/6          No              No
```

show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format `show ip dhcp snooping binding [{static|dynamic}] [interface slot/port] [vlan id]`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease Time (sec)	The remaining lease time for the entry.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip dhcp snooping binding

Total number of bindings: 2

MAC Address          IP Address   VLAN  Interface  Type  Lease time (Secs)
-----------------  ------------  ----  ---------  ---- ------------------
00:02:B3:06:60:80   210.1.1.3      10   0/1                  86400
00:0F:FE:00:13:04   210.1.1.4      10   0/1                  86400
```

show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format `show ip dhcp snooping database`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

Format `show ip dhcp snooping interfaces`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip dhcp snooping interfaces

 Interface    Trust State  Rate Limit   Burst Interval
                             (pps)        (seconds)
-----------   ----------   ----------   --------------
   1/g1           No           15              1
   1/g2           No           15              1
   1/g3           No           15              1

(UBNT EdgeSwitch) #show ip dhcp snooping interfaces ethernet 1/g15

 Interface    Trust State  Rate Limit   Burst Interval
                             (pps)        (seconds)
-----------   ----------   ----------   --------------
   1/g15          Yes          15              1
```

show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format `show ip dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The IP address of the interface in slot/port format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip dhcp snooping statistics

 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
0/2                0            0            0
0/3                0            0            0
0/4                0            0            0
0/5                0            0            0
0/6                0            0            0
0/7                0            0            0
0/8                0            0            0
0/9                0            0            0
0/10               0            0            0
0/11               0            0            0
0/12               0            0            0
0/13               0            0            0
0/14               0            0            0
0/15               0            0            0
0/16               0            0            0
0/17               0            0            0
0/18               0            0            0
0/19               0            0            0
0/20               0            0            0
```

clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format	`clear ip dhcp snooping binding [interface slot/port]`
Mode	• Privileged EXEC • User EXEC

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format	`clear ip dhcp snooping statistics`
Mode	• Privileged EXEC • User EXEC

IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP Snooping. The EdgeSwitch software supports IGMP Versions 1, 2, and 3. The IGMP Snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.



Note: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP Snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP Snooping on all interfaces participating in a VLAN.

If IGMP Snooping is enabled on an interface, enabling routing on the interface or giving the interface port-channel (LAG) membership disables the interface's IGMP Snooping functionality. IGMP Snooping functionality is restored if routing is disabled or if port-channel (LAG) membership is removed from the interface.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

The optional *vlan_id* parameter is supported only in VLAN Config mode.

Default	disabled
Format	`set igmp [vlan_id]`
Mode	Global Config, Interface Config, VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN. The optional *vlan_id* parameter is supported only in VLAN Config mode.

Format	`no set igmp [vlan_id]`
Mode	Global Config, Interface Config, VLAN Config

set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If IGMP Snooping is enabled on an interface, enabling routing on the interface or giving it membership in a port-channel (LAG), disables the interface's IGMP Snooping functionality. IGMP Snooping functionality is restored if routing is disabled or if port-channel (LAG) membership is removed from the interface.

Default	disabled
Format	`set igmp interfacemode`
Mode	Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format	`no set igmp interfacemode`
Mode	Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a VLAN. Enabling fast-leave allows the switch to immediately remove the Layer-2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each Layer-2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same Layer-2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

The optional *vlan_id* parameter is supported only in VLAN Config mode.

Default	disabled
Format	`set igmp fast-leave [vlan_id]`
Mode	Interface Config, Interface Range, VLAN Config

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface. The optional *vlan_id* parameter is supported only in VLAN Config mode.

Format	`no set igmp fast-leave [vlan_id]`
Mode	Interface Config, Interface Range, VLAN Config

set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

The optional *vlan_id* parameter is supported only in VLAN Config mode.

Default	260 seconds
Format	`set igmp groupmembership-interval [vlan_id] 2-3600`
Mode	Interface Config, Global Config, VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value. The optional *vlan_id* parameter is supported only in VLAN Config mode.

Format	`no set igmp groupmembership-interval [vlan_id]`
Mode	Interface Config, Global Config, VLAN Config

set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds. The optional *vlan_id* parameter is supported only in VLAN Config mode.

Default	10 seconds
Format	`set igmp maxresponse [vlan_id] 1-25`
Mode	Global Config, Interface Config, VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

The optional *vlan_id* parameter is supported only in VLAN Config mode.

Format	`no set igmp maxresponse [vlan_id]`
Mode	Global Config, Interface Config, VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout; i.e., no expiration. The optional *vlan_id* parameter is supported only in VLAN Config mode.

Default	0
Format	`set igmp mcrtrexpiretime [vlan_id] 0-3600`
Mode	Global Config, Interface Config, VLAN Config

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN. The optional *vlan_id* parameter is supported only in VLAN Config mode.

Format	`no set igmp mcrtrexpiretime [vlan_id]`
Mode	Global Config, Interface Config, VLAN Config

set igmp mrouter

This command configures the VLAN ID (*vlan_id*) that has the multicast router mode enabled.

Format	`set igmp mrouter vlan_id`
Mode	Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (*vlan_id*).

Format	`no set igmp mrouter vlan_id`
Mode	Interface Config

set igmp mrouter interface

This command configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default	disabled
Format	`set igmp mrouter interface`
Mode	Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format	`no set igmp mrouter interface`
Mode	Interface Config

set igmp report-suppression

Use this command to suppress the IGMP reports on a given VLAN ID. In order to optimize the number of reports traversing the network with no added benefits, a Report Suppression mechanism is implemented. When more than one client responds to an MGMD query for the same Multicast Group address within the max-response-time, only the first response is forwarded to the query and others are suppressed at the switch.

Default Disabled

Format `set igmp report-suppression vlan-id`

Mode VLAN Config

Parameter	Description
vlan-id	A valid VLAN ID. Range is 1 to 4093.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #vlan database
(UBNT EdgeSwitch) (Vlan)#set igmp report-suppression ?

<1-4093>                Enter VLAN ID.

(UBNT EdgeSwitch) (Vlan)#set igmp report-suppression 1
```

no set igmp report-suppression

Use this command to return the system to the default.

Format `no set igmp report-suppression`

Mode VLAN Config

show igmpsnooping

This command displays IGMP Snooping information for a given *slot/port* or VLAN. Configured information is displayed whether or not IGMP Snooping is enabled.

Format `show igmpsnooping [slot/port | vlan_id]`

Mode Privileged EXEC

When the optional arguments *slot/port* or *vlan_id* are not used, the command displays the following:

Term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the *slot/port* values, the following information appears:

Term	Definition
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlan_id*, the following information appears:

Term	Definition
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval (secs)	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Maximum Response Time (secs)	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time (secs)	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.
Report Suppression Mode	Indicates whether IGMP reports (set by the command **"set igmp report-suppression" on page 284**) is enabled or not.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show igmpsnooping 1

VLAN ID..................................... 1
IGMP Snooping Admin Mode.................... Disabled
Fast Leave Mode............................. Disabled
Group Membership Interval (secs)............ 260
Max Response Time (secs).................... 10
Multicast Router Expiry Time (secs)......... 0
Report Suppression Mode..................... Enabled
```

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter interface slot/port`

Mode Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter vlan slot/port`

Mode Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping ssm

This command displays information about Source Specific Multicasting (SSM) by entry, group, or statistics. SSM delivers multicast packets to receivers that originated from a source address specified by the receiver. SSM is only available with IGMPv3 and MLDv2.

Format `show igmpsnooping ssm {entries | groups | stats}`

Mode Privileged EXEC

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format `show mac-address-table igmpsnooping`

Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is six 2-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Querier Commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the *IGMP Querier*. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.



Note: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If IGMP Snooping Querier is enabled on a VLAN, disabling IGMP Snooping on the VLAN also disables the VLAN's IGMP Snooping Querier functionality. The VLAN's IGMP Snooping Querier functionality is restored if IGMP Snooping again becomes operational on the VLAN.



Note: The Querier IP Address assigned for a VLAN takes precedence over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default	disabled
Format	`set igmp querier [vlan-id] [address ipv4_address]`
Mode	Global Config VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional `address` parameter to reset the querier address to 0.0.0.0.

Format	`no set igmp querier [vlan-id] [address]`
Mode	Global Config VLAN Mode

set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default	disabled
Format	`set igmp querier query-interval 1-1800`
Mode	Global Config

no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format	`no set igmp querier query-interval`
Mode	Global Config

set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default	60 seconds
Format	`set igmp querier timer expiry` *`60-300`*
Mode	Global Config

no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format	`no set igmp querier timer expiry`
Mode	Global Config

set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default	1
Format	`set igmp querier` *`version 1-2`*
Mode	Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format	`no set igmp querier version`
Mode	Global Config

set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	`set igmp querier election participate`
Mode	VLAN Config

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	`no set igmp querier election participate`
Mode	VLAN Config

show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format	`show igmpsnooping querier [{detail | vlan` *`vlanid`*`}]`
Mode	Privileged EXEC

When the optional argument *vlanid* is not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following additional information appears.

Field	Description
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.



Note: To enable the SNMP trap specific to port security, see **"snmp-server enable traps violation" on page 74**.

port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default	disabled
Format	`port-security`
Mode	• Global Config (to enable port locking globally) • Interface Config (to enable port locking on an interface or range of interfaces)

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format	`no port-security`
Mode	• Global Config • Interface Config

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port. The valid range is 0–600.

Default	600
Format	`port-security max-dynamic` *`maxvalue`*
Mode	Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format	`no port-security max-dynamic`
Mode	Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port. The valid range is 0–20.

Default	1
Format	`port-security max-static` *`maxvalue`*
Mode	Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format	`no port-security max-static`
Mode	Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *vid* parameter is the VLAN ID.

Format	port-security mac-address *mac-address vid*
Mode	Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format	no port-security mac-address *mac-address vid*
Mode	Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format	port-security mac-address move
Mode	Interface Config

port-security mac-address sticky

This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN ID (for Interface Config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The *vid* parameter is the VLAN ID. The Global command applies the sticky mode to all valid interfaces (physical and LAG). There is no global sticky mode as such.

Dynamically learned sticky addresses will appear in show running-config output as port-security mac-address sticky *mac-address vid* entries. This distinguishes them from static entries.

Format	port-security mac-address sticky [*mac-address vid*]
Mode	• Global Config • Interface Config

Example: The following shows an example of the command.

```
(EdgeSwitch)(Config)# port-security mac-address sticky
(EdgeSwitch)(Interface)# port-security mac-address sticky
(EdgeSwitch)(Interface)# port-security mac-address sticky
  00:00:00:00:00:01 2
```

no port-security mac-address sticky

The no form removes the sticky mode. The sticky MAC address can be deleted using the command no port-security mac-address *mac-address vid*.

Format	no port-security mac-address sticky [*mac-address vid*]
Mode	• Global Config • Interface Config

show port-security

This command displays the port-security settings for the port(s). If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface or on all interfaces. Instead of *slot/port*, lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format	show port-security [{*slot/port* | all}]
Mode	Privileged EXEC

Term	Definition
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Term	Definition
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.
Sticky Mode	The administrative mode of the port security Sticky Mode feature on the interface.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show port-security 0/1

        Admin    Dynamic     Static     Violation  Sticky
Intf    Mode      Limit      Limit      Trap Mode  Mode
------  -------  ----------  ---------  ---------  --------
0/1     Disabled 1           1          Disabled   Enabled
```

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port. Instead of *slot/port*, you can also use `lag` *lag-intf-num* to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format `show port-security dynamic` *slot/port*

Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port. Instead of *slot/port*, you can also use `lag` *lag-intf-num* to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format `show port-security static` *slot/port*

Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of statically locked MAC.

Example: The following shows example CLI display output for the command.

```
(EdgeSwitch) #show port-security static 0/1

 Number of static MAC addresses configured: 2

 Statically configured MAC Address    VLAN ID    Sticky
 ---------------------------------    -------    ------
 00:00:00:00:00:01                    2            Yes
 00:00:00:00:00:02                    2            No
```

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port. Instead of *slot/port*, `lag` *lag-intf-num* can also be used to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format `show port-security violation` *slot/port*

Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of discarded packet on locked port.

LLDP (802.1AB) Commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default	disabled
Format	`lldp transmit`
Mode	Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format	`no lldp transmit`
Mode	Interface Config

lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default	disabled
Format	`lldp receive`
Mode	Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format	`no lldp receive`
Mode	Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *`interval-seconds`* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The *`hold-value`* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The *`reinit-seconds`* is the delay before reinitialization, and the range is 1-10 seconds.

Default	• `interval`: 30 seconds • `hold`: 4 • `reinit`: 2 seconds
Format	`lldp timers [interval` *`interval-seconds`*`] [hold` *`hold-value`*`] [reinit` *`reinit-seconds`*`]`
Mode	Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format	`no lldp timers [interval] [hold] [reinit]`
Mode	Global Config

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs from an interface or range of interfaces. Use `sys-name` to transmit the system name TLV. To configure the system name, see **"snmp-server" on page 73**. Use `sys-desc` to transmit the system description TLV. Use `sys-cap` to transmit the system capabilities TLV. Use `port-desc` to transmit the port description TLV. To configure the port description, see **"description" on page 197**.

Default	no optional TLVs are included
Format	`lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`
Mode	Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format	`no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`
Mode	Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format	`lldp transmit-mgmt`
Mode	Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format	`no lldp transmit-mgmt`
Mode	Interface Config

lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default	disabled
Format	`lldp notification`
Mode	Interface Config

no lldp notification

Use this command to disable notifications.

Default	disabled
Format	`no lldp notification`
Mode	Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The *`interval`* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default	5
Format	`lldp notification-interval` *`interval`*
Mode	Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format `no lldp notification-interval`

Mode Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format `clear lldp statistics`

Mode Privileged Exec

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format `clear lldp remote-data`

Mode Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format `show lldp`

Mode Privileged Exec

Term	Definition
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before reinitialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format `show lldp interface {slot/port | all}`

Mode Privileged Exec

Term	Definition
Interface	The interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format `show lldp statistics {slot/port | all}`

Mode Privileged Exec

Term	Definition
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	Definition
Interface	The interface in slot/port format.
Transmit Total	Total number of LLDP packets transmitted on the port.
Receive Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format `show lldp remote-device {slot/port | all}`

Mode Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show lldp remote-device all

LLDP Remote Device Summary

Local
Interface RemID    Chassis ID            Port ID             System Name
-------  -------   --------------------  ------------------  ------------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7         2      00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7         3      00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7         4      00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7         5      00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7         1      00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7         6      00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format `show lldp remote-device detail` *slot/port*

Mode Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show lldp remote-device detail 0/7

LLDP Remote Device Detail

Local Interface: 0/7

Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format `show lldp local-device {slot/port | all}`

Mode Privileged EXEC

Term	Definition
Interface	The interface in a unit/slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format `show lldp local-device detail slot/port`

Mode Privileged EXEC

Term	Definition
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

LLDP-MED Commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default disabled

Format `lldp med`

Mode Interface Config

no lldp med

Use this command to disable MED.

Format `no lldp med`

Mode Interface Config

lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default disabled

Format `lldp med confignotification`

Mode Interface Config

no lldp med confignotification

Use this command to disable notifications.

Format `no lldp med confignotification`

Mode Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default By default, the capabilities and network policy TLVs are included.

Format `lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`

Mode Interface Config

Parameter	Definition
`capabilities`	Transmit the LLDP capabilities TLV.
`ex-pd`	Transmit the LLDP extended PD TLV.
`ex-pse`	Transmit the LLDP extended PSE TLV.
`inventory`	Transmit the LLDP inventory TLV.
`location`	Transmit the LLDP location TLV.
`network-policy`	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format `no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`

Mode Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format `lldp med all`

Mode Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format `lldp med confignotification all`

Mode Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. The *count* is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default 3

Format `lldp med faststartrepeatcount [count]`

Mode Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format `no lldp med faststartrepeatcount`

Mode Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format `lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`

Mode Global Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format	`show lldp med`
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch ) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(UBNT EdgeSwitch) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. The *slot/port* indicates a specific physical interface. The `all` parameter indicates all valid LLDP interfaces.

Format	`show lldp med interface {slot/port | all}`
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/1        Down    Disabled  Disabled  Disabled     0,1
0/2        Up      Disabled  Disabled  Disabled     0,1
0/3        Down    Disabled  Disabled  Disabled     0,1
0/4        Down    Disabled  Disabled  Disabled     0,1
0/5        Down    Disabled  Disabled  Disabled     0,1
0/6        Down    Disabled  Disabled  Disabled     0,1
0/7        Down    Disabled  Disabled  Disabled     0,1
0/8        Down    Disabled  Disabled  Disabled     0,1
0/9        Down    Disabled  Disabled  Disabled     0,1
0/10       Down    Disabled  Disabled  Disabled     0,1
0/11       Down    Disabled  Disabled  Disabled     0,1
0/12       Down    Disabled  Disabled  Disabled     0,1
0/13       Down    Disabled  Disabled  Disabled     0,1
0/14       Down    Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(UBNT EdgeSwitch) #show lldp med interface 0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/2        Up      Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(UBNT EdgeSwitch) #
```

show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. unit/slot/port indicates a specific physical interface.

Format	`show lldp med local-device detail` *slot/port*
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show lldp med local-device detail 0/8

LLDP MED Local Device Detail

Interface: 0/8

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format `show lldp med remote-device {slot/port | all}`

Mode Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Device Class	Device classification of the remote device.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
0/8            1      Class I
0/9            2      Not Defined
0/10           3      Class II
0/11           4      Class III
0/12           5      Network Con
```

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format `show lldp med remote-device detail slot/port`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show lldp med remote-device detail 0/8

LLDP MED Remote Device Detail

Local Interface: 0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
```

```
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

Denial of Service Commands



Note: Denial of Service (DataPlane) is supported on XGS-III and later platforms only.

This section describes the commands you use to configure Denial of Service (DoS) Control. The EdgeSwitch software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- SIP = DIP: Source IP address = Destination IP address.
- First Fragment: TCP Header size smaller then configured value.
- TCP Fragment: IP Fragment Offset = 1.
- TCP Flag: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- L4 Port: Source TCP/UDP Port = Destination TCP/UDP Port.
- ICMP: Limiting the size of ICMP Ping packets.
- SMAC = DMAC: Source MAC address = Destination MAC address.
- TCP Port: Source TCP Port = Destination TCP Port.
- UDP Port: Source UDP Port = Destination UDP Port.
- TCP Flag & Sequence: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- TCP Offset: TCP Header Offset = 1.
- TCP SYN: TCP Flag SYN set.
- TCP SYN & FIN: TCP Flags SYN and FIN set.
- TCP FIN & URG & PSH: TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- ICMP V6: Limiting the size of ICMPv6 Ping packets.
- ICMP Fragment: Checks for fragmented ICMP packets.

dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	`dos-control all`
Mode	Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format	`no dos-control all`
Mode	Global Config

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control sipdip`
Mode	Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format	`no dos-control sipdip`
Mode	Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled. The default is disabled. If you enable `dos-control firstfrag`, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

Default	disabled (20)
Format	`dos-control firstfrag [0-255]`
Mode	Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of disabled.

Format	`no dos-control firstfrag`
Mode	Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpfrag`
Mode	Global Config

no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Format	`no dos-control tcpfrag`
Mode	Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflag`
Mode	Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format	`no dos-control tcpflag`
Mode	Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Note: Some applications mirror source and destination L4 ports – RIP for example uses 520 for both. If you enable `dos-control l4port`, applications such as RIP may experience packet loss which would render the application inoperable.

Default	disabled
Format	`dos-control l4port`
Mode	Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format	`no dos-control l4port`
Mode	Global Config

dos-control smacdmac

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control smacdmac`
Mode	Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format	`no dos-control smacdmac`
Mode	Global Config

dos-control tcpport

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpport`
Mode	Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format	`no dos-control tcpport`
Mode	Global Config

dos-control udpport

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control udpport`
Mode	Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	`no dos-control udpport`
Mode	Global Config

dos-control tcpflagseq

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflagseq`
Mode	Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

dos-control tcpoffset

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpoffset`
Mode	Global Config

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format	`no dos-control tcpoffset`
Mode	Global Config

dos-control tcpsyn

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsyn`
Mode	Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	`no dos-control tcpsyn`
Mode	Global Config

dos-control tcpsynfin

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsynfin`
Mode	Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	`no dos-control tcpsynfin`
Mode	Global Config

dos-control tcpfinurgpsh

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpfinurgpsh`
Mode	Global Config

no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format	`no dos-control tcpfinurgpsh`
Mode	Global Config

dos-control icmpv4

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	`dos-control icmpv4 [0-16376]`
Mode	Global Config

no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv4`
Mode	Global Config

dos-control icmpv6

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	`dos-control icmpv6 0-16376`
Mode	Global Config

no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv6`
Mode	Global Config

dos-control icmpfrag

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control icmpfrag`
Mode	Global Config

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format	`no dos-control icmpfrag`
Mode	Global Config

show dos-control

This command displays Denial of Service configuration information.

Format	`show dos-control`
Mode	Privileged EXEC



Note: Some of the information below is displayed only if you are using the BCM56224 and BCM5621x platforms.

Term	Definition
First Fragment Mode	The administrative mode of First Fragment DoS prevention. When enabled, this causes the switch to drop packets that have a TCP header smaller then the configured Min TCP Hdr Size.
Min TCP Hdr Size	The minimum TCP header size the switch will accept if First Fragment DoS prevention is enabled.
ICMPv4 Mode	The administrative mode of ICMPv4 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 Payload Size.
Max ICMPv4 Payload Size	The maximum ICMPv4 payload size to accept when ICMPv4 DoS protection is enabled.

Term	Definition
ICMPv6 Mode	The administrative mode of ICMPv6 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Payload Size.
Max ICMPv6 Payload Size	The maximum ICMPv6 payload size to accept when ICMPv6 DoS protection is enabled.
ICMPv4 Fragment Mode	The administrative mode of ICMPv4 Fragment DoS prevention. When enabled, this causes the switch to drop fragmented ICMPv4 packets.
TCP Port Mode	The administrative mode of TCP Port DoS prevention. When enabled, this causes the switch to drop packets that have the TCP source port equal to the TCP destination port.
UDP Port Mode	The administrative mode of UDP Port DoS prevention. When enabled, this causes the switch to drop packets that have the UDP source port equal to the UDP destination port.
SIPDIP Mode	The administrative mode of SIP=DIP DoS prevention. Enabling this causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
SMACDMAC Mode	The administrative mode of SMAC=DMAC DoS prevention. Enabling this causes the switch to drop packets that have a source MAC address equal to the destination MAC address.
TCP FIN&URG& PSH Mode	The administrative mode of TCP FIN & URG & PSH DoS prevention. Enabling this causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.
TCP Flag & Sequence Mode	The administrative mode of TCP Flag DoS prevention. Enabling this causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0.
TCP SYN Mode	The administrative mode of TCP SYN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN set.
TCP SYN & FIN Mode	The administrative mode of TCP SYN & FIN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN and FIN set.
TCP Fragment Mode	The administrative mode of TCP Fragment DoS prevention. Enabling this causes the switch to drop packets that have an IP fragment offset equal to 1.
TCP Offset Mode	The administrative mode of TCP Offset DoS prevention. Enabling this causes the switch to drop packets that have a TCP header Offset equal to 1.

MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The seconds parameter must be within the range of 10 to 1,000,000 seconds.

Default 300

Format `bridge aging-time 10-1000000`

Mode Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format `no bridge aging-time`

Mode Global Config

show forwardingdb agetime

This command displays the timeout for address aging.

Default all

Format `show forwardingdb agetime`

Mode Privileged EXEC

Term	Definition
Forwarding DB ID	Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system. This field will not be displayed in an SVL system.
Agetime	• In an IVL system, this parameter displays the address aging timeout for the associated forwarding database. • In an SVL system, this will display the system's address aging timeout value in seconds.

show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC address by specifying the MAC address as an optional parameter.

Format `show mac-address-table multicast [macaddr]`

Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is six 2-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format `show mac-address-table stats`

Mode Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

Chapter 5: Routing Commands

This chapter describes the routing commands available in the EdgeSwitch CLI.

The chapter contains the following sections:

- **"Address Resolution Protocol Commands" on page 316**
- **"IP Routing Commands" on page 320**
- **"Routing Policy Commands" on page 333**
- **"Router Discovery Protocol Commands" on page 343**
- **"Virtual LAN Routing Commands" on page 346**
- **"IP Helper Commands" on page 349**
- **"ICMP Throttling Commands" on page 355**



Note: The commands in this chapter consist of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Address Resolution Protocol Commands

This section describes the commands you use to configure Address Resolution Protocol (ARP) and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

arp

This command creates an ARP entry. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device.

The format of the MAC address is six 2-digit hexadecimal numbers separated by colons; e.g., 00:06:29:32:81:40.

Format	`arp ipaddress macaddr`
Mode	Global Config

no arp

This command deletes an ARP entry. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface.

Format	`no arp ipaddress`
Mode	Global Config

arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform-specific integer value. The default size also varies depending on the platform.

Format	`arp cachesize platform_specific_integer_value`
Mode	Global Config

no arp cachesize

This command sets the ARP cache size to the default (platform-dependent) value.

Format	`no arp cachesize`
Mode	Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host may be lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default	disabled
Format	`arp dynamicrenew`
Mode	Privileged EXEC

no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format	`no arp dynamicrenew`
Mode	Privileged EXEC

arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format	`arp purge` *`ipaddr`*
Mode	Privileged EXEC

arp resptime

This command configures the ARP request response timeout.

The value for seconds is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for seconds is between 1-10 seconds.

Default	1
Format	`arp resptime` *`1-10`*
Mode	Global Config

no arp resptime

This command sets the ARP request response timeout to the default.

Format	`no arp resptime`
Mode	Global Config

arp retries

This command configures the ARP count of maximum request for retries.

The value for retries is an integer, which represents the maximum number of request for retries. The range for retries is an integer between 0-10 retries.

Default	4
Format	`arp retries` *`0-10`*
Mode	Global Config

no arp retries

This command sets the ARP count of maximum request for retries to the default.

Format	`no arp retries`
Mode	Global Config

arp timeout

This command configures the ARP entry ageout time.

The value for seconds is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for seconds is between 15-21600 seconds.

Default	1200
Format	`arp timeout` *`15-21600`*
Mode	Global Config

no arp timeout

This command sets the ARP entry ageout time to the default.

Format	`no arp timeout`
Mode	Global Config

clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the `gateway` keyword is specified, the dynamic entries of type gateway are purged as well.

Format	`clear arp-cache [gateway]`
Mode	Privileged EXEC

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, ping from the remote system to the DUT, issue the `show arp switch` command to see the ARP entries, and then issue the `clear arp-switch` command and check the `show arp switch` entries. There will be no more ARP entries.

Format	`clear arp-switch`
Mode	Privileged EXEC

show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the `show arp` results in conjunction with the `show arp switch` results.

Format	`show arp`
Mode	Privileged EXEC

Term	Definition
Age Time (seconds)	The time (in seconds) it takes for an ARP entry to age out. This value is configurable.
Response Time (seconds)	The time (in seconds) it takes for an ARP request timeout. This value is configurable.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current/Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current/Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Term	Definition
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing slot/port associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format `show arp brief`

Mode Privileged EXEC

Term	Definition
Age Time (seconds)	The time (in seconds) it takes for an ARP entry to age out. This value is configurable.
Response Time (seconds)	The time (in seconds) it takes for an ARP request timeout. This value is configurable.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current/ Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current/ Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format `show arp switch`

Mode Privileged EXEC

Term	Definition
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing slot/port associated with the device's ARP entry.

IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

routing

This command enables IPv4 and IPv6 routing for an interface or range of interfaces. You can view the current value for this function with the `show ip brief` command. The value is labeled as `Routing Mode`.

Default	disabled
Format	`routing`
Mode	Interface Config

no routing

This command disables routing for an interface. You can view the current value for this function with the `show ip brief` command. The value is labeled as `Routing Mode`.

Format	`no routing`
Mode	Interface Config

ip routing

This command enables the IP Router Admin Mode for the master switch.

Format	`ip routing`
Mode	Global Config

no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format	`no ip routing`
Mode	Global Config

ip address

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface by specifying the `secondary` option. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links. This command adds the label IP address in the command **"show ip interface" on page 326**.

Note: The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because the EdgeSwitch acts as a host, not a router, on these management interfaces.

Format	`ip address` *`ipaddr`* `{`*`subnetmask`* `|` */masklen*`}` `[secondary]`
Mode	Interface Config

Parameter	Description
`ipaddr`	The IP address of the interface.
`subnetmask`	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
`masklen`	Implements RFC 3021. Using the "/" notation of the subnet mask, this is an integer that indicates the length of the subnet mask. Range is 5 to 32 bits.

Example: The following example of the command shows the configuration of the subnet mask with an IP address in the dotted decimal format on interface 4/1.

```
(UBNT EdgeSwitch) #config
(UBNT EdgeSwitch) (Config)#interface 4/1
(UBNT EdgeSwitch) (Interface 4/1)#ip address 192.168.10.1 255.255.255.254
```

Example: The following example shows the configuration of the subnet mask with an IP address in the "/" notation on interface 4/1.

```
(UBNT EdgeSwitch) #config
(UBNT EdgeSwitch) (Config)#interface 4/1
(UBNT EdgeSwitch) (Interface 4/1)#ip address 192.168.10.1 /31
```

no ip address

This command deletes an IP address from an interface. The value for *ipaddr* is the IP address of the interface in *a.b.c.d* format where the range for *a*, *b*, *c*, and *d* is 1-255. The value for *subnetmask* is a 4-digit dotted-decimal number which represents the subnet mask of the interface. To remove *all* of the IP addresses (primary and secondary) configured on the interface, enter the command `no ip address`.

Format	`no ip address [{`*ipaddr subnetmask* `[secondary]}]`
Mode	Interface Config

ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option, use the `ip address dhcp client-id configuration` command in interface configuration mode.

Default	disabled
Format	`ip address dhcp [client-id]`
Mode	Interface Config

Example: In the following example, DHCPv4 is enabled on interface 4/1.

```
(UBNT EdgeSwitch) #config
(UBNT EdgeSwitch) (Config)#interface 4/1
(UBNT EdgeSwitch) (Interface 4/1)#ip address dhcp
```

no ip address dhcp

This command releases a leased address and disables DHCPv4 on an interface. The `no` form of the `ip address dhcp client-id` command removes the `client-id` option and also disables the DHCP client on the in-band interface.

Format	`no ip address dhcp [client-id]`
Mode	Interface Config

ip default-gateway

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway. The system installs a default IPv4 route with the gateway address as the next hop address. The route preference is 253. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server.

Format	`ip default-gateway` *ipaddr*
Mode	Global Config

Parameter	Description
ipaddr	The IPv4 address of an attached router.

Example: The following example sets the default gateway to 10.1.1.1.

```
(UBNT EdgeSwitch) #config
(UBNT EdgeSwitch) (Config)#ip default-gateway 10.1.1.1
```

no ip default-gateway

This command removes the default gateway address from the configuration.

Format	`no ip default-gateway` *`ipaddr`*
Mode	Interface Config

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface. The DHCP client sends a DHCP Release message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another.

Format	`release dhcp` *`slot/port`*
Mode	Privileged EXEC

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.



Note: This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format	`renew dhcp` *`slot/port`*
Mode	Privileged EXEC

renew dhcp network-port

Use this command to renew an IP address on a network port.

Format	`renew dhcp network-port`
Mode	Privileged EXEC

renew dhcp service-port

Use this command to renew an IP address on a service port.

Format	`renew dhcp service-port`
Mode	Privileged EXEC

ip route

This command configures a static route. The *`ipaddr`* parameter is a valid IP address, and *`subnetmask`* is a valid subnet mask. The *`nexthopip`* parameter is a valid IP address of the next hop router. Specifying `Null0` for the *`nexthopip`* parameter adds a static reject route.

The optional *`preference`* parameter is an integer value (from 1 to 255) that allows you to specify the preference value (sometimes called "administrative distance") of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable IP routing globally.
- Enable IP routing for the interface.
- Confirm that the associated link is also up.

Default	preference – 1
Format	`ip route ipaddr subnetmask [nexthopip | Null0] [preference]`
Mode	Global Config

no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* parameter, the next hop is deleted. If you use the *preference* value, the preference value of the static route is reset to its default.

Format	`no ip route ipaddr subnetmask [{nexthopip [preference] | Null0}]`
Mode	Global Config

ip route default

This command configures the default route. The value for *nexthopip* is a valid IP address of the next hop router. The *preference* is an integer value from 1-255. A route with a preference of 255 cannot be used to forward traffic.

Default	preference – 1
Format	`ip route default nexthopip [preference]`
Mode	Global Config

no ip route default

This command deletes all configured default routes. If the optional *nexthopip* parameter is designated, the specific next hop is deleted from the configured default route and if the optional *preference* value is designated, the preference of the configured default route is reset to its default.

Format	`no ip route default [{nexthopip | preference}]`
Mode	Global Config

ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The `ip route` and `ip route default` commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the `ip route distance` command.

Default	1
Format	`ip route distance 1-255`
Mode	Global Config

no ip route distance

This command sets the static route preference value in the router to the default. Lower route preference values are preferred when determining the best route.

Format	`no ip route distance`
Mode	Global Config

ip netdirbcast

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled, they are dropped.

Default	disabled
Format	`ip netdirbcast`
Mode	Interface Config

no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network-directed broadcasts are dropped.

Format	`no ip netdirbcast`
Mode	Interface Config

ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface. Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency (unless OSPF has been instructed to ignore differences in IP MTU with the `ip ospf mtu-ignore` command).

Note: The IP MTU size refers to the maximum size of the IP packet (IP header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see **"mtu" on page 198**) must take into account the size of the Ethernet header.

Default	1500 bytes
Format	`ip mtu` *`68-9198`*
Mode	Interface Config

no ip mtu

This command resets the IP MTU to the default value.

Format	`no ip mtu`
Mode	Interface Config

encapsulation

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be `ethernet` or `snap`.

Default	ethernet
Format	`encapsulation {ethernet | snap}`
Mode	Interface Config

Note: Routed frames are always Ethernet-encapsulated when a frame is routed to a VLAN.

show dhcp lease

This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

Format `show dhcp lease [interface slot/port]`

Mode Privileged EXEC

Term	Definition
IP address, Subnet mask	The IP address and network mask leased from the DHCP server.
DHCP Lease server	The IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface.
DHCP transaction ID	The transaction ID of the DHCPv4 Client.
Lease	The time (in seconds) that the IP address was leased by the server.
Renewal	The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address.
Rebind	The time (in seconds) when the DHCP Rebind process starts.
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds.

show ip brief

This command displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format `show ip brief`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. Burst-interval is from 0 to 2147483647 milliseconds. The default burst-interval is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip brief

Default Time to Live.......................... 64
Routing Mode.................................. Disabled
Maximum Next Hops............................. 4
Maximum Routes................................ 128
ICMP Rate Limit Interval...................... 1000 msec
ICMP Rate Limit Burst Size.................... 100 messages
ICMP Echo Replies............................. Enabled
ICMP Redirects................................ Enabled
```

show ip interface

This command displays all pertinent information about the IP interface. The parameter *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format show ip interface {*slot/port* | vlan *1-4093*}

Modes Privileged EXEC, User EXEC

Term	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Routing Mode	The administrative mode of router interface participation. The possible values are Enable or Disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are Enable or Disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled (Enable) or disabled (Disable). This value is configurable.
Active State	Displays whether the interface is Active or Inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned-in physical address of the specified interface. The format is six 2-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (Enabled or Disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (Enabled or Disabled).
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the in-band interface. See **"ip address dhcp" on page 321**.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)#show ip interface 0/2

Routing Interface Status..................... Down
Primary IP Address........................... 1.2.3.4/255.255.255.0
Method....................................... Manual
Secondary IP Address(es)..................... 21.2.3.4/255.255.255.0
.............................................. 22.2.3.4/255.255.255.0
Helper IP Address............................ 1.2.3.4
.............................................. 1.2.3.5
Routing Mode................................. Disable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts.............. Disable
Active State................................. Inactive
Link Speed Data Rate......................... Inactive
MAC Address.................................. 00:10:18:82:0C:68
Encapsulation Type........................... Ethernet
IP MTU....................................... 1500
Bandwidth.................................... 100000 kbps
Destination Unreachables..................... Enabled
ICMP Redirects............................... Enabled
```

Example: In the following example the DHCP client is enabled on a VLAN routing interface.

```
(UBNT EdgeSwitch) #show ip interface vlan 10

Routing Interface Status..................... Up
Method.......................................... DHCP
Routing Mode.................................... Enable
Administrative Mode............................. Enable
Forward Net Directed Broadcasts................. Disable
Active State.................................... Inactive
Link Speed Data Rate............................ 10 Half
MAC address..................................... 00:10:18:82:16:0E
Encapsulation Type.............................. Ethernet
IP MTU.......................................... 1500
Bandwidth....................................... 10000 kbps
Destination Unreachables........................ Enabled
ICMP Redirects.................................. Enabled
Interface Suppress Status....................... Unsuppressed
```

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router, and indicates how each IP address was assigned.

Format `show ip interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Method	Indicates how each IP address was assigned. The field contains one of the following values: • **DHCP** The address is leased from a DHCP server. • **Manual** The address is manually configured.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip interface brief

Interface    State  IP Address      IP Mask         Method
----------   -----  --------------- --------------- --------
  0/17       Up     192.168.75.1    255.255.255.0   DHCP
```

show ip route

This command displays the routing table. The *ip-address* specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The *mask* specifies the subnet mask for the given *ip-address*. When you use the `longer-prefixes` keyword, the *ip-address* and *mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *protocol* parameter to specify the protocol that installed the routes. The value for *protocol* can be `connected` or `static`. Use the `all` parameter to display all routes including best and nonbest routes. If you do not use the `all` parameter, the command displays only the best route.

Note: If you use the `connected` keyword for *protocol*, the `all` option is not available because there are no best or nonbest connected routes.

Note: If you use the `static` keyword for *`protocol`*, the `description` option is also available, for example: `show ip route` *`ip-address`* `static description`. This command shows the description configured with the specified static route(s).

Format `show ip route [{`*`ip-address`* `[`*`protocol`*`] | {`*`ip-address mask`* `[longer-prefixes] [`*`protocol`*`] | `*`protocol`*`} [all] | all}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The `show ip route` command displays the routing tables in the following format:

```
Code   IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated
```

The columns for the routing table display the following information:

Term	Definition
Code	The codes for the routing protocols that created the routes.
Default Gateway	The IP address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp is: Days:Hours:Minutes if days ≥ 1 Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.
T	This flag is appended to a route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a T after the interface name.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip route

Route Codes: C - Connected, S - Static

Default gateway is 1.1.1.2

C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,   00h:00m:01s,  0/5
C 11.11.11.0/24 [0/1] directly connected,   0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 10.3.2.0/24 [1/0] via 1.1.1.2, 0/11
```

Example: The following shows example CLI display output for the command to indicate a truncated route.

```
(UBNT EdgeSwitch) #show ip route

Route Codes: C - Connected, S - Static

O E1   100.1.161.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.162.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.163.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
```

show ip route ecmp-groups

This command reports all current ECMP groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv4 address and outgoing interface of each next hop in each group.

Format	`show ip route ecmp-groups`
Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip route ecmp-groups

ECMP Group 1 with 2 next hops (used by 1 route)
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34

ECMP Group 2 with 3 next hops (used by 1 route)
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34

ECMP Group 3 with 4 next hops (used by 1 route)
  172.20.31.100 on interface 2/31
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
```

show ip route summary

This command displays a summary of the state of the routing table. When the optional `all` keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Format	`show ip route summary [all]`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by the BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.

Term	Definition
OSPF Routes	Total number of routes installed by OSPF protocol.
Intra Area Routes	Total number of Intra Area routes installed by OSPF protocol.
Inter Area Routes	Total number of Inter Area routes installed by OSPF protocol.
External Type-1 Routes	Total number of External Type-1 routes installed by OSPF protocol.
External Type-2 Routes	Total number of External Type-2 routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination. The value in parentheses indicates the highest count of unique best routes since counters were last cleared.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes. The value in parentheses indicates the highest count of unique next hops since counters were last cleared.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip route summary
Connected Routes.............................. 7
Static Routes................................. 1
RIP Routes.................................... 20
BGP Routes.................................... 10
  External.................................... 0
  Internal.................................... 10
  Local....................................... 0
```

```
OSPF Routes..................................... 1004
  Intra Area Routes............................. 4
  Inter Area Routes............................. 1000
  External Type-1 Routes........................ 0
  External Type-2 Routes........................ 0
Reject Routes..................................... 0
Total routes...................................... 1032

Best Routes (High)................................ 1032 (1032)
Alternate Routes.................................. 0
Route Adds........................................ 1010
Route Modifies.................................... 1
Route Deletes..................................... 10
Unresolved Route Adds............................. 0
Invalid Route Adds................................ 0
Failed Route Adds................................. 0
Reserved Locals................................... 0

Unique Next Hops (High)........................... 13 (13)
Next Hop Groups (High)............................ 13 (14)
ECMP Groups (High)................................ 2 (3)
ECMP Routes....................................... 1001
Truncated ECMP Routes............................. 0
ECMP Retries...................................... 0
Routes with 1 Next Hop............................ 31
Routes with 2 Next Hops........................... 1
Routes with 4 Next Hops........................... 1000
```

clear ip route counters

The command resets to zero the IPv4 routing table counters reported in the command **"show ip route summary" on page 329**. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format	`clear ip route counters`
Mode	Privileged EXEC

show ip route preferences

This command displays detailed information about the route preferences for each type of route. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format	`show ip route preferences`
Modes	Privileged EXEC, User EXEC

Term	Definition
Local	The local route preference value.
Static	The static route preference value.
Configured Default Gateway	The route preference value of the statically-configured default gateway
DHCP Default Gateway	The route preference value of the default gateway learned from the DHCP server.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip route preferences

Local.......................................... 0
Static......................................... 1
Configured Default Gateway..................... 253
DHCP Default Gateway........................... 254
```

show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format	`show ip stats`
Modes	Privileged EXEC, User EXEC

show routing heap summary

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

Format	`show routing heap summary`
Mode	Privileged EXEC

Parameter	Description
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show routing heap summary

Heap Size..................... 95053184
Memory In Use................. 56998
Memory on Free List........... 47
Memory Available in Heap...... 94996170
In Use High Water Mark........ 57045
```

Routing Policy Commands

This section describes the commands you use to configure IP routing policies on the switch.

ip policy route-map

Use this command to identify a route map to use for policy-based routing on an interface specified by *route-map-name*. Policy-based routing is configured on the interface that *receives* the packets, not on the interface from which the packets are sent.

When a route-map applied on the interface is changed – that is, if new statements are added to route-map or match/set terms are added or removed from route-map statement, or if route-map that is applied on an interface is removed – then route-map needs to be removed from the interface and added back again in order for the changed route-map configuration to be effective.

Format	`ip policy route-map-name`
Mode	Interface Config

Example: The following is an example of this command.

```
(UBNT EdgeSwitch) (Config)#interface 0/1
(UBNT EdgeSwitch) (Interface 0/1)#
(UBNT EdgeSwitch) (Interface 0/1)# #ip policy route-map equal-access
```

In order to disable policy based routing from an interface, use the `no` form of this command:

```
no ip policy route-map-name
```

ip prefix-list

To create a prefix list or add a prefix list entry, use the `ip prefix-list` command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route's prefix using the `match ip address` command (**"match ip address" on page 335**).

Up to 128 prefix lists may be configured. The maximum number of statements allowed in the prefix list is 64.

Default	No prefix lists are configured by default. When neither the `ge` nor the `le` option is configured, the destination prefix must match the network/length exactly. If the `ge` option is configured without the `le` option, any prefix with a network mask greater than or equal to the `ge` value is considered a match. Similarly, if the `le` option is configured without the `ge` option, a prefix with a network mask less than or equal to the `le` value is considered a match.
Format	`ip prefix-list list-name {[seq number] {permit | deny} network/length [ge length] [le length] | renumber renumber-interval first-statement-number}`
Mode	Global Configuration

Parameter	Description
list-name	The text name of the prefix list. Up to 32 characters.
`seq` *number*	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered by this number (lowest to highest) and applied in that order. If no sequence number is specified, the system automatically selects a sequence number five larger than the last sequence number in the list. Two statements may not be assigned the same sequence number. The value ranges from 1 to 4,294,967,294.
`permit`	Permit routes whose destination prefix matches the statement.
`deny`	Deny routes whose destination prefix matches the statement.
network/length	Specifies the match criteria for routes being compared to the prefix list statement. The network can be any valid IP prefix. The length is any IPv4 prefix length from 0 to 32.
`ge` *length*	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.

Parameter	Description
`le length`	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.
`renumber`	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for *renumber-interval* is 1 – 100, and the valid range for *first-statement-number* is 1 – 1000.

Example: The following example configures a prefix list that allows routes with one of two specific destination prefixes, 172.20.0.0/16 and 192.168.1.0/24:

```
(UBNT EdgeSwitch)(config)# ip prefix-list apple seq 10 permit 172.20.0.0/16
(UBNT EdgeSwitch)(config)# ip prefix-list apple seq 20 permit 192.168.10/24
```

Example: The following example disallows only the default route.

```
(UBNT EdgeSwitch)(config)# ip prefix-list orange deny 0.0.0.0/0
(UBNT EdgeSwitch)(config)# ip prefix-list orange permit 0.0.0.0/0 ge 1
```

no ip prefix-list

To delete a prefix list or a statement in a prefix list, use the `no` form of this command. The command `no ip prefix-list list-name` deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Format	`no ip prefix-list` *list-name* `[seq` *number*`] { permit | deny } network/length [ge` *length*`] [le` *length*`]`
Mode	Global Configuration

ip prefix-list description

To apply a text description to a prefix list, use the `ip prefix-list description` command in Global Configuration mode.

Default	No description is configured by default.
Format	`ip prefix-list` *list-name* `description` *text*
Mode	Global Configuration

Parameter	Description
list-name	The text name of the prefix list.
`description` *text*	Text description of the prefix list. Up to 80 characters.

no ip prefix-list description

To remove the text description, use the `no` form of this command.

route-map

To create a route map and enter Route Map Configuration mode, use the `route-map` command in Global Configuration mode. One use of a route map is to limit the redistribution of routes to a specified range of route prefixes.

The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed. EdgeSwitch accepts up to 64 route maps.

Default	No route maps are configured by default. If no permit or deny tag is given, permit is the default.
Format	`route-map` *map-tag* `[permit|deny] [`*sequence-number*`]`
Mode	Global Configuration

Parameter	Description
map-tag	Text name of the route map. Route maps with the same name are grouped together in order of their sequence numbers. A route map name may be up to 32 characters long.
permit	(Optional) Permit routes that match all of the match conditions in the route map.
deny	(Optional) Deny routes that match all of the match conditions in the route map.
sequence-number	(Optional) An integer used to order the set of route maps with the same name. Route maps are ordered from lowest to greatest sequence number, with lower sequence numbers being considered first. If no sequence number is specified, the system assigns a value ten greater than the last statement in the route map. The range is 0 to 65,535.

no route-map

To delete a route map or one of its statements, use the `no` form of this command.

Format `no route-map map-tag [permit|deny] [sequence-number]`

Mode Global Configuration

match ip address

To configure a route map to match based on a destination prefix, use the `match ip address` command in Route Map Configuration mode. If you specify multiple prefix lists in one statement, then a match occurs if a prefix matches any one of the prefix lists. If you configure a `match ip address` statement within a route map section that already has a `match ip address` statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default No match criteria are defined by default.

Format `match ip address prefix-list prefix-list-name [prefix-list-name...]`

Mode Route Map Configuration

Parameter	Description
prefix-list-name	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

no match ip address

To delete a match statement from a route map, use the `no` form of this command.

Format `no match ip address [prefix-list prefix-list-name [prefix-list-name...]]`

Mode Route Map Configuration

match ip address *access-list-number | access-list-name*

Use this command to configure a route map in order to match based on the match criteria configured in an IP access-list. Note that an IP ACL must be configured before it is linked to a route-map. Actions present in an IP ACL configuration are applied with other actions involved in route-map. If an IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

If you specify multiple access lists in one statement, a match occurs if a prefix matches any one of the prefix lists. If there are duplicate IP access-list numbers/names in this command, the duplicate configuration is ignored.

Default No match criteria are defined by default.

Format `match ip address access-list-number | access-list-name [...access-list-number | access-list-name ]`

Mode Route Map Configuration

Parameter	Description
access-list-number	The number that identifies an access list configured through access list CLI configuration commands. 1 to 99 for standard access list number. This number is 100 to 199 for extended access list number.
access-list-name	The access-list name that identifies named IP ACLs. Access-list name can be up to 31 characters in length. A maximum of 16 ACLs can be specified in this 'match' clause.

Example: The following sequence shows an example of creating a route-map with the "match" clause on an ACL number and applying that route-map on an interface, where:

- The `ip policy route-map equal-access` command is applied to interface 0/1. All packets coming inside 0/1 are policy-routed.
- Sequence number 10 in route map `equal-access` is used to match all packets sourced from any host in subnet 10.1.0.0. If there is a match, and if the router has no explicit route for the packet's destination, it is sent to next-hop address 192.168.6.6.
- Sequence number 20 in route map `equal-access` is used to match all packets sourced from any host in subnet 10.2.0.0. If there is a match, and if the router has no explicit route for the packet's destination, it is sent to next-hop address 172.16.7.7.
- All other packets are forwarded as per normal L3 destination-based routing.

```
(UBNT EdgeSwitch) (config)#access-list 1 permit ip 10.1.0.0 0.0.255.255
(UBNT EdgeSwitch) (config)#access-list 2 permit ip 10.2.0.0 0.0.255.255
(UBNT EdgeSwitch) (config)#route-map equal-access permit 10
(UBNT EdgeSwitch) (config-route-map)#match ip address 1
(UBNT EdgeSwitch) (config-route-map)#set ip default next-hop 192.168.6.6
(UBNT EdgeSwitch) (config-route-map)#route-map equal-access permit 20
(UBNT EdgeSwitch) (config-route-map)#match ip address 2
(UBNT EdgeSwitch) (config-route-map)#set ip default next-hop 172.16.7.7
(UBNT EdgeSwitch) (config)#interface 0/1
(UBNT EdgeSwitch) (Interface 0/1)#ip address 10.1.1.1 255.255.255.0
(UBNT EdgeSwitch) (Interface 0/1)#ip policy route-map equal-access
(UBNT EdgeSwitch) (config)#interface 0/2
(UBNT EdgeSwitch) (Interface 0/2)#ip address 192.168.6.5 255.255.255.0
(UBNT EdgeSwitch) (config)#interface 0/3
(UBNT EdgeSwitch) (Interface 0/3)#ip address 172.16.7.6 255.255.255.0
```

Example: This example illustrates the scenario where an IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL (this is how configuration is rejected):

```
(UBNT EdgeSwitch) #show ip access-lists

Current number of ACLs: 9  Maximum number of ACLs: 100

ACL ID/Name                     Rules  Direction  Interface(s)      VLAN(s)
------------------------------  -----  ---------  ----------------  ----------
1                               1
2                               1
3                               1
4                               1
5                               1
madan                           1

(UBNT EdgeSwitch) #show mac access-lists

Current number of all ACLs: 9  Maximum number of all ACLs: 100

MAC ACL Name                    Rules  Direction  Interface(s)       VLAN(s)
------------------------------  -----  ---------  ----------------  ----------
madan                           1
mohan                           1
goud                            1

(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure

(UBNT EdgeSwitch) (Config)#route-map madan
```

```
(UBNT EdgeSwitch) (route-map)#match ip address 1 2 3 4 5 madan

(UBNT EdgeSwitch) (route-map)#match mac-list madan mohan goud

(UBNT EdgeSwitch) (route-map)#exit

(UBNT EdgeSwitch) (Config)#exit

(UBNT EdgeSwitch) #show route-map

route-map madan permit 10
     Match clauses:
       ip address (access-lists) : 1 2 3 4 5 madan
       mac-list (access-lists) : madan mohan goud
     Set clauses:

(UBNT EdgeSwitch) (Config)#access-list 2 permit every

Request denied. Another application using this ACL restricts the number of rules allowed.

(UBNT EdgeSwitch) (Config)#ip access-list madan

(UBNT EdgeSwitch) (Config-ipv4-acl)#permit udp any any

Request denied. Another application using this ACL restricts the number of rules allowed.
```

no match ip address

To delete a match statement from a route map, use the `no` form of this command.

Format	`no match ip address [access-list-number | access-list-name]`
Mode	Route Map Configuration

match length

Use this command to configure a route map to match based on the Layer-3 packet length between specified minimum and maximum values. The *`min`* parameter specifies the packet's minimum Layer-3 length, inclusive, allowed for a match. The *`max`* parameter specifies the packet's maximum Layer-3 length, inclusive, allowed for a match. Each route-map statement can contain one 'match' statement on packet length range.

Default	No match criteria are defined by default.
Format	`match length min max`
Mode	Route Map Configuration

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (config-route-map)# match length 64 1500
```

no match length

Use this command to delete a match statement from a route map.

Format	`no match length`
Mode	Route Map Configuration

match mac-list

Use this command to configure a route map in order to match based on the match criteria configured in a MAC access-list.

A MAC ACL is configured before it is linked to a route-map. Actions present in MAC ACL configuration are applied with other actions involved in route-map. When a MAC ACL referenced by a route-map is removed, the route-map rule is also removed and the corresponding rule is not effective.

When a MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

Default	No match criteria are defined by default.
Format	`match mac-list mac-list-name [mac-list-name]`
Mode	Route Map Configuration

Parameter	Description
mac-list-name	The mac-list name that identifies MAC ACLs. MAC Access-list name can be up to 31 characters in length.

Example: The following is an example of the command.

```
(UBNT EdgeSwitch) (config-route-map)# match mac-list MacList1
```

Example: This example illustrates the scenario where a MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL (this is how configuration is rejected):

```
(UBNT EdgeSwitch) #show mac access-lists

Current number of all ACLs: 9  Maximum number of all ACLs: 100

MAC ACL Name                     Rules  Direction  Interface(s)       VLAN(s)
-------------------------------  -----  ---------  ----------------  ----------
madan                            1
mohan                            1
goud                             1

(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #
(UBNT EdgeSwitch) #configure

(UBNT EdgeSwitch) (Config)#route-map madan

(UBNT EdgeSwitch) (route-map)#match mac-list madan mohan goud

(UBNT EdgeSwitch) (route-map)#exit

(UBNT EdgeSwitch) (Config)#exit

(UBNT EdgeSwitch) #show route-map

route-map madan permit 10
     Match clauses:
       mac-list (access-lists) : madan mohan goud
     Set clauses:

(UBNT EdgeSwitch) (Config)#mac access-list extended madan

(UBNT EdgeSwitch) (Config-mac-access-list)#permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:ff any

Request denied. Another application using this ACL restricts the number of rules allowed.
```

no match mac-list

To delete a match statement from a route map, use the `no` form of this command.

Format	`no match mac-list [...mac-list-name]`
Mode	Route Map Configuration

set interface

If the network administrator does not want to revert to normal forwarding but instead wants to drop a packet that does not match the specified criteria, a `set` statement needs to be configured to route the packets to interface `null0` as the last entry in the route-map.

Configure `set interface null0` in a separate statement. It should not be added along with any other statement having other match/set terms.

A route-map statement that is used for PBR is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet meeting the match criteria. If the statement is marked as permit, and if the packet meets all the match criteria, then `set` commands in the route-map statement are applied. If no match is found in the route-map, the packet is not dropped; instead the packet is forwarded using the routing decision taken by performing destination-based routing.

Format	`set interface null0`
Mode	Route Map Configuration

set ip next-hop

Use this command to specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IP address is specified, the first IP address associated with a currently up-connected interface is used to route the packets.

This command affects all incoming packet types and is always used if configured. If the configured next-hop is not present in the routing table, an ARP request is sent from the router. In a route-map statement, the terms `set ip next-hop` and `set ip default next-hop` are mutually exclusive; however, `set ip default next-hop` can be configured in a separate route-map statement.

Format	`set ip next-hop ip-address [...ip-address]`
Mode	Route Map Configuration

Parameter	Description
ip-address	The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this `set` clause.

no set ip next-hop

Use this command to remove a `set` command from a route map.

Format	`no set ip next-hop ip-address [...ip-address]`
Mode	Route Map Configuration

set ip default next-hop

Use this command to set a list of default next-hop IP addresses. If more than one IP address is specified, the first next-hop specified that appears to be adjacent to the router is used. The optional specified IP addresses are tried in turn.

A packet is routed to the next hop specified by this command only if there is *no* explicit route for the packet's destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.

In a route-map statement, the terms `set ip next-hop` and `set ip default next-hop` are mutually exclusive; however, `set ip next-hop` can be configured in a separate route-map statement.

Format `set ip default next-hop ip-address [...ip-address]`

Mode Route Map Configuration

Parameter	Description
ip-address	The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this `set` clause.

no set ip default next-hop

Use this command to remove a `set` command from a route map.

Format `no set ip default next-hop ip-address [...ip-address]`

Mode Route Map Configuration

set ip precedence

Use this command to set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the IP precedence; values 0 through 7 are defined. This command is used when implementing QoS and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Format `set ip precedence 0-7`

Mode Route Map Configuration

Parameter	Description
0	Sets the routine precedence
1	Sets the priority precedence
2	Sets the immediate precedence
3	Sets the Flash precedence
4	Sets the Flash override precedence
5	Sets the critical precedence
6	Sets the internetwork control precedence
7	Sets the network control precedence

no set ip precedence

Use this command to reset the three IP precedence bits in the IP packet header to the default.

Format `no set ip precedence`

Mode Route Map Configuration

show ip policy

This command lists the route map associated with each interface.

Format `show ip policy`

Mode Privileged Exec

Term	Definition
Interface	The interface
Route-map	The route map

show ip prefix-list

This command displays configuration and status for a prefix list.

Format `show ip prefix-list [detail | summary] prefix-list-name [network/length] [seq sequence-number] [longer] [first-match]`

Mode Privileged EXEC

Parameter	Description
`detail | summary`	(Optional) Displays detailed or summarized information about all prefix lists.
`prefix-list-name`	(Optional) The name of a specific prefix list.
`network/length`	(Optional) The network number and length (in bits) of the network mask.
`seq`	(Optional) Applies the sequence number to the prefix list entry.
`sequence-number`	(Optional) The sequence number of the prefix list entry.
`longer`	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
`first-match`	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

```
show ip prefix-list prefix-list-name network/length first-match
show ip prefix-list prefix-list-name network/length longer
show ip prefix-list prefix-list-name network/length
show ip prefix-list prefix-list-name seq sequence-number
show ip prefix-list prefix-list-name
show ip prefix-list summary
show ip prefix-list summary prefix-list-name
show ip prefix-list detail
show ip prefix-list detail prefix-list-name
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip prefix-list fred

ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
   seq 5 permit 10.10.1.1/20 ge 22
   seq 10 permit 10.10.1.2/20 le 30
   seq 15 permit 10.10.1.2/20 ge 29 le 30
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip prefix-list summary fred

ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip prefix-list detail fred

ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
   seq 5 permit 10.10.1.1/20 ge 22 (hitcount: 0)
   seq 10 permit 10.10.1.2/20 le 30 (hitcount: 0)
   seq 15 permit 10.10.1.2/20 ge 29 le 30 (hitcount: 0)
```

show route-map

To display a route map, use the `show route-map` command in Privileged EXEC mode.

Format	`show route-map [map-name]`
Mode	Privileged EXEC

Parameter	Description
map-name	(Optional) Name of a specific route map.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) # show route-map test

route-map test, permit, sequence 10
     Match clauses:
       ip address prefix-lists: orange
            Set clauses:
              set metric 50
```

clear ip prefix-list

To reset IP prefix-list counters, use the `clear ip prefix-list` command in Privileged EXEC mode. This command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Format	`clear ip prefix-list [[prefix-list-name] [network/length]]`
Mode	Privileged EXEC

Parameter	Description
prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) Network number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) # clear ip prefix-list orange 20.0.0.0/8
```

Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

ip irdp

This command enables router discovery on an interface or range of interfaces.

Default	disabled
Format	`ip irdp`
Mode	Interface Config

no ip irdp

This command disables router discovery on an interface.

Format	`no ip irdp`
Mode	Interface Config

ip irdp address

This command configures the address that the interface uses to send the router discovery advertisements. The valid values for *`ipaddr`* are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

Default	224.0.0.1
Format	`ip irdp address` *`ipaddr`*
Mode	Interface Config

no ip irdp address

This command sets the address used to advertise the router for the interface to the default.

Format	`no ip irdp address`
Mode	Interface Config

ip irdp holdtime

This command configures the value, in seconds, of the `holdtime` field of the router advertisement sent from this interface. The `holdtime` range is 4 to 9000 seconds.

Default	3 * maxinterval
Format	`ip irdp holdtime` *`4-9000`*
Mode	Interface Config

no ip irdp holdtime

This command sets the value, in seconds, of the `holdtime` field of the router advertisement sent from this interface, to the default.

Format	`no ip irdp holdtime`
Mode	Interface Config

ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for `maxadvertinterval` is 4 to 1800 seconds.

Default	600
Format	`ip irdp maxadvertinterval` *`4-1800`*
Mode	Interface Config

no ip irdp maxadvertinterval

This command sets the maximum time, in seconds to the default.

Format	`no ip irdp maxadvertinterval`
Mode	Interface Config

ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for `minadvertinterval` is 3–1800 seconds.

Default	0.75 * maxadvertinterval
Format	`ip irdp minadvertinterval 3-1800`
Mode	Interface Config

no ip irdp minadvertinterval

This command sets the `minadvertinterval` to the default.

Format	`no ip irdp minadvertinterval`
Mode	Interface Config

ip irdp multicast

This command configures the destination IP address for router advertisements as 224.0.0.1, which is the default address. The `no` form of the command configures the IP address as 255.255.255.255 to send router advertisements to the limited broadcast address.

Format	`ip irdp multicast ip-address`
Mode	Interface Config

no ip irdp multicast

To send router advertisements to the limited broadcast address, 255.255.255.255, instead of the default IP address of 224.0.0.1, use the `no` form of this command.

Format	`no ip irdp multicast`
Mode	Interface Config

ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Default	0
Format	`ip irdp preference -2147483648 to 2147483647`
Mode	Interface Config

no ip irdp preference

This command sets the preferability of the address as a default router address, relative to other router addresses on the same subnet, to the default.

Format	`no ip irdp preference`
Mode	Interface Config

show ip irdp

This command displays the router discovery information for all interfaces, a specified interface, or specified VLAN. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Format show ip irdp {*slot/port* | vlan *1-4093* | all}

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
slot/port	The slot/port that corresponds to a physical routing interface or vlan routing interface.
vlan	Use this keyword to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Term	Definition
Interface	The slot/port that corresponds to a physical routing interface or vlan routing interface.
vlan	Use this keyword to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.
Ad Mode	The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Dest Address	The destination IP address for router advertisements.
Max Int	The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	The amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	The preference of the address as a default router address, relative to other router addresses on the same subnet.

Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

vlan routing

This command enables routing on a VLAN. The *vlanid* value has a range of 1-4093. The *interface-ID* value has a range of 1-128. Typically, you will not supply the *interface-ID* argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the slot/port for the VLAN routing interface. If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the `vlan routing` command for the text configuration ensures that the slot/port for the VLAN interface stays the same across a restart. Keeping the slot/port the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format	`vlan routing` *vlanid* [*interface-ID*]
Mode	VLAN Config

no vlan routing

This command deletes routing on a VLAN.

Format	`no vlan routing` *vlanid*
Mode	VLAN Config

Example 1: This example shows the command specifying a *vlanid* value. The *interface-ID* argument is not used.

```
(UBNT EdgeSwitch)(Vlan)#vlan 14
(UBNT EdgeSwitch)(Vlan)#vlan routing 14 ?
<cr>                      Press enter to execute the command.
<1-24>                   Enter interface ID
```

Typically, you press **Enter** without supplying the interface ID value; the system automatically selects the interface ID.

Example 2: In this example, the command specifies interface ID 51 for the VLAN 14 interface. The interface ID becomes the port number in the slot/port for the VLAN routing interface. In this example, the slot/port is 4/51 for the VLAN 14 interface.

```
(UBNT EdgeSwitch)(Vlan)#vlan 14 51
(UBNT EdgeSwitch)(Vlan)#
(UBNT EdgeSwitch)#show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36

           Logical
VLAN ID    Interface        IP Address       Subnet Mask
-------  --------------  ---------------  ---------------
10       4/1             172.16.10.1      255.255.255.0
11       4/50            172.16.11.1      255.255.255.0
12       4/3             172.16.12.1      255.255.255.0
13       4/4             172.16.13.1      255.255.255.0
14       4/51            0.0.0.0          0.0.0.0          <— slot/port is 4/51 for VLAN 14 interface
```

Example 3: In this example, an interface ID that is already in use is selected. In this case, the CLI displays an error message and does not create the VLAN interface.

```
(UBNT EdgeSwitch) #show ip vlan

MAC Address used by Routing VLANs:   00:11:88:59:47:36
```

```
           Logical
VLAN ID    Interface         IP Address        Subnet Mask
-------  --------------  ---------------  ---------------
10         4/1             172.16.10.1      255.255.255.0
11         4/50            172.16.11.1      255.255.255.0
12         4/3             172.16.12.1      255.255.255.0
13         4/4             172.16.13.1      255.255.255.0
14         4/51            0.0.0.0          0.0.0.0

(UBNT EdgeSwitch)#config

(UBNT EdgeSwitch)(Config)#exit

(UBNT EdgeSwitch)#vlan database

(UBNT EdgeSwitch)(Vlan)#vlan 15

(UBNT EdgeSwitch)(Vlan)#vlan routing 15 1

Interface ID 1 is already assigned to another interface
```

Example 4: The `show running configuration` command always lists the interface ID for each routing VLAN, as shown below.

```
(UBNT EdgeSwitch) #show running-config
!Current Configuration:
!
!System Description "EdgeSwitch 24-Port 500W, 0.8.0.4712594, Linux 3.6.5-f4a26ed5"
!System Software Version "0.8.0.4712594"
!System Up Time          "1 days 4 hrs 22 mins 0 secs"
!Additional Packages     QOS,IPv6 Management,Routing
!Current SNTP Synchronized Time: SNTP Last Attempt Status Is Not Successful
!
vlan database
exit

configure
no logging console
aaa authentication enable “enableNetList” none
line console
serial timeout 0
exit

line telnet
exit

line ssh
exit

!
router rip
exit
router ospf
exit
ipv6 router ospf
exit
exit
```

interface vlan

Use this command to enter interface configuration mode for the specified VLAN. The valid *vlan-id* range is from 1 to 4093.

Format `interface vlan vlan-id`

Mode Global Config

show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format `show ip vlan`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical slot/port associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	The subnet mask that is associated with this VLAN.

IP Helper Commands

This section describes the commands to configure and monitor the IP Helper agent. IP Helper relays DHCP and other broadcast UDP packets from a local client to one or more servers which are not on the same network at the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on nonlocal subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet's destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in **Table 12 on page 349**. This is the list of default ports.

Table 12. Default Ports - UDP Port Numbers Implied by Wildcard

Protocol	UDP Port Number
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as he likes. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed.

Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF)
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

clear ip helper statistics

Use this command to reset to zero the statistics displayed in the `show ip helper statistics` command.

Format	`clear ip helper statistics`
Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #clear ip helper statistics
```

ip helper-address (Global Config)

Use this command to configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

Default	No helper addresses are configured.
Format	`ip helper-address server-address [`*`dest-udp-port`*` | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`
Mode	Global Config

Parameter	Description
`server-address`	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
`dest-udp-port`	A destination UDP port number from 0 to 65535.
port name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • **dhcp** Port 67 • **domain** Port 53 • **isakmp** Port 500 • **mobile-ip** Port 434 • **nameserver** Port 42 • **netbios-dgm** Port 138 • **netbios-ns** Port 137 • **ntp** Port 123 • **pim-auto-rp** Port 496 • **rip** Port 520 • **tacacs** Port 49 • **tftp** Port 69 • **time** Port 37 Other ports must be specified by number.

Example: To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
(UBNT EdgeSwitch)#config
(UBNT EdgeSwitch)(config)#ip helper-address 10.1.1.1 dhcp
(UBNT EdgeSwitch)(config)#ip helper-address 10.1.2.1 dhcp
```

Example: To relay UDP packets received on any interface for all default ports to the server at 20.1.1.1, use the following commands:

```
(UBNT EdgeSwitch)#config
(UBNT EdgeSwitch)(config)#ip helper-address 20.1.1.1
```

no ip helper-address (Global Config)

Use the `no` form of the command to delete an IP helper entry. The command `no ip helper-address` with no arguments clears all global IP helper addresses.

Format `no ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Mode Global Config

ip helper-address (Interface Config)

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

Default No helper addresses are configured.

Format `ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Mode Interface Config

Parameter	Description
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be in a subnet on the interface where the relay entry is configured, and cannot be an IP address configured on any interface of the local router.
discard	Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
dest-udp-port	A destination UDP port number from 0 to 65535.
port name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • **dhcp** Port 67 • **domain** Port 53 • **isakmp** Port 500 • **mobile-ip** Port 434 • **nameserver** Port 42 • **netbios-dgm** Port 138 • **netbios-ns** Port 137 • **ntp** Port 123 • **pim-auto-rp** Port 496 • **rip** Port 520 • **tacacs** Port 49 • **tftp** Port 69 • **time** Port 37 Other ports must be specified by number.

Example: To relay DHCP packets received on interface 0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```
(UBNT EdgeSwitch)#config
(UBNT EdgeSwitch)(config)#interface 0/2
(UBNT EdgeSwitch)(interface 0/2)#ip helper-address 192.168.10.1 dhcp
(UBNT EdgeSwitch)(interface 0/2)#ip helper-address 192.168.20.1 dhcp
```

Example: To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```
(UBNT EdgeSwitch)#config
(UBNT EdgeSwitch)(config)#interface 0/2
(UBNT EdgeSwitch)(interface 0/2)#ip helper-address 192.168.30.1 dhcp
(UBNT EdgeSwitch)(interface 0/2)#ip helper-address 192.168.30.1 dns
```

Example: This command takes precedence over an `ip helper-address` command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than 0/2 and 0/17 to 192.168.40.1, relays DHCP and DNS packets received on 0/2 to 192.168.40.2, relays SNMP traps (port 162) received on interface 0/17 to 192.168.23.1, and drops DHCP packets received on 0/17:

```
(UBNT EdgeSwitch)#config
(UBNT EdgeSwitch)(config)#ip helper-address 192.168.40.1 dhcp
(UBNT EdgeSwitch)(config)#interface 0/2
(UBNT EdgeSwitch)(interface 0/2)#ip helper-address 192.168.40.2 dhcp
(UBNT EdgeSwitch)(interface 0/2)#ip helper-address 192.168.40.2 domain
(UBNT EdgeSwitch)(interface 0/2)#exit
(UBNT EdgeSwitch)(config)#interface 0/17
(UBNT EdgeSwitch)(interface 0/17)#ip helper-address 192.168.23.1 162
(UBNT EdgeSwitch)(interface 0/17)#ip helper-address discard dhcp
```

no ip helper-address (Interface Config)

Use this command to delete a relay entry on an interface. The `no` command with no arguments clears all helper addresses on the interface.

Format	`no ip helper-address [server-address | discard ][dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`
Mode	Interface Config

ip helper enable

Use this command to enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the `bootpdhcprelay enable` command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Default	disabled
Format	`ip helper enable`
Mode	Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch)(config)#ip helper enable
```

no ip helper enable

Use the `no` form of this command to disable relay of all UDP packets.

Format	`no ip helper enable`
Mode	Global Config

show ip helper-address

Use this command to display the IP helper address configuration. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format.

Format show ip helper-address [{*slot/port*|vlan *1-4093*}]

Mode Privileged EXEC

Term	Description
Interface	The relay configuration is applied to packets that arrive on this interface. This field is set to any for global IP helper entries.
UDP Port	The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as any are applied to packets with the destination UDP ports listed in Table 4.
Discard	If Yes, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip helper-address

IP helper is enabled

   Interface     UDP Port     Discard   Hit Count   Server Address
---------------  -----------  --------  ----------  ---------------
      0/1           dhcp        No          10       10.100.1.254
                                                     10.100.2.254
      0/17          any         Yes          2
      any           dhcp        No           0       10.200.1.254
```

show ip helper statistics

Use this command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.

Format show ip helper statistics

Mode Privileged EXEC

Term	Description
DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL>1 and having valid source and destination IP addresses.
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	The number of DHCP server messages relayed to a client.
UDP clients messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP clients messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP message hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.

Term	Description
DHCP message with secs field below min	The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)#show ip helper statistics

DHCP client messages received..................... 8
DHCP client messages relayed...................... 2
DHCP server messages received..................... 2
DHCP server messages relayed...................... 2
UDP client messages received...................... 8
UDP client messages relayed....................... 2
DHCP message hop count exceeded max............... 0
DHCP message with secs field below min............ 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL.......................... 0
Packets that matched a discard entry.............. 0
```

ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

ip unreachables

Use this command to enable the generation of ICMP Destination Unreachable messages on an interface or range of interfaces. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default	enable
Format	`ip unreachables`
Mode	Interface Config

no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format	`no ip unreachables`
Mode	Interface Config

ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default	enable
Format	`ip redirects`
Mode	• Global Config • Interface Config

no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the router.

Format	`no ip redirects`
Mode	• Global Config • Interface Config

ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default	enable
Format	`ip icmp echo-reply`
Mode	Global Config

no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format	`no ip icmp echo-reply`
Mode	Global Config

ip icmp error-interval

Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. The *burst-interval* is from 0 to 2147483647 milliseconds (msec). The *burst-size* is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default	*burst-interval* of 1000 msec *burst-size* of 100 messages
Format	`ip icmp error-interval burst-interval [burst-size]`
Mode	Global Config

no ip icmp error-interval

Use the `no` form of the command to return *burst-interval* and *burst-size* to their default values.

Format	`no ip icmp error-interval`
Mode	Global Config

Chapter 6: IPv6 Management Commands

This chapter describes the IPv6 commands available in the EdgeSwitch CLI.

This chapter includes the following sections:

- **"IPv6 Management Commands" on page 358**



Note: The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

IPv6 Management Commands

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (i.e., independent from the IPv6 Routing package). For routing/IPv6 builds dual IPv4/IPv6 operation over the service port is enabled. The EdgeSwitch has capabilities such as:

- Static assignment of IPv6 addresses and gateways for the service/network ports.
- The ability to ping an IPv6 link-local address over the service/network port.
- Using IPv6 management commands, you can send SNMP traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a routing interface or the service port).

network ipv6 enable

Use this command to enable IPv6 operation on the network port.

Default	enabled
Format	`network ipv6 enable`
Mode	Privileged EXEC

no network ipv6 enable

Use this command to disable IPv6 operation on the network port.

Format	`no network ipv6 enable`
Mode	Privileged EXEC

network ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information for the network port. Multiple IPv6 addresses can be configured on the network port.

Format	`network ipv6 address {`*`address/prefix-length`* `[eui64]	autoconfig	dhcp}`
Mode	Privileged EXEC

Parameter	Description
`address`	IPv6 prefix in IPv6 global address format.
`prefix-length`	IPv6 prefix length value.
`eui64`	Formulate IPv6 address in eui64 format.
`autoconfig`	Configure stateless global address autoconfiguration capability.
`dhcp`	Configure dhcpv6 client protocol.

no network ipv6 address

The command `no network ipv6 address` removes all configured IPv6 prefixes.

Use this command with the address option to remove the manually configured IPv6 global address on the network port interface.

Use this command with the autoconfig option to disable the stateless global address autoconfiguration on the network port.

Use this command with the dhcp option disables the dhcpv6 client protocol on the network port.

Format	`no network ipv6 address {`*`address/prefix-length`* `[eui64]	autoconfig	dhcp}`
Mode	Privileged EXEC

network ipv6 gateway

Use this command to configure IPv6 gateway (i.e. default routers) information for the network port.

Format `network ipv6 gateway gateway-address`

Mode Privileged EXEC

Parameter	Description
gateway-address	Gateway address in IPv6 global or link-local address format.

no network ipv6 gateway

Use this command to remove IPv6 gateways on the network port interface.

Format `no network ipv6 gateway`

Mode Privileged EXEC

network ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for this network port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format `network ipv6 neighbor ipv6-address macaddr`

Mode Privileged EXEC

Parameter	Description
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

no network ipv6 neighbor

Use this command to remove IPv6 neighbors from the neighbor table.

Format `no network ipv6 neighbor ipv6-address macaddr`

Mode Privileged EXEC

show network ipv6 neighbors

Use this command to display the information about the IPv6 neighbor entries cached on the network port. The information is updated to show the type of the entry.

Default None

Format `show network ipv6 neighbors`

Mode Privileged EXEC

Term	Description
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC Address of the neighbor.
isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; if FALSE, it is not a router.
Neighbor State	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Age	The time in seconds that has elapsed since an entry was added to the cache.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry: Static if the entry is manually configured, Dynamic if dynamically resolved.

Example: The following is an example of the command.

```
(UBNT EdgeSwitch) #show network ipv6 neighbors

                                                    Neighbor  Age
IPv6 Address             MAC Address       isRtr State    (Secs)      Type
------------------------ ----------------- ----- --------- ------      ------
FE80::5E26:AFF:FEBD:852C 5c:26:0a:bd:85:2c FALSE Reachable 0           Static
```

ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and browser-based UI interfaces. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation.

The terminal interface sends three pings to the target station. Use the *ipv6-global-address|hostname* parameter to ping an interface by using the global IPv6 address of the interface. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format. Use the optional `size` keyword to specify the size of the ping packet.

You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address *ipv6-global-address|hostname*. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or traceroute request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the service or network port interface by using the `network` parameter.

Default
count: 1
interval: 3 seconds
size: 0 bytes

Format
`ping ipv6 {`*ipv6-global-address|hostname* `| {interface {`*slot/port* `| vlan` *1-4093* `| network} link-local-address} [size` *datagram-size*`]}`

Mode
- Privileged EXEC
- User Exec

ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation.

The terminal interface sends three pings to the target station. You can use a network port, service port, VLAN, or physical interface as the source. The parameter *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Format
`ping ipv6 interface {`*slot/port* `| vlan` *1-4093* `| network} {link-local-address` *link-local-address* `|` *ipv6-address*`} [size` *datagram-size*`]`

Modes
- Privileged EXEC
- User Exec

Parameter	Description
`interface`	Use the interface keyword to ping an interface by using the link-local address or the global IPv6 address of the interface.
`size`	Use the optional size keyword to specify the size of the ping packet.
ipv6-address	The link local IPv6 address of the device you want to query.

Chapter 7: Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands available in the EdgeSwitch CLI.

The chapter contains the following sections:

- **"Class of Service Commands" on page 362**
- **"Differentiated Services Commands" on page 368**
- **"DiffServ Class Commands" on page 369**
- **"DiffServ Policy Commands" on page 375**
- **"DiffServ Service Commands" on page 380**
- **"DiffServ Show Commands" on page 381**
- **"MAC Access Control List Commands" on page 386**
- **"IP Access Control List Commands" on page 390**
- **"IPv6 Access Control List Commands" on page 399**
- **"Time Range Commands for Time-Based ACLs" on page 404**
- **"Auto-Voice over IP Commands" on page 406**



Note: The commands in this chapter consist of two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.



Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *userpriority* values can range from 0-7. The *trafficclass* values range from 0 to 6, although the actual number of available traffic classes depends on the platform.

Format	`classofservice dot1p-mapping` *userpriority trafficclass*
Modes	Global Config, Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format	`no classofservice dot1p-mapping`
Modes	Global Config, Interface Config

classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The *ipdscp* value is specified as either an iinteger from 0 to 63, or symbolically using one of the following keywords: `af11`, `af12`, `af13`, `af21`, `af22`, `af23`, `af31`, `af32`, `af33`, `af41`, `af42`, `af43`, `be`, `cs0`, `cs1`, `cs2`, `cs3`, `cs4`, `cs5`, `cs6`, `cs7`, `ef`.

The *trafficclass* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format	`classofservice ip-dscp-mapping` *ipdscp trafficclass*
Mode	Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format	`no classofservice ip-dscp-mapping`
Mode	Global Config

classofservice ip-precedence-mapping

This command maps an IP Precedence value to an internal traffic class for a specific interface. The optional *0-7* parameter (IP precedence value) is only valid on platforms that support independent per-port class of service mappings.

Format	`classofservice ip-precedence-mapping [`*0-7*`]`
Mode	Global Config

no classofservice ip-precedence-mapping

This command returns the mapping to its default value.

Format	`no classofservice ip-dscp-mapping`
Mode	Global Config

classofservice trust

This command sets the class of service trust mode of an interface or range of interfaces. You can set the mode to trust the Dot1p (802.1p) or IP DSCP packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the `show running-config` command because Dot1p is the default.

Default	dot1p
Format	`classofservice trust {dot1p | ip-dscp | untrusted}`
Modes	Global Config, Interface Config

no classofservice trust

This command sets the interface mode to the default value (Dot1p).

Format	`no classofservice trust`
Modes	Global Config, Interface Config

cos-queue max-bandwidth

This command specifies the maximum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no maximum bandwidth. The sum of all values entered must not exceed 100.

Format	`cos-queue max-bandwidth` *`bw-0 bw-1...bw-n`*
Modes	Global Config, Interface Config

no cos-queue max-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format	`no cos-queue min-bandwidth`
Modes	• Global Config, Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. The total number of queues, *`n`*, supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format	`cos-queue min-bandwidth` *`bw-0 bw-1...bw-n`*
Modes	Global Config, Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format	`no cos-queue min-bandwidth`
Modes	Global Config, Interface Config

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format	`cos-queue random-detect` *`queue-id-1 [queue-id-2...queue-id-n]`*
Modes	Global Config, Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than *n*, queue ID values are specified with this command. Duplicate queue ID values are ignored. Each queue ID value ranges from 0 to (*n*–1), where n is the total number of queues supported per interface. The number *n* is platform dependent and corresponds to the number of supported queues (traffic classes).

no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format	`no cos-queue random-detect` *`queue-id-1 [queue-id-2...queue-id-n]`*
Modes	Global Config, Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

Format	`cos-queue strict` *`queue-id-1 [queue-id-2...queue-id-n]`*
Modes	Global Config, Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format	`no cos-queue strict` *`queue-id-1 [queue-id-2...queue-id-n]`*
Modes	Global Config, Interface Config

random-detect

This command is used to enable WRED for the interface as a whole, and is only available when per-queue WRED activation control is not supported by the device Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format	`random-detect`
Modes	Global Config, Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Format	`no random-detect`
Modes	Global Config, Interface Config

random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Format	`random-detect exponential-weighting-constant` *`0-15`*
Modes	Interface Config

random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the `cos-queue random-detect` command).

Format `random-detect queue-parms queue-id-1 [queue-id-2...queue-id-n] min-thresh thresh-prec-1...thresh-prec-n max-thresh thresh-prec-1...thresh-prec-n drop-probability prob-prec-1...prob-prec-n`

Modes Global Config, Interface Config

Each parameter is specified for each possible drop precedence (color of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

Parameter	Definition
`min-thresh`	Minimum threshold - Queue depth (as a percentage) where WRED starts marking and dropping traffic.
`max-thresh`	Maximum threshold - Queue depth (as a percentage) above which WRED marks/drops all traffic.
`drop-probability`	The percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format `no random-detect queue-parms queue-id-1 [queue-id-2...queue-id-n]`

Modes Global Config, Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. The bandwidth values are from 0-100 in increments of 1. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format `traffic-shape bw`

Modes Global Config, Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format `no traffic-shape`

Modes Global Config, Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The optional parameter `slot/port` is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see **"Voice VLAN Commands" on page 226**.

Format `show classofservice dot1p-mapping [slot/port]`

Modes Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format `show classofservice ip-dscp-mapping`

Mode Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show classofservice ip-precedence-mapping [slot/port]`

Mode Privileged EXEC

Term	Definition
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

show classofservice trust

This command displays the current trust mode setting for a specific interface. The optional *slot/port* parameter is only valid on platforms that support independent per-port class of service mappings. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

Format `show classofservice trust [slot/port]`

Mode Privileged EXEC

Term	Definition
Class of Service Trust Mode	The the trust mode, which is either Dot1P, IP DSCP, or Untrusted.
Non-IP Traffic Class	(IP DSCP mode only) The traffic class used for non-IP traffic.
Untrusted Traffic Class	(Untrusted mode only) The traffic class used for all untrusted traffic.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The optional parameter *slot/port* is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show interfaces cos-queue [slot/port]`

Mode Privileged EXEC

Term	Definition
Interface Shaping Rate	The global interface shaping rate value.
WRED Decay Exponent	The global WRED decay exponent value.
Queue Id	An interface supports n queues numbered 0 to (*n*-1). The specific *n* value is platform-dependent.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Maximum Bandwidth	The maximum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Term	Definition
Interface	The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.
WRED Decay Exponent	The configured WRED decay exponent for a CoS queue interface.

show interfaces random-detect

This command displays the global WRED settings for each CoS queue. If you specify the *slot/port*, the command displays the WRED settings for each CoS queue on the specified interface.

Format `show interfaces random-detect [slot/port]`

Mode Privileged EXEC

Term	Definition
Queue ID	An interface supports n queues numbered 0 to (*n*-1). The specific *n* value is platform dependent.
WRED Minimum Threshold	The configured minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
WRED Maximum Threshold	The configured maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

show interfaces tail-drop-threshold

This command displays the tail drop threshold information. If you specify the *slot/port*, the command displays the tail drop threshold information for the specified interface.

Format `show interfaces tail-drop-threshold [slot/port]`

Mode Privileged EXEC

Differentiated Services Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
   a. Creating and deleting classes.
   b. Defining match criteria for a class.
2. Policy
   a. Creating and deleting policies
   b. Associating classes with a policy
   c. Defining policy statements for a policy/class combination
3. Service
   a. Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.



Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the Layer-2 packet header.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`diffserv`
Mode	Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`no diffserv`
Mode	Global Config

DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria).

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.



Note: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is class-map.

class-map

This command defines a DiffServ class of type `match-all`. When used without any match condition, this command enters the class-map mode. The *`class-map-name`* is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.



Note: The class-map-name `default` is reserved and must not be used.

The class type of `match-all` indicates all of the individual match conditions must be true for a packet to be considered a member of the class.This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.



Note: The CLI mode is changed to Class-Map Config when this command is successfully executed depending on the keyword specified.

Format	`class-map match-all` *`class-map-name`* `[ipv4 | ipv6]`
Mode	Global Config

no class-map

This command eliminates an existing DiffServ class. The *`class-map-name`* is the name of an existing DiffServ class. (The class name `default` is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format	`no class-map` *`class-map-name`*
Mode	Global Config

class-map rename

This command changes the name of a DiffServ class. The *`class-map-name`* is the name of an existing DiffServ class. The *`new-class-map-name`* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default	none
Format	`class-map rename` *`class-map-name new-class-map-name`*
Mode	Global Config

match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The `ethertype` value is specified as one of the following keywords: `appletalk`, `arp`, `ibmsna`, `ipv4`, `ipv6`, `ipx`, `mplsmcast`, `mplsucast`, `netbios`, `novell`, `pppoe`, `rarp`; or as a custom EtherType value in the range of 0x0600-0xFFFF. Use the `not` option to negate the match condition.

Format	`match [not] ethertype {keyword | custom 0x0600-0xFFFF}`
Mode	Class-Map Config

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] any`
Mode	Class-Map Config

match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The *`refclassname`* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default	none
Format	`match class-map refclassname`
Mode	Class-Map Config



Note:

- The parameters *`refclassname`* and *`class-map-name`* cannot be the same.
- Only one other class may be referenced by a class.
- Any attempt to delete the *`refclassname`* class while the class is still referenced by any *`class-map-name`* fails.
- The combined match criteria of *`class-map-name`* and *`refclassname`* must be an allowed combination based on the class type.
- Any subsequent changes to the *`refclassname`* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The *`refclassname`* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format	`no match class-map refclassname`
Mode	Class-Map Config

match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] cos 0-7`
Mode	Class-Map Config

match secondary-cos

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] secondary-cos 0-7`
Mode	Class-Map Config, Ipv6-Class-Map Config

match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The *macaddr* parameter is any Layer-2 MAC address formatted as six 2-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a Layer-2 MAC address bit mask, which need not be contiguous, and is formatted as six 2-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the `not` option to negate the match condition.

Default	none
Format	`match [not] destination-address mac macaddr macmask`
Mode	Class-Map Config

match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] dstip ipaddr ipmask`
Mode	Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination Layer-4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *portkey* is one of the supported port name keywords. The currently supported *portkey* values are: `domain`, `echo`, `ftp`, `ftpdata`, `http`, `smtp`, `snmp`, `telnet`, `tftp`, `www`. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one Layer-4 port number is required. The port number is an integer from 0 to 65535. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] dstl4port {portkey | 0-65535}`
Mode	Class-Map Config

match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Use the not option to negate the match condition.



Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	match [not] ip dscp *dscpval*
Mode	Class-Map Config

match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7. Use the not option to negate the match condition.



Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	match [not] ip precedence *0-7*
Mode	Class-Map Config

match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of *tosbits* is a 2-digit hexadecimal number from 00-ff. The value of *tosmask* is a two-digit hexadecimal number from 00-ff. The *tosmask* denotes the bit positions in *tosbits* that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a tosbits value of a0 (hex) and a *tosmask* of a2 (hex). Use the not option to negate the match condition.



Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.



Note: This "free form" version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Default	none
Format	match [not] ip tos *tosbits tosmask*
Mode	Class-Map Config

match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for *protocol-name* is one of the supported protocol name keywords. The currently supported values are: icmp, igmp, ip, tcp, udp. A value of ip matches all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Use the not option to negate the match condition.



Note: This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Format	match [not] protocol {*protocol-name* | *0-255*}
Mode	Class-Map Config, Ipv6-Class-Map Config

match signature

This command maps the available signatures from the rules file to the AppIQ class. When the appiq class is created, this menu displays an index number and its signature pattern. A single signature can be mapped using a number or multiple signatures can be selected and mapped to a class. Using this command without an index value maps all the available signatures to the same class.

Default	none
Format	match signature [*StartIndex-EndIndex*]
Mode	Class-Map Config

match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The address parameter is any Layer-2 MAC address formatted as six 2-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a Layer-2 MAC address bit mask, which may not be contiguous, and is formatted as six 2-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the not option to negate the match condition.

Default	none
Format	match [not] source-address mac *address macmask*
Mode	Class-Map Config

match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The ipaddr parameter specifies an IP address. The ipmask parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the not option to negate the match condition.

Default	none
Format	match [not] srcip *ipaddr ipmask*
Mode	Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source Layer-4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for *portkey* is one of the supported port name keywords: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one Layer-4 port number is required. The port number is an integer from 0 to 65535. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] srcl4port {portkey | 0-65535}`
Mode	Class-Map Config

match src port

This command adds a match condition for a range of Layer-4 source ports. If an interface receives traffic that is within the configured range of Layer-4 source ports, then only the appiq class is in effect. The `portvalue` parameter specifies a single source port.

Default	none
Format	`match src port {portstart-portend | portvalue}`
Mode	Class-Map Config

match vlan

This command adds to the specified class definition a match condition based on the value of the Layer-2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 0-4093. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] vlan 0-4093`
Mode	Class-Map Config

match secondary-vlan

This command adds to the specified class definition a match condition based on the value of the Layer-2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN-tagged packet). The secondary VLAN ID is an integer from 0-4093. Use the `not` option to negate the match condition.

Default	none
Format	`match [not] secondary-vlan 0-4093`
Mode	Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes.

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.



Note: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is policy-map.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The *queueid* is an integer from 0 to *n*-1, where *n* is the number of egress queues supported by the device.

Format	`assign-queue queueid`
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	`drop`
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format	`mirror slot/port`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Format	`redirect slot/port`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the `police` command where the fields for the conform level are specified. The parameter *`class-map-name`* is the name of an existing DiffServ class map.

Note: This command may only be used after specifying a `police` command for the policy-class instance.

Format	`conform-color` *`class-map-name`*
Mode	Policy-Class-Map Config

class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The *`classname`* is the name of an existing DiffServ class.

Note:
- This command causes the specified policy to create a reference to the class definition.
- The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	`class` *`classname`*
Mode	Policy-Map Config

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. The parameter *`classname`* is the names of an existing DiffServ class.

Note: This command removes the reference to the class definition for the specified policy.

Format	`no class` *`classname`*
Mode	Policy-Map Config

mark cos

This command marks all packets for the associated traffic stream with the specified class of service (CoS) value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Default	1
Format	`mark-cos` *`0-7`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark secondary-cos

This command marks the outer VLAN tags in the packets for the associated traffic stream as secondary CoS.

Default	1
Format	`mark secondary-cos` *`0-7`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format	`mark cos-as-sec-cos`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config-policy-classmap)#mark cos-as-sec-cos
```

mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value. The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: `af11`, `af12`, `af13`, `af21`, `af22`, `af23`, `af31`, `af32`, `af33`, `af41`, `af42`, `af43`, `be`, `cs0`, `cs1`, `cs2`, `cs3`, `cs4`, `cs5`, `cs6`, `cs7`, `ef`.

Format	`mark ip-dscp` *dscpval*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Format	`mark ip-precedence` *0-7*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the `police` command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are `drop`, `set-cos-as-sec-cos`, `set-cos-transmit`, `set-sec-cos-transmit`, `set-dscp-transmit`, `set-prec-transmit`, or `transmit`. In this simple form of the `police` command, the conform action defaults to `transmit` and the violate action defaults to `drop`. These actions can be set with this command once the style has been configured.

For `set-dscp-transmit`, a dscpval value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: `af11`, `af12`, `af13`, `af21`, `af22`, `af23`, `af31`, `af32`, `af33`, `af41`, `af42`, `af43`, `be`, `cs0`, `cs1`, `cs2`, `cs3`, `cs4`, `cs5`, `cs6`, `cs7`, `ef`.

For `set-prec-transmit`, an IP Precedence value is required and is specified as an integer from 0-7.

For `set-cos-transmit` an 802.1p priority value is required and is specified as an integer from 0-7.

Format	`police-simple {`*1-4294967295 1-128* `conform-action {drop | set-cos-as-sec-cos | set-cos-transmit` *0-7* `| set-sec-cos-transmit` *0-7* `| set-prec-transmit` *0-7* `| set-dscp-transmit` *0-63* `| transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit` *0-7* `| set-sec-cos-transmit` *0-7* `| set-prec-transmit` *0-7* `| set-dscp-transmit` *0-63* `| transmit}]}`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config-policy-classmap)#police-simple 1 128 conform-action transmit
violate-action drop
```

police-single-rate

This command is the single-rate form of the `police` command and is used to establish the traffic policing style for the specified class.

For each outcome, the only possible actions are `drop`, `set-cos-as-sec-cos`, `set-cos-transmit`, `set-sec-cos-transmit`, `set-dscp-transmit`, `set-prec-transmit`, or `transmit`. In this single-rate form of the `police` command, the conform action defaults to `transmit`, the exceed action defaults to `drop`, and the violate action defaults to `drop`. These actions can be set with this command once the style has been configured.

Format

```
police-single-rate {1-4294967295 1-128 1-128 conform-action {drop |
set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 |
set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action
{drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 |
set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} [violate-action
{drop | set-cos-as-sec-cos-transmit | set-cos-transmit 0-7 |
set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 |
transmit}]}
```

Mode Policy-Class-Map Config

police-two-rate

This command is the two-rate form of the police command and is used to establish the traffic policing style for the specified class.

For each outcome, the only possible actions are `drop`, `set-cos-as-sec-cos`, `set-cos-transmit`, `set-sec-cos-transmit`, `set-dscp-transmit`, `set-prec-transmit`, or `transmit`. In this two-rate form of the `police` command, the conform action defaults to `transmit`, the exceed action defaults to `drop`, and the violate action defaults to `drop`. These actions can be set with this command once the style has been configured.

Format

```
police-two-rate {1-4294967295 1-4294967295 1-128 1-128 conform-action {drop |
set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 |
set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action
{drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 |
set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} [violate-action {drop
| set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-
prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}]}
```

Mode Policy-Class-Map Config

policy-map

This command establishes a new DiffServ policy. The *policyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the `in` parameter, or the outbound traffic direction as indicated by the `out` parameter, respectively.



Note: The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format

```
policy-map policyname {in|out}
```

Mode Global Config

no policy-map

This command eliminates an existing DiffServ policy. The *policyname* parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format	`no policy-map` *policyname*
Mode	Global Config

policy-map rename

This command changes the name of a DiffServ policy. The *policyname* is the name of an existing DiffServ class. The *newpolicyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format	`policy-map rename` *policyname newpolicyname*
Mode	Global Config

DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is service-policy.

service-policy

This command attaches a policy to an interface in the inbound direction as indicated by the in parameter, or the outbound direction as indicated by the out parameter, respectively. The policyname parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.



Note: This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative "mode" command for DiffServ.



Note: This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format	`service-policy {in|out} policymapname`
Modes	Global Config, Interface Config



Note: Each interface can have one policy attached.

no service-policy

This command detaches a policy from an interface in the inbound direction as indicated by the in parameter, or the outbound direction as indicated by the out parameter, respectively. The *policyname* parameter is the name of an existing DiffServ policy.



Note: This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction or an interface in the outbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format	`no service-policy {in|out} policymapname`
Modes	Global Config, Interface Config

DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

show class-map

This command displays all configuration information for the specified class.

Format `show class-map [class-name]`

Modes Privileged EXEC, User EXEC

If *class-name* (the name of an existing DiffServ class) is specified, then the following fields are displayed:

Term	Definition
Class Name	The name of this class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Class Layer3 Protocol	The Layer-3 protocol for this class. Possible value is IPv4.
Match Criteria	Match Criteria fields are only displayed if they are configured. Not all platforms support all match criteria. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If *class-name* is not specified, a list of all defined DiffServ classes is displayed with the following fields:

Term	Definition
Class Name	The name of this class. (Classes are not necessarily displayed in the order in which they were created.)
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format `show diffserv`

Mode Privileged EXEC

Term	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size Current/Max	The current and maximum number of entries (rows) in the Class Table.
Class Rule Table Size Current/Max	The current and maximum number of entries (rows) in the Class Rule Table.
Policy Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Table.
Policy Instance Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Instance Table.
Policy Attribute Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Attribute Table.
Service Table Size Current/Max	The current and maximum number of entries (rows) in the Service Table.

show policy-map

This command displays all configuration information for the specified policy.

Format `show policy-map [policyname]`

Mode Privileged EXEC

If *policyname* (the name of an existing DiffServ policy) is specified, then the following fields are displayed:

Term	Definition
Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)
Class Members	The class that is a member of the policy.

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Term	Definition
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Class Name	The name of this class.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform Color Mode	The current setting for the color mode. Policing uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.
Conform COS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Exceed Color Mode	The current setting for the color of exceeding traffic that the user may optionally specify.
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark CoS as Secondary CoS	The secondary 802.1p priority value (second/inner VLAN tag. Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Non-Conform COS	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.

Term	Definition
Peak Rate	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is transmitted or dropped (per type of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AP traffic class (although average rate shaping could also be used.)
Peak Burst Size	(PBS). The network administrator can set the PBS as a means to limit the damage expedited forwarding traffic could inflict on other traffic (e.g., a token bucket rate limiter) Traffic exceeding this limit is discarded.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

If *policyname* is not specified, the command displays a list of all defined DiffServ policies. The following fields are displayed:

Term	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

Example: The following shows example CLI display output including the `mark-cos-as-sec-cos` option specified in the policy action.

```
(UBNT EdgeSwitch) #show policy-map p1
Policy Name..................................... p1
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS....................... Yes
```

Example: The following shows example CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(UBNT EdgeSwitch) #show policy-map p2
Policy Name..................... p2
Policy Type..................... In
Class Name...................... c2
Policing Style.................. Police Two Rate
Committed Rate.................. 1
Committed Burst Size............ 1
Peak Rate....................... 1
Peak Burst Size................. 1
Conform Action.................. Mark CoS as Secondary CoS
Exceed Action................... Mark CoS as Secondary CoS
Non-Conform Action.............. Mark CoS as Secondary CoS
Conform Color Mode.............. Blind
Exceed Color Mode............... Blind
```

show diffserv service

This command displays policy service information for the specified interface and direction. The *slot/port* parameter specifies a valid slot/port number for the system.

Format `show diffserv service slot/port in`

Mode Privileged EXEC

Term	Definition
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	The slot/port.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.
Policy Details	Attached policy details, whose content is identical to that described for the `show policy-map policymapname` command (content not repeated here for brevity).

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format `show diffserv service brief [in]`

Mode Privileged EXEC

Term	Definition
DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Term	Definition
Interface	The slot/port.
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The *slot/port* parameter specifies a valid interface for the system. Instead of *slot/port*, you can also use `lag` *lag-intf-num* to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Note: This command is only allowed while the DiffServ administrative mode is enabled.

Format `show policy-map interface` *slot/port* `[in]`

Mode Privileged EXEC

Term	Definition
Interface	The slot/port.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Term	Definition
Class Name	The name of this class instance.
In Discarded Packets	The number of packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format	`show service-policy in`
Mode	Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Term	Definition
Interface	The slot/port.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC Access Control List Commands

This section describes the commands you use to configure MAC Access Control List (ACL) settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.

mac access-list extended

This command creates a MAC Access Control List (ACL) identified by *name*, consisting of classification fields defined for the Layer-2 header of an Ethernet frame. The *name* parameter is a case-sensitive alphanumeric string of 1-31 characters uniquely identifying the MAC access list. The rate-limit attribute configures the committed rate and the committed burst size.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.



Note: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format	`mac access-list extended name`
Mode	Global Config

no mac access-list extended

This command deletes a MAC ACL identified by name from the system.

Format	`no mac access-list extended name`
Mode	Global Config

mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The name parameter is the name of an existing MAC ACL. The *newname* parameter is a case-sensitive alphanumeric string of 1-31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *newname* already exists.

Format	`mac access-list extended rename name newname`
Mode	Global Config

{deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	`{deny|permit} {srcmac | any} {dstmac | any} [ethertypekey | 0x0600-0xFFFF] [vlan {eq 0-4095}] [cos 0-7] [[log] [time-range time-range-name] [assign-queue queue-id]] [{mirror | redirect} slot/port] [rate-limit rate burst-size]`
Mode	Mac-Access-List Config

Note:

- The `no` form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and respecified.
- An implicit deny all MAC rule always terminates the access list.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *`ethertypekey`* values are: `appletalk`, `arp`, `ibmsna`, `ipv4`, `ipv6`, `ipx`, `mplsmcast`, `mplsucast`, `netbios`, `novell`, `pppoe`, `rarp`. Each of these translates into its equivalent Ethertype value(s).

Table 13. Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The `vlan` and `cos` parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The `time-range` parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter *`time-range-name`*. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see **"Time Range Commands for Time-Based ACLs" on page 404**.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`queue-id`* value is 0 to (*n*-1), where *n* is the number of user configurable queues available for the hardware platform. The `assign-queue` parameter is valid only for a permit rule.

The `mirror` parameter allows the traffic matching this rule to be copied to the specified *`slot/port`*, while the `redirect` parameter allows the traffic matching this rule to be forwarded to the specified *`slot/port`*. The `assign-queue` and `redirect` parameters are only valid for a permit rule.

Note: The special command form `{deny | permit} any any` is used to match all Ethernet Layer-2 packets, and is the equivalent of the IP access list "match every" rule.

The `permit` command's optional attribute `rate-limit` allows you to permit only the allowed rate of traffic as per the configured *`rate`* in kbps, and *`burst-size`* in kbytes.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)#mac access-list extended mac1
(UBNT EdgeSwitch) (Config-mac-access-list)#permit 00:00:00:00:aa:bb ff:ff:ff:ff:00:00
any rate-limit 32 16
(UBNT EdgeSwitch) (Config-mac-access-list)#exit
```

mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *name* to an interface or range of interfaces, or associates it with a VLAN ID, in a given direction. The *name* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Note: You should be aware that the `out` option may or may not be available, depending on the platform.

Format `mac access-group name {{in|out} vlan vlan-id {in|out}} [sequence 1–4294967295]`

Modes Global Config, Interface Config

Parameter	Description
name	The name of the Access Control List.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.
sequence	A optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch)(Config)#mac access-group mac1
```

no mac access-group

This command removes a MAC ACL identified by name from the interface in a given direction.

Format `no mac access-group name {{in|out} vlan vlan-id {in|out}}`

Modes Global Config, Interface Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch)(Config)#no mac access-group mac1
```

show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the [name] parameter to identify a specific MAC ACL to display. The rate-limit attribute displays committed rate and committed burst size.

Note: The command output varies based on the match criteria configured within the rules of an ACL.

Format `show mac access-lists [name]`

Mode Privileged EXEC

Term	Definition
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Source MAC Mask	The source MAC mask for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show mac access-lists mac1

ACL Name: mac1

Rule Number: 1
Action..................................... permit
Source MAC Address......................... 00:00:00:00:AA:BB
Source MAC Mask............................ FF:FF:FF:FF:00:00
Committed Rate............................. 32
Committed Burst Size....................... 16
```

IP Access Control List Commands

This section describes the commands you use to configure IP Access Control List (ACL) settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- EdgeSwitch software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. Table 14 describes the parameters for the `access-list` command.

IP Standard ACL:

Format `access-list 1-99 {deny | permit} {every | srcip srcmask} [log] [time-range time-range-name] [assign-queue queue-id] [{mirror | redirect} slot/port]`

Mode Global Config

IP Extended ACL:

Format `access-list 100-199 {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0-255} {srcip srcmask|any|host srcip} [range {portkey|startport} {portkey|endport} {eq|neq|lt|gt} {portkey|0-65535}] {dstip dstmask|any|host dstip} [range {portkey|startport} {portkey|endport} {eq|neq|lt|gt} {portkey|0-65535}] [flag [+fin|-fin] [+syn|-syn] [+rst|-rst] [+psh|-psh] [+ack|-ack] [+urg|-urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} slot/port] [rate-limit rate burst-size]`

Mode Global Config

Note: IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The `rate-limit` command is not supported.

Table 14. ACL Command Parameters

Parameter	Description
`1-99` or `100-199`	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
`{deny | permit}`	Specifies whether the IP ACL rule permits or denies an action.
`every`	Match every packet.
`{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0-255}`	Specifies the protocol to filter for an extended IP ACL rule.
`srcip srcmask | any | host scrip`	Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying `any` specifies the source IP as 0.0.0.0 and the source IP mask as 255.255.255.255. Specifying `host A.B.C.D` specifies the source IP as A.B.C.D and source IP mask as 0.0.0.0.

Table 14. ACL Command Parameters (Continued)

{{range {*portkey*|*startport*} {*portkey*|*endport*} | {eq|neq|lt|gt} {*portkey*|*0-65535*}}]	Note: This option is available only if the protocol is TCP or UDP. Specifies the source Layer-4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the portkey, which can be one of the following keywords: • For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3. • For UDP: domain, echo, ntp, rip, snmp, tftp, time, and who. For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If range is specified, the IP ACL rule matches only if the Layer-4 port number falls within the specified port range. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the Layer-4 port range. When eq is specified, the IP ACL rule matches only if the Layer-4 port number is equal to the specified port number or *portkey*. When lt is specified, the IP ACL rule matches if the Layer-4 port number is less than the specified port number or *portkey*. It is equivalent to specifying a range of 0-<*specified port number*-1>. When gt is specified, the IP ACL rule matches if the Layer-4 port number is greater than the specified port number or *portkey*. It is equivalent to specifying a range of <*specified port number*+1>-65535. When neq is specified, the IP ACL rule matches only if the Layer-4 port number is not equal to the specified port number or *portkey*. Two rules are added in the hardware one with range equal to 0-<*specified port number*-1> and one with range equal to <*specified port number*+1>-65535. Note: Port number matches only apply to unfragmented or first fragments.
dstip dstmask | any | host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies a destination IP of 0.0.0.0 and destination mask of 255.255.255.255. Specifying host *A.B.C.D* implies a destination IP of A.B.C.D and destination mask of 0.0.0.0.
precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp*, *precedence*, *tos*/*tosmask*. Note: *tosmask* is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Note: This option is available only if the protocol is tcp. Specifies that the IP ACL rule matches on the TCP flags. When +fin, +syn, +rst, +psh, +ack, or +urg is specified, a match occurs if the specified flag is set in the TCP header. When -fin, -syn, -rst, -psh, -ack, or -urg is specified, a match occurs if the specified flag is *not* set in the TCP header. When established is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the established option is specified.
icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*	Note: This option is available only if the protocol is icmp. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies that both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable.
igmp-type *igmp-type*	This option is available only if the protocol is IGMP. When *igmp-type* is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
fragments	Specifies that the IP ACL rule matches on fragmented IP packets.
log	Specifies that this rule is to be logged.

Table 14. ACL Command Parameters (Continued)

`time-range time-range-name`	Allows imposing time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see **"Time Range Commands for Time-Based ACLs" on page 404**.
`assign-queue queue-id`	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
`{mirror | redirect} slot/port`	Specifies the mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively.
`rate-limit rate burst-size`	Specifies the allowed rate of traffic as per the configured *rate* in kbps, and *burst-size* in kbytes.

no access-list

This command deletes an IP ACL that is identified by the parameter accesslistnumber from the system. The range for *accesslistnumber* is 1-99 for standard access lists and 100-199 for extended access lists.

Format `no access-list accesslistnumber`

Mode Global Config

ip access-list

This command creates an extended IP Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv4 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Note: The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format `ip access-list name`

Mode Global Config

no ip access-list

This command deletes the IP ACL identified by *name* from the system.

Format `no ip access-list name`

Mode Global Config

ip access-list rename

This command changes the name of an IP Access Control List (ACL). The *name* parameter specifies the names of an existing IP ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails if an IP ACL by the name *newname* already exists.

Format `ip access-list rename name newname`

Mode Global Config

{deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified using the keyword `any` to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format `{deny|permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0-255} {srcip srcmask | any | host srcip} [range {portkey|startport} {portkey|endport} | {eq|neq|lt|gt} {portkey|0-65535}] {dstip dstmask | any | host dstip} [range {portkey|startport} {portkey|endport} | {eq|neq|lt|gt} {portkey|0-65535}] [flag [+fin|-fin] [+syn|-syn] [+rst|-rst] [+psh|-psh] [+ack|-ack] [+urg|-urg] [established]] [{+|-}fin] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} slot/port] [rate-limit rate burst-size]`

Mode Ipv4-Access-List Config

Note: The `no` form of this command is not supported, since the rules within an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and respecified.

Note: An implicit deny all IP rule always terminates the access list.

Note: For IPv4, the following are not supported for egress ACLs:

- A match on port ranges.
- The `rate-limit` command.

The `time-range` parameter allows imposing atime limitation on the IP ACL rule as defined by the specified time range (*`time-range-name`*). If the specified time range does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If the specified time range exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the specified time range becomes active. The ACL rule is removed when the specified time range becomes inactive. For information about configuring time ranges, see **"Time Range Commands for Time-Based ACLs" on page 404**.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`queue-id`* value is from 0 to (*n*-1), where *n* is the number of user configurable queues available for the hardware platform. The `assign-queue` parameter is valid only for a permit rule.

The `permit` command's optional attribute `rate-limit` allows you to permit only the allowed *`rate`* of traffic as per the configured rate in kbps, and *`burst-size`* in kbytes.

Parameter	Description
`{deny | permit}`	Specifies whether the IP ACL rule permits or denies the matching traffic.
`every`	Match every packet.
`eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0-255`	Specifies the protocol to match for the IP ACL rule.
`srcip srcmask` | `any` | `host` *`srcip`*	Specifies a source IP address and source netmask to match for the IP ACL rule. Specifying `any` implies a source IP of 0.0.0.0 and the source IP mask of 255.255.255.255. Specifying `host` *`A.B.C.D`* implies a source IP of A.B.C.D and the source IP mask of 0.0.0.0.

Parameter	Description
[{range {*portkey*|*startport*} {*portkey*|*endport*} | {eq|neq|lt|gt} {*portkey*|*0-65535*}]	Note: This option is available only if the protocol is tcp or udp. Specifies the Layer-4 port match condition for the IP ACL rule. Port number can be used, which ranges from 0-65535, or the *portkey*, which can be one of the following keywords: • For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 • For UDP: domain, echo, ntp, rip, snmp, tftp, time, who Each of these keywords translates into its equivalent port number. If range is specified, the IP ACL rule matches only if the Layer-4 port number falls within the specified port range. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the Layer-4 port range. When eq is specified, the IP ACL rule matches only if the Layer-4 port number is equal to the specified port number or *portkey*. When lt is specified, the IP ACL rule matches if the Layer-4 port number is less than the specified port number or *portkey*. It is equivalent to specifying a range of 0-<*specified port number*-1>. When gt is specified, the IP ACL rule matches if the Layer-4 port number is greater than the specified port number or *portkey*. It is equivalent to specifying a range of <*specified port number*+1>-65535. When neq is specified, IP ACL rule matches only if the Layer-4 port number is not equal to the specified port number or *portkey*. Two rules are added in the hardware one with range equal to 0-<*specified port number*-1> and one with range equal to <*specified port number*+1>-65535. Note: Port number matches only apply to unfragmented or first fragments.
dstip dstmask | any | host *dstip*	Specifies a destination IP address and netmask to match for the IP ACL rule. Specifying any implies a destination IP of 0.0.0.0 and destination mask of 255.255.255.255. Specifying host *A.B.C.D* implies a destination IP of A.B.C.D and destination mask of 0.0.0.0.
precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp*, *precedence*, tos/*tosmask*. Note: *tosmask* is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Note: This option is available only if the protocol is tcp. Specifies that the IP ACL rule matches on the TCP flags. When +fin, +syn, +rst, +psh, +ack, or +urg is specified, a match occurs if the specified flag is set in the TCP header. When -fin, -syn, -rst, -psh, -ack, or -urg is specified, a match occurs if the specified flag is *not* set in the TCP header. When established is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the established option is specified.
icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*	Note: This option is available only if the protocol is icmp. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies that both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable. The ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type.
igmp-type *igmp-type*	Note: This option is visible only if the protocol is igmp. When *igmp-type* is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
fragments	Specifies that the IP ACL rule matches on fragmented IP packets.
log	Specifies that this rule is to be logged.
time-range *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.

Parameter	Description
`assign-queue queue-id`	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
`{mirror | redirect} slot/port`	Specifies the mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively.
`rate-limit rate burst-size`	Specifies the allowed rate of traffic as per the configured *rate* in kbps, and *burst-size* in kbytes.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)#ip access-list ip1
(UBNT EdgeSwitch) (Config-ipv4-acl)#permit icmp any any rate-limit 32 16
(UBNT EdgeSwitch) (Config-ipv4-acl)#exit
```

ip access-group

This command either attaches a specific IP Access Control List (ACL) identified by *accesslistnumber* or *name* to an interface, range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter name is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Default	none
Format	`ip access-group {accesslistnumber|name} {in|out} | vlan vlan-id {in|out}} [sequence 1-4294967295]`
Modes	Interface Config, Global Config

Parameter	Description
accesslistnumber	Identifies a specific IP ACL. The range is 1 to 199.
name	The name of the Access Control List.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.
`sequence`	A optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)#ip access-group ip1
```

no ip access-group

This command removes a specified IP ACL from an interface.

Default	none
Format	`no ip access-group {accesslistnumber|name} {{in|out} | vlan vlan-id {in|out}}`
Mode	Interface Config, Global Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch)(Config)#no ip access-group ip1
```

acl-trapflags

This command enables the ACL trap mode.

Default	disabled
Format	`acl-trapflags`
Mode	Global Config

no acl-trapflags

This command disables the ACL trap mode.

Format	`no acl-trapflags`
Mode	Global Config

show ip access-lists

Use this command to view summary information about all IP ACLs configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL. The rate-limit attribute displays committed rate and committed burst size.

Format	`show ip access-lists [accesslistnumber | name]`
Mode	Privileged EXEC

Term	Definition
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into (ingress) or leaving (egress) the interface.
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).

If you specify an IP ACL number or name, the following information is displayed:

Note: Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Term	Definition
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
ICMP Type	Note: This is shown only if the protocol is ICMP. The ICMP message type for this rule.
Starting Source L4 port	The starting source Layer-4 port.
Ending Source L4 port	The ending source Layer-4 port.
Starting Destination L4 port	The starting destination Layer-4 port.
Ending Destination L4 port	The ending destination Layer-4 port.
ICMP Code	Note: This is shown only if the protocol is ICMP. The ICMP message code for this rule.
Fragments	If the ACL rule matches on fragmented IP packets.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.

Term	Definition
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IP ACL rule.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ip access-lists ip1

ACL Name: ip1
Inbound Interface(s): 0/30

Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 1(icmp)
Committed Rate............................. 32
Committed Burst Size....................... 16
```

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. Instead of *slot/port*, you can use `lag` *lag-intf-num* as an alternate way to specify the LAG interface, where *lag-intf-num* is the LAG port number.

Format `show access-lists interface {`*slot/port* `in|out}`

Mode Privileged EXEC

Parameter	Description
`in|out`	• `in` Display Access List information for a particular interface and the in direction. • `out` Display Access List information for a particular interface and the out direction.

Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) #show access-lists interface

ACL Type                ACL ID                      Sequence Number
--------          ------------------------------  ---------------
IPv6                    ip61                                  1
```

show access-lists vlan

This command displays Access List information for a particular VLAN ID. The *vlan-id* parameter is the VLAN ID of the VLAN with the information to view. The {in | out} options specify the direction of the VLAN ACL information to view.

Format show access-lists vlan *vlan-id* in|out

Mode Privileged EXEC

Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

IPv6 Access Control List Commands

This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv6 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.



Note: The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format	`ipv6 access-list name`
Mode	Global Config

no ipv6 access-list

This command deletes the IPv6 ACL identified by *name* from the system.

Format	`no ipv6 access-list name`
Mode	Global Config

ipv6 access-list rename

This command changes the name of an IPv6 ACL. The name parameter is the name of an existing IPv6 ACL. The newname parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name *newname* already exists.

Format	`ipv6 access-list rename name newname`
Mode	Global Config

{deny | permit} (IPv6)

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the `every` keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword `any` to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format

```
{deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | 0-255}
{source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[{range {portkey|startport} {portkey|endport} | {eq | neq | lt | gt}
{portkey|0-65535}] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [{range {portkey|startport} {portkey|endport} |
{eq | neq | lt | gt} {portkey|0-65535}] [flag [+fin|-fin] [+syn|-syn]
[+rst|-rst] [+psh|-psh] [+ack|-ack] [+urg|-urg] [established]]
[flow-label value] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message
icmp-message] [routing] [fragments] [dscp dscp]}} [log] [assign-queue queue-id]
[{mirror | redirect} slot/port] [rate-limit rate burst-size]
```

Mode IPv6-Access-List Config



Note:

- The `no` form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.
- An implicit deny all IPv6 rule always terminates the access list.

The `time-range` parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter *`time-range-name`*. If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see **"Time Range Commands for Time-Based ACLs" on page 404**.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`queue-id`* value is 0 to (*n*-1), where *n* is the number of user-configurable queues available for the hardware platform. The `assign-queue` parameter is valid only for a permit rule.

The `mirror` parameter allows the traffic matching this rule to be copied to the specified *`slot/port`*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified slot/port. The `assign-queue` and `redirect` parameters are only valid for a permit rule.

The `permit` command's optional attribute `rate-limit` allows you to permit only the allowed rate of traffic as per the configured *`rate`* in kbps, and *`burst-size`* in kbytes.

IPv6 ACLs have the following limitations:

- Port ranges are not supported for egress IPv6 ACLs.
- The rate-limit command is not supported for egress IPv6 ACLs.

Parameter	Description
`{deny | permit}`	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
`every`	Specifies to match every packet.
`{protocolkey | number}`	*`protocolkey`* specifies the protocol to match for the IPv6 ACL rule: `icmpv6`, `ipv6`, `tcp`, or `udp`. *`number`* is the protocol number: `0-255`.
`source-ipv6-prefix/prefix-length` `| any | host` *`source-ipv6-address`*	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0 " Specifying `host` *`source-ipv6-address`* implies matching the specified IPv6 address. The *`source-ipv6-address`* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Parameter	Description
[{range {*portkey*|*startport*} {*portkey*|*endport*} | {eq | neq | lt | gt} {*portkey*|*0-65535*}]	Note: This option is available only if the protocol is TCP or UDP. Specifies the Layer-4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0-65535, or the *portkey*, which can be one of the following keywords: • For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 • For UDP: domain, echo, ntp, rip, snmp, tftp, time, who Each of these keywords translates into its equivalent port number. When range is specified, IPv6 ACL rule matches only if the Layer-4 port number falls within the specified port range. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between are part of the Layer-4 port range. When eq is specified, IPv6 ACL rule matches only if the Layer-4 port number is equal to the specified port number or *portkey*. When lt is specified, IPv6 ACL rule matches if the Layer-4 port number is less than the specified port number or *portkey*. It is equivalent to specifying the range as 0 to <*specified port number*-1>. When gt is specified, IPv6 ACL rule matches if the Layer-4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <*specified port number*+1> to 65535. When neq is specified, IPv6 ACL rule matches only if the Layer-4 port number is not equal to the specified port number or *portkey*. Two rules are added in the hardware, one with range equal to 0 to <*specified port number*-1> and one with range equal to <*specified port number*+1> to 65535.
destination-ipv6-prefix/prefix-length | any | host *destination-ipv6-address*	Specifies a destination IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0". Specifying host *destination-ipv6-address* implies matching the specified IPv6 address. The *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
[dscp *dscp*]	Specifies the DSCP value to match for for the IPv6 rule.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IPv6 ACL rule matches on the tcp flags. When +fin, +syn, +rst, +psh, +ack, or +urg is specified, a match occurs if the specified flag is set in the TCP header. When -fin, -syn, -rst, -psh, -ack, or -urg is specified, a match occurs if the specified flag is *not* set in the TCP header. When established is specified, a match occurs if specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware when established option is specified. This option is visible only if protocol is tcp.
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	Note: This option is available only if the protocol is icmpv6. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IPv6 ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, time-exceeded, and unreachable. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.
fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (Packets that have the next header field is set to 44).
routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have routing extension headers (the next header field is set to 43).
log	Specifies that this rule is to be logged.

Parameter	Description
time-range *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with the specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
assign-queue *queue-id*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
{mirror | redirect} *slot/port*	Specifies the mirror or redirect interface which is the *slot/port* to which packets matching this rule are copied or forwarded, respectively.
rate-limit *rate burst-size*	Specifies the allowed rate of traffic as per the configured *rate* in kbps, and *burst-size* in kbytes.

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)#ipv6 access-list ip61

(UBNT EdgeSwitch) (Config-ipv6-acl)#permit udp any any rate-limit 32 16

(UBNT EdgeSwitch) (Config-ipv6-acl)#exit
```

ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by *name* to an interface or range of interfaces, or associates it with a VLAN ID in a given direction. The *name* parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this MAC access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specifiedIPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The vlan keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

Format ipv6 traffic-filter *name* {{in|out}|vlan *vlan-id* {in|out}} [sequence *1-4294967295*]

Modes Global Config, Interface Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch)(Config)#ipv6 traffic-filter ip61
```

no ipv6 traffic-filter

This command removes an IPv6 ACL identified by name from the interface(s) in a given direction.

Format no ipv6 traffic-filter *name* {{in|out} | vlan *vlan-id* {in|out}}

Modes Global Config, Interface Config

Example: The following shows an example of the command.

```
(UBNT EdgeSwitch) (Config)#no ipv6 traffic-filter ip61
```

show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the *name* parameter to identify a specific IPv6 ACL to display. The rate-limit attribute displays committed rate and committed burst size.

Format	`show ipv6 access-lists [name]`
Mode	Privileged EXEC



Note: Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Term	Definition
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show ipv6 access-lists ip61

ACL Name: ip61

Rule Number: 1
Action..................................... permit
Match Every................................ FALSE
Protocol................................... 17(udp)
Committed Rate............................. 32
Committed Burst Size....................... 16
```

Time Range Commands for Time-Based ACLs

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit *deny all* rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined within an ACL.

time-range

Use this command to create a time range identified by *name*, consisting of one absolute time entry and/or one or more periodic time entries. The *name* parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alphanumeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries.



Note: When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

Format	`time-range name`
Mode	Global Config

no time-range

This command deletes a time-range identified by *name*.

Format	`no time-range name`
Mode	Global Config

absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The *time* parameter is based on the currently configured time zone.

The `[start time date]` parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of *hours:minutes*. For example, `8:00` is 8:00 am and `20:00` is 8:00 pm. The date is expressed in the format *day month year*. If no start time and date are specified, the configuration statement is in effect immediately.

The `[end time date]` parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format	`absolute [start time date] [end time date]`
Mode	Time-Range Config

no absolute

This command deletes the absolute time entry in the time range.

Format	`no absolute`
Mode	Time-Range Config

periodic

Use this command to add a periodic time entry to a time range. The *time* parameter is based off of the currently configured time zone.

The first occurrence of the *days-of-the-week* argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end *days-of-the-week* are the same as the start, they can be omitted.

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily: Monday through Sunday
- weekdays: Monday through Friday
- weekend: Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first *time* parameter is the starting *hours:minutes* at which the configuration that referenced the time range goes into effect. The second *time* parameter is the ending *hours:minutes* at which the configuration that referenced the time range is no longer in effect.

The *hours:minutes* are expressed in a 24-hour clock. For example, 8:00 is 8:00 am; 20:00 is 8:00 pm.

Format	periodic *days-of-the-week time* to *time*
Mode	Time-Range Config

no periodic

This command deletes a periodic time entry from a time range.

Format	no periodic *days-of-the-week time* to *time*
Mode	Time-Range Config

show time-range

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the *name* parameter to identify a specific time range to display. When *name* is not specified, all the time ranges defined in the system are displayed.

Format	show time-range [*name*]
Mode	Privileged EXEC

The information in the following table is displayed when no time range name is specified.

Term	Definition
Admin Mode	The administrative mode of the time range feature on the switch
Current number of all Time Ranges	The number of time ranges currently configured in the system.
Maximum number of all Time Ranges	The maximum number of time ranges that can be configured in the system.
Time Range Name	Name of the time range.
Status	Status of the time range (active/inactive)
Periodic Entry count	The number of periodic entries configured for the time range.
Absolute Entry	Indicates whether an absolute entry has been configured for the time range (Exists).

Auto-Voice over IP Commands

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

auto-voip

Use this command to configure auto VoIP mode. The supported modes are protocol-based and oui-based. Protocol-based auto VoIP prioritizes the voice data based on the Layer-4 port used for the voice session. OUI-based auto VoIP prioritizes the phone traffic based on the known OUI of the phone.

When both modes are enabled, if the connected phone OUI is one of the configured OUI, then the voice data is prioritized using OUI Auto VoIP, otherwise protocol-based auto VoIP is used to prioritize the voice data.

Active sessions are cleared if protocol-based auto VoIP is disabled on the port.

Default	oui-based
Format	`auto-voip [protocol-based | oui-based]`
Mode	Global Config, Interface Config

no auto-voip

Use the `no` form of the command to set the default mode.

auto-voip oui

Use this command to configure an OUI for Auto VoIP. The traffic from the configured OUI will get the highest priority over the other traffic. The *`oui-prefix`* is a unique OUI that identifies the device manufacturer or vendor. The OUI is specified in three octet values (each octet represented as two hexadecimal digits) separated by colons. The *`string`* is a description of the OUI that identifies the manufacturer or vendor associated with the OUI.

Default	A list of known OUIs is present.
Format	`auto-voip oui` *`oui-prefix`* `oui-desc` *`string`*
Mode	Global Config

Example: The following example shows how to add an OUI to the table.

```
(UBNT EdgeSwitch) (Config)#auto-voip oui 00:03:6B desc “Cisco VoIPPhone”
```

no auto-voip oui

Use the `no` form of the command to remove a configured OUI prefix from the table.

Format	`no auto-voip oui` *`oui-prefix`*
Mode	Global Config

auto-voip oui-based priority

Use this command to configure the global OUI based auto VoIP priority. If the phone OUI is matches one of the configured OUI, then the priority of traffic from the phone is changed to OUI priority configured through this command. The *priority-value* is the 802.1p priority used for traffic that matches a value in the known OUI list. If the interface detects an OUI match, the switch assigns the traffic in that session to the traffic class mapped to this priority value. Traffic classes with a higher value are generally used for time-sensitive traffic.

Default	Highest available priority.
Format	`auto-voip oui-based priority` *priority-value*
Mode	Global Config

Example: The following example shows how to add an OUI to the table.

```
(UBNT EdgeSwitch) (Config)#auto-voip oui 00:03:6B desc “Cisco VoIPPhone”
```

no auto-voip oui

Use the `no` form of the command to remove a configured OUI prefix from the table.

Format	`no auto-voip oui` *oui-prefix*
Mode	Global Config, Interface Config

auto-voip protocol-based

Use this command to configure the global protocol-based auto VoIP remarking priority or traffic-class. If remark priority is configured, the voice data of the session is remarked with the priority configured through this command. The *remark-priority* is the 802.1p priority used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device marks traffic in that session with the specified 802.1p priority value to ensure voice traffic always gets the highest priority throughout the network path.

The *tc* value is the traffic class used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device assigns the traffic in that session to the configured Class of Service (CoS) queue. Traffic classes with a higher value are generally used for time-sensitive traffic. The CoS queue associated with the specified traffic class should be configured with the appropriate bandwidth allocation to allow priority treatment for VoIP traffic.



Note: You must enable tagging on auto VoIP enabled ports to remark the voice data upon egress.

Default	Traffic class 7
Format	`auto-voip protocol-based {remark` *remark-priority* `| traffic-class` *tc*`}`
Mode	Global Config, Interface Config

no auto-voip protocol-based

Use this command to reset the global protocol based auto VoIP remarking priority or traffic-class to the default.

Format	`no auto-voip protocol-based {remark` *remark-priority* `| traffic-class` *tc*`}`
Mode	Global Config, Interface Config

auto-voip vlan

Use this command to configure the global Auto VoIP VLAN ID. The VLAN behavior is depend on the configured auto VoIP mode. The auto-VoIP VLAN is the VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN.

Default	None
Format	`auto-voip vlan` *vlan-id*
Mode	Global Config

no auto-voip vlan

Use the `no` form of the command to reset the auto-VoIP VLAN ID to the default value.

Format `no auto-voip vlan`

Mode Global Config

show auto-voip

Use this command to display the auto VoIP settings on the interface or interfaces of the switch.

Format `show auto-voip {protocol-based|oui-based} interface {slot/port|all}`

Mode Privileged EXEC

Term	Description
VoIP VLAN ID	The global VoIP VLAN ID.
Prioritization Type	The type of prioritization used on voice traffic.
Class Value	• If the Prioritization Type is configured as traffic-class, then this value is the queue value. • If the Prioritization Type is configured as remark, then this value is 802.1p priority used to remark the voice traffic.
Priority	The 802.1p priority. This field is valid for OUI auto VoIP.
AutoVoIP Mode	The Auto VoIP mode on the interface.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)# show auto-voip protocol-based interface all

VoIP VLAN Id..................................... 2
Prioritization Type.............................. traffic-class
Class Value...................................... 7

Interface      Auto VoIP    Operational Status
                  Mode
---------    -------------- -----------------
0/1          Disabled       Down
0/2          Disabled       Down
0/3          Disabled       Down
0/4          Disabled       Down
```

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)# show auto-voip oui-based interface all

VoIP VLAN Id..................................... 2
Priority......................................... 7

Interface    Auto VoIP    Operational Status
               Mode
---------  -------------- ------------------
0/1        Disabled       Down
0/2        Disabled       Down
0/3        Disabled       Down
0/4        Disabled       Down
0/5        Disabled       Down
```

show auto-voip oui-table

Use this command to display the VoIP OUI table information.

Format `show auto-voip oui-table`

Mode Privileged EXEC

Term	Description
`OUI`	OUI of the source MAC address.
`Status`	Default or configured entry.
`OUI Description`	Description of the OUI.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch)# show auto-voip oui-table

OUI          Status         Description
---------    ----------     ---------
00:01:E3     Default        SIEMENS
00:03:6B     Default        CISCO1
00:01:01     Configured     VoIP phone
```

Chapter 8: Power over Ethernet (PoE) Commands

This chapter describes the PoE commands available in the EdgeSwitch CLI.

This chapter includes the following sections:

- **"PoE Management Commands" on page 411**



Note: The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

PoE Management Commands

This section lists the available PoE commands on the EdgeSwitch.

show poe counters

This command displays the related counters of PoE status on specific port(s).

Format `show poe counters {all | intf-range}`

Mode Privileged EXEC

Term	Description
Intf	The valid PoE slot/port number.
MPS Absent	Number of times the powered device has no longer requested power from the port (MPS is the Maintenance Power Signature.)
Invalid Signature	Counter of invalid signature in specific PoE port.
Power Denied	Counter of power denied in specific PoE port.
Over Load	Counter of over loading in specific PoE port.
Short Counter	Counter of short in specific PoE port.

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show poe counters all

          MPS    Invalid   Power  Over Short
Intf      Absent Signature Denied Load Counter
--------- ------ --------- ------ ---- -------
0/1       0      3298      0      0    0
0/2       0      3298      0      0    0
0/3       0      3298      0      0    0
0/4       0      3298      0      0    0
0/5       0      3947      0      0    0
0/6       0      3947      0      0    0
...
```

clear poe counters

This command clears the related counter of PoE status on specific port(s).

Format `clear poe counters {all | intf-range}`

Mode Privileged EXEC

show poe port

This command displays the PoE configuration of specific ports.

Format `show poe port {all | intf-range}`

Mode Privileged EXEC

Term	Description
Intf	The valid PoE slot/port number.
OP Mode	PoE Operational Mode
HP Enable	High Power Enable
HP Mode	High Power Mode
Detect Enable	Detect Enable
Disconnect Enable	Disconnect Enable
Class Enable	Class Enable

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show poe port all

          OP          HP       HP       Detect  Disconnect Class
Intf      Mode        Enable   Mode     Enable  Enable     Enable
--------- ----------- -------  -------  ------- ---------- -------
0/1       Auto        Enable   802.3at  Enable  Enable     Enable
0/2       Auto        Enable   802.3at  Enable  Enable     Enable
0/3       Auto        Enable   802.3at  Enable  Enable     Enable
0/4       Auto        Enable   802.3at  Enable  Enable     Enable
0/5       Auto        Enable   802.3at  Enable  Enable     Enable
0/6       Auto        Enable   802.3at  Enable  Enable     Enable
...
```

show poe status

This command displays the PoE status on specific ports.

Format `show poe status {all | intf-range}`

Mode Privileged EXEC

Term	Description
Intf	The valid PoE slot/port number.
Detection	Detection Status
Class	Class status
Consumed(W)	Consumed Power
Voltage(V)	Port Voltage
Current(mA)	Port Current
Temperature(C)	Temperature

Example: The following shows example CLI display output for the command.

```
(UBNT EdgeSwitch) #show poe status all

Intf      Detection      Class   Consumed(W) Voltage(V) Current(mA) Temperature(C)
--------- -------------- ------- ----------- ---------- ----------- --------------
0/1       Short          Unknown        0.00       0.00        0.00             37
0/2       Open Circuit   Unknown        0.00       0.00        0.00             37
0/3       Open Circuit   Unknown        0.00       0.00        0.00             37
0/4       Open Circuit   Unknown        0.00       0.00        0.00             37
0/5       Open Circuit   Unknown        0.00       0.00        0.00             41
0/6       Open Circuit   Unknown        0.00       0.00        0.00             41
...
```

poe opmode

This command sets the PoE operational mode on specific port(s).

Format `poe opmode {auto | passive24V | shutdown}`

Mode Interface Config, Interface Range Config

Parameter	Description
`auto`	Configure auto for PoE operational mode.
`passive24v`	Configure passive 24V mode for PoE operation mode. Note: Cannot be set before the port linkup.
`shutdown`	Disable PoE power on specific port.

Appendix A: Log Messages

This chapter lists common log messages that are provided by the EdgeSwitch, along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem will assist Ubiquiti in determining the root cause of such a problem. The most recent log messages are displayed first.



Note: This chapter is not a complete list of all syslog messages.

The chapter contains the following sections:

- **"Core" on page 414**
- **"Utilities" on page 416**
- **"Management" on page 419**
- **"Switching" on page 421**
- **"QoS" on page 427**
- **"Technologies" on page 428**
- **"O/S Support" on page 430**

Core

Table 15. NIM Log Messages

Component	Message	Cause
NIM	`NIM: L7_ATTACH out of order for interface unit x slot x port x`	Interface creation out of order.
NIM	`NIM: Failed to find interface at unit x slot x port x for event(x)`	There is no mapping between the USP and Interface number.
NIM	`NIM: L7_DETACH out of order for interface unit x slot x port x`	Interface creation out of order.
NIM	`NIM: L7_DELETE out of order for interface unit x slot x port x`	Interface creation out of order.
NIM	`NIM: event(x),intf(x),component(x), in wrong phase`	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	`NIM: Failed to notify users of interface change`	Event was not propagated to the system.
NIM	`NIM: failed to send message to NIM message Queue.`	NIM message queue full or non-existent.
NIM	`NIM: Failed to notify the components of L7_CREATE event`	Interface not created.
NIM	`NIM: Attempted event (x), on USP x.x.x before phase 3`	A component issued an interface event during the wrong initialization phase.
NIM	`NIM: incorrect phase for operation`	An API call was made during the wrong initialization phase.
NIM	`NIM: Component(x) failed on event(x) for interface`	A component responded with a fail indication for an interface event.
NIM	`NIM: Timeout event(x), interface remainingMask = xxxx`	A component did not respond before the NIM timeout occurred.

Table 16. SIM Log Message

Component	Message	Cause
SIM	`IP address conflict on service port/ network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx`	This message appears when an address conflict is detected in the LAN for the service port/network port IP address.

Table 17. System Log Messages

Component	Message	Cause
SYSTEM	`Configuration file fastpath.cfg size is 0 (zero) bytes`	The configuration file could not be read. This message may occur on a system where no configuration has ever been saved or whose configuration has been erased.
SYSTEM	`could not separate SYSAPI_CONFIG_ FILENAME`	The configuration file could not be read. This message may occur on a system where no configuration has ever been saved or whose configuration has been erased.
SYSTEM	`Building defaults for file filename version version_num`	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.
SYSTEM	`File filename: same version (version_ num) but the sizes (version_size – expected_version_size) differ`	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	`Migrating config file filename from version version_num to version_num`	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.

Table 17. System Log Messages (Continued)

Component	Message	Cause
SYSTEM	`Building Defaults`	The configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	`sysapiCfgFileGet failed size = expected_size_of_file_version = expected_version`	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

Utilities

Table 18. Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	`Link Up/Down: slot/port`	An interface changed link state.

Table 19. DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	`Unable to create r/w lock for DHCP Filtering`	Unable to create semaphore used for dhcp filtering configuration structure.
DHCP Filtering	`Failed to register with nv Store.`	Unable to register save and restore functions for configuration save.
DHCP Filtering	`Failed to register with NIM`	Unable to register with NIM for interface callback functions.
DHCP Filtering	`Error on call to sysapiCfgFileWrite file`	Error on trying to save configuration.

Table 20. NVStore Log Messages

Component	Message	Cause
NVStore	`Building defaults for file XXX`	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	`Error on call to osapiFsWrite routine on file XXX`	Either the file cannot be opened or the OS's file I/O returned an error trying to write to the file.
NVStore	`File XXX corrupted from file system. Checksum mismatch.`	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	`Migrating config file XXX from version Y to Z`	A configuration file version mismatch was detected so a configuration file migration has started.

Table 21. RADIUS Log Messages

Component	Message	Cause
RADIUS	`RADIUS: Invalid data length - xxx`	The RADIUS Client received an invalid message from the server.
RADIUS	`RADIUS: Failed to send the request`	A problem communicating with the RADIUS server.
RADIUS	`RADIUS: Failed to send all of the request`	A problem communicating with the RADIUS server during transmit.
RADIUS	`RADIUS: Could not get the Task Sync semaphore!`	Resource issue with RADIUS Client service.
RADIUS	`RADIUS: Buffer is too small for response processing`	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	`RADIUS: Could not allocate accounting requestInfo`	Resource issue with RADIUS Client service.
RADIUS	`RADIUS: Could not allocate requestInfo`	Resource issue with RADIUS Client service.
RADIUS	`RADIUS: osapiSocketRecvFrom returned error`	Error while attempting to read data from the RADIUS server.
RADIUS	`RADIUS: Accounting-Response failed to validate, id = xxx`	The RADIUS Client received an invalid message from the server.
RADIUS	`RADIUS: User (xxx) needs to respond for challenge`	An unexpected challenge was received for a configured user.
RADIUS	`RADIUS: Could not allocate a buffer for the packet`	Resource issue with RADIUS Client service.
RADIUS	`RADIUS: Access-Challenge failed to validate, id = xxx`	The RADIUS Client received an invalid message from the server.

Table 21. RADIUS Log Messages (Continued)

Component	Message	Cause
RADIUS	`RADIUS: Failed to validate Message-Authenticator, id = xxx`	The RADIUS Client received an invalid message from the server.
RADIUS	`RADIUS: Access-Accept failed to validate, id = xxx`	The RADIUS Client received an invalid message from the server.
RADIUS	`RADIUS: Invalid packet length — xxx`	The RADIUS Client received an invalid message from the server.
RADIUS	`RADIUS: Response is missing Message-Authenticator, id = xxx`	The RADIUS Client received an invalid message from the server.
RADIUS	`RADIUS: Server address doesn't match configured server`	RADIUS Client received a server response from an unconfigured server.

Table 22. TACACS+ Log Messages

Component	Message	Cause
TACACS+	`TACACS+: authentication error, no server to contact`	TACACS+ request needed, but no servers are configured.
TACACS+	`TACACS+: connection failed to server x.x.x.x`	TACACS+ request sent to server `x.x.x.x` but no response was received.
TACACS+	`TACACS+: no key configured to encrypt packet for server x.x.x.x`	No key configured for the specified server.
TACACS+	`TACACS+: received invalid packet type from server.`	Received packet type that is not supported.
TACACS+	`TACACS+: invalid major version in received packet.`	Major version mismatch.
TACACS+	`TACACS+: invalid minor version in received packet.`	Minor version mismatch.

Table 23. LLDP Log Message

Component	Message	Cause
LLDP	`lldpTask(): invalid message type:xx. xxxxxx:xx`	Unsupported LLDP packet received.

Table 24. SNTP Log Message

Component	Message	Cause
SNTP	`SNTP: system clock synchronized on %s UTC`	Indicates that SNTP has successfully synchronized the time of the box with the server.

Table 25. DHCPv6 Client Log Messages

Component	Message	Cause
DHCP6 Client	`ip6Map dhcp add failed.`	This message appears when the update of a DHCP leased IP address to IP6Map fails.
DHCP6 Client	`osapiNetAddrV6Add failed on interface xxx.`	This message appears when the update of a DHCP leased IP address to the kernel IP Stack fails.
DHCP6 Client	`Failed to add DNS Server xxx to DNS Client.`	This message appears when the update of a DNS6 Server address given by the DHCPv6 Server to the DNS6 Client fails.
DHCP6 Client	`Failed to add Domain name xxx to DNS Client.`	This message appears when the update of a DNS6 Domain name info given by the DHCPv6 Server to the DNS6 Client fails.

Table 26. DHCPv4 Client Log Messages

Component	Message	Cause
DHCP4 Client	`Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt`	This message appears when a message is received from the DHCP Server that contains an unsupported Vendor Option.
DHCP4 Client	`Failed to acquire an IP address on xxx; DHCP Server did not respond.`	This message appears when the DHCP Client fails to lease an IP address from the DHCP Server.
DHCP4 Client	`DNS name server entry add failed.`	This message appears when the update of a DNS Domain name server info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	`DNS domain name list entry addition failed.`	This message appears when the update of a DNS Domain name list info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	`Interface xxx Link State is Down. Connect the port and try again.`	This message appears when the Network protocol is configured with DHCP without any active links in the Management VLAN.

Management

Table 27. SNMP Log Message

Component	Message	Cause
SNMP	`EDB Callback: Unit Join: x.`	A new unit has joined the stack.

Table 28. EmWeb Log Messages

Component	Message	Cause
EmWeb	`EMWEB (Telnet): Max number of Telnet login sessions exceeded`	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	`EMWEB (SSH): Max number of SSH login sessions exceeded`	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	`Handle table overflow`	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	`ConnectionType EmWeb socket accept() failed: errno`	Socket accept failure for the specified connection type.
EmWeb	`ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.`	Socket receive failure.
EmWeb	`EmWeb: connection allocation failed`	Memory allocation failure for the new connection.
EmWeb	`EMWEB TransmitPending: EWOULDBLOCK error sending data`	Socket error on send.
EmWeb	`ewaNetHTTPEnd: internal error - handle not in Handle table`	EmWeb handle index not valid.
EmWeb	`ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!`	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	`EmWeb accept: XXXX`	Accept function for new SSH connection failed. *XXXX* indicates the error info.

Table 29. CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	`Telnet Send Failed errno = 0x%x`	Failed to send text string to the telnet client.
CLI_UTIL	`osapiFsDir failed`	Failed to obtain the directory information from a volume's directory.

Table 30. WEB Log Messages

Component	Message	Cause
WEB	`Max clients exceeded`	This message is shown when the maximum allowed java client connections to the switch is exceeded.
WEB	`Error on send to sockfd XXXX, closing connection`	Failed to send data to the java clients through the socket.
WEB	`# (XXXX) Form Submission Failed. No Action Taken.`	The form submission failed and no action is taken. *XXXX* indicates the file under consideration.
WEB	`ewaFormServe_file_download() - WEB Unknown return code from tftp download result`	Unknown error returned while downloading file using TFTP from web interface.
WEB	`ewaFormServe_file_upload() - Unknown return code from tftp upload result`	Unknown error returned while uploading file using TFTP from web interface.
WEB	`Web UI Screen with unspecified access attempted to be brought up`	Failed to get application-specific authorization handle provided to EmWeb/Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.

Table 31. CLI_WEB_MGR Log Messages

Component	Message	Cause
CLI_WEB_MGR	`File size is greater than 2K`	The banner file size is greater than 2K bytes.
CLI_WEB_MGR	`No. of rows greater than allowed maximum of XXXX`	When the number of rows exceeds the maximum allowed rows.

Table 32. SSHD Log Messages

Component	Message	Cause
SSHD	`SSHD: Unable to create the global (data) semaphore`	Failed to create semaphore for global data protection.
SSHD	`SSHD: Msg Queue is full, event = XXXX`	Failed to send the message to SSHD message queue as message queue is full. *XXXX* is the event to be sent.
SSHD	`SSHD: Unknown UI event in message, event = XXXX`	Failed to dispatch the UI event to the appropriate SSHD function as it is an invalid event. *XXXX* indicates the event to be dispatched.
SSHD	`sshdApiCnfgrCommand: Failed calling sshdIssueCmd.`	Failed to send the message to the SSHD message queue.

Table 33. SSLT Log Messages

Component	Message	Cause
SSLT	`SSLT: Exceeded maximum, ssltConnectionTask`	Exceeded maximum allowed SSLT connections.
SSLT	`SSLT: Error creating Secure server socket6`	Failed to create secure server socket for IPV6.
SSLT	`SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ`	Failed to open connection to unsecure server. *XXXX* is the unsecure server socket address. *YYYY* is the result returned from connect function and *ZZZZ* is the error code.
SSLT	`SSLT: Msg Queue is full, event = XXXX`	Failed to send the received message to the SSLT message queue as message queue is full. *XXXX* indicates the event to be sent.
SSLT	`SSLT: Unknown UI event in message, event = XXXX`	Failed to dispatch the received UI event to the appropriate SSLT function as it is an invalid event. *XXXX* indicates the event to be dispatched.
SSLT	`ssltApiCnfgrCommand: Failed calling ssltIssueCmd.`	Failed to send the message to the SSLT message queue.
SSLT	`SSLT: Error loading certificate from file XXXX`	Failed while loading the SSLcertificate from specified file. *XXXX* indicates the file from where the certificate is being read.
SSLT	`SSLT: Error loading private key from file`	Failed while loading private key for SSL connection.
SSLT	`SSLT: Error setting cipher list (no valid ciphers)`	Failed while setting cipher list.
SSLT	`SSLT: Could not delete the SSL semaphores`	Failed to delete SSL semaphores during cleanup of all resources associated with OpenSSL Locking semaphores.

Table 34. User_Manager Log Messages

Component	Message	Cause
User_Manager	`User Login Failed for XXXX`	Failed to authenticate user login. *XXXX* indicates the username to be authenticated.
User_Manager	`Access level for user XXXX could not be determined. Setting to READ_ONLY.`	Invalid access level specified for the user. The access level is set to `READ_ONLY`. *XXXX* indicates the username.
User_Manager	`Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.`	Failed to migrate the config file. *XXXX* is the config file name. *YYYY* is the old version number and *ZZZZ* is the new version number.

Switching

Table 35. Protected Ports Log Messages

Component	Message	Cause
Protected Ports	`Protected Port: failed to save configuration`	This appears when the protected port configuration cannot be saved.
Protected Ports	`protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port`	This appears when protectedPortCfgRWLock Fails.
Protected Ports	`protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback`	This appears when nimRegisterIntfChange with VLAN fails.
Protected Ports	`Cannot add interface` *`xxx`* `to group` *`yyy`*	This appears when an interface could not be added to a particular group.
Protected Ports	`unable to set protected port group`	This appears when a dtl call fails to add interface mask at the driver level.
Protected Ports	`Cannot delete interface xxx from group` *`yyy`*	This appears when a dtl call to delete an interface from a group fails.
Protected Ports	`Cannot update group` *`YYY`* `after deleting interface` *`XXX`*	This message appears when an update group for a interface deletion fails.
Protected Ports	`Received an interface change callback while not ready to receive it`	This appears when an interface change call back has come before the protected port component is ready.

Table 36. IP Subnet VLANs Log Messages

Component	Message	Cause
IP subnet VLANs	`ERROR vlanIpSubnetSubnetValid:Invalid subnet`	This occurs when an invalid pair of subnet and netmask has come from the CLI.
IP subnet VLANs	`IP Subnet Vlans: failed to save configuration`	This message appears when save configuration of subnet VLANs failed.
IP subnet VLANs	`vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet`	This appears when a read/write lock creations fails.
IP subnet VLANs	`vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback`	This appears when this component unable to register for VLAN change notifications.
IP subnet VLANs	`vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore`	This appears when a semaphore deletion of this component fails.
IP subnet VLANs	`vlanIpSubnetDtlVlanCreate: Failed`	This appears when a dtl call fails to add an entry into the table.
IP subnet VLANs	`vlanIpSubnetSubnetDeleteApply: Failed`	This appears when a dtl fails to delete an entry from the table.
IP subnet VLANs	`vlanIpSubnetVlanChangeCallback: Failed to add an Entry`	This appears when a dtl fails to add an entry for a vlan add notify event.
IP subnet VLANs	`vlanIpSubnetVlanChangeCallback: Failed to delete an Entry`	This appears when a dtl fails to delete an entry for a VLAN delete notify event.

Table 37. MAC-based VLANs Log Messages

Component	Message	Cause
MAC based VLANs	`MAC VLANs: Failed to save configuration`	This message appears when save configuration of MAC VLANs failed.
MAC based VLANs	`vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac`	This appears when a read/write lock creations fails.
MAC based VLANs	`Unable to register for VLAN change callback`	This appears when this component unable to register for VLAN change notifications.
MAC based VLANs	`vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore`	This appears when a semaphore deletion of this component fails.

Table 37. MAC-based VLANs Log Messages (Continued)

Component	Message	Cause
MAC based VLANs	`vlanMacAddApply: Failed to add an entry`	This appears when a dtl call fails to add an entry into the table.
MAC based VLANs	`vlanMacDeleteApply: Unable to delete an Entry`	This appears when a dtl fails to delete an entry from the table.
MAC based VLANs	`vlanMacVlanChangeCallback: Failed to add an entry`	This appears when a dtl fails to add an entry for a VLAN add notify event.
MAC based VLANs	`vlanMacVlanChangeCallback: Failed to delete an entry`	This appears when a dtl fails to delete an entry for an VLAN delete notify event.

Table 38. 802.1X Log Messages

Component	Message	Cause
802.1X	`function: Failed calling dot1xIssueCmd`	802.1X message queue is full.
802.1X	`function: EAP message not received from server`	RADIUS server did not send required EAP message.
802.1X	`function: Out of System buffers`	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	`function: could not set state to authorized/unauthorized, intf` *xxx*	DTL call failed setting authorization state of the port.
802.1X	`dot1xApplyConfigData: Unable to enable/disable dot1x in driver`	DTL call failed enabling/disabling 802.1X.
802.1X	`dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed`	Failed sending message to RADIUS server.
802.1X	`dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex =` *xxx*	Failed sending accounting start to RADIUS server.
802.1X	`function: failed sending terminate cause, intf` *xxx*	Failed sending accounting stop to RADIUS server.

Table 39. IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	`function: osapiMessageSend failed`	IGMP Snooping message queue is full.
IGMP Snooping	`Failed to set global igmp snooping mode to` *xxx*	Failed to set global IGMP Snooping mode due to message queue being full.
IGMP Snooping	`Failed to set igmp snooping mode xxx for interface` *yyy*	Failed to set interface IGMP Snooping mode due to message queue being full.
IGMP Snooping	`Failed to set igmp mrouter mode` *xxx* `for interface` *yyy*	Failed to set interface multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	`Failed to set igmp snooping mode` *xxx* `for vlan` *yyy*	Failed to set VLAN IGMP Snooping mode due to message queue being full.
IGMP Snooping	`Failed to set igmp mrouter mode%d for interface` *xxx* `on Vlan` *yyy*	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	`snoopCnfgrInitPhase1Process: Error allocating small buffers`	Could not allocate buffers for small IGMP packets.
IGMP Snooping	`snoopCnfgrInitPhase1Process: Error allocating large buffers`	Could not allocate buffers for large IGMP packets.

Table 40. GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/GMRP	`garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:`	The garpQueue is full, logs specifics of the message content like internal interface number, type of message, etc.
GARP/GVRP/GMRP	`GarpSendPDU: QUEUE SEND FAILURE`	The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle, etc.
GARP/GVRP/GMRP	`garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.`	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
GARP/GVRP/GMRP	`garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent`	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/GMRP	`gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X`	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/GMRP	`gmd_create_entry: GMRP failure adding MFDB entry: vlan %d and address %s`	MFDB table is full.

Table 41. 802.3ad Log Messages

Component	Message	Cause
802.3ad	`dot3adReceiveMachine: received default event %x`	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	`dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)`	The event sent to NIM was not completed successfully.

Table 42. FDB Log Message

Component	Message	Cause
FDB	`fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d`	Unable to set the age time in the hardware.

Table 43. Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	`dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d`	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 44. IPV6 Provisioning Log Message

Component	Message	Cause
IPV6 Provisioning	`ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d`	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 45. MFDB Log Message

Component	Message	Cause
MFDB	`mfdbTreeEntryUpdate: entry does not exist`	Trying to update a non existing entry.

Table 46. 802.1Q Log Messages

Component	Message	Cause
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d – %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config.
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify its member set via management.
802.1Q	dtl failure when adding ports to vlan id %d – portMask = %s	Failed to add the ports to VLAN entry in hardware.
802.1Q	dtl failure when deleting ports from vlan id %d – portMask = %s	Failed to delete the ports for a VLAN entry from the hardware.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d – portMask = %s	Failed to add the port to the tagged list in hardware.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d – portMask = %s”	Failed to delete the port to the tagged list from the hardware.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x”	Failed to receive the dot1q message from dot1q message queue.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Failed to create VLAN ID, VLAN Database reached maximum values.
802.1Q	Attempt to create a vlan (%d) that already exists	Creation of the existing Dynamic VLAN ID from the CLI.
802.1Q	DTL call to create VLAN %d failed with rc %d”	Failed to create VLAN ID in hardware.
802.1Q	Problem unrolling data for VLAN %d	Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.
802.1Q	VLan %d does not exist	Failed to delete VLAN entry.
802.1Q	VLan %d requestor type %d does not exist	Failed to delete dynamic VLAN ID if the given requestor is not valid.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Failed to delete, as some unknown component has taken the ownership.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Failed to delete VLAN ID from the hardware.
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Failed to modify the VLAN group filter.
802.1Q	Cannot find vlan %d to convert it to static	Failed to convert Dynamic VLAN to static VLAN. VLAN ID does not exist.

Table 46. 802.1Q Log Messages (Continued)

Component	Message	Cause
802.1Q	`Only Dynamically created VLANs can be converted`	Error while trying to convert the static created VLAN ID to static.
802.1Q	`Cannot modify tagging of interface %s to non existence vlan %d"`	Error for a given interface sets the tagging property for all the VLANs in the vlan mask.
802.1Q	`Error in updating data for VLAN %d in VLAN database`	Failed to add VLAN entry into VLAN database.
802.1Q	`DTL call to create VLAN %d failed with rc %d`	Failed to add VLAN entry in hardware.
802.1Q	`Not valid permission to delete the VLAN %d`	Failed to delete static VLAN ID. Invalid requestor.
802.1Q	`Attempt to set access vlan with an invalid vlan id %d`	Invalid VLAN ID.
802.1Q	`Attempt to set access vlan with (%d) that does not exist`	VLAN ID does not exist.
802.1Q	`VLAN create currently underway for VLAN ID  %d`	Creating a VLAN which is already under process of creation.
802.1Q	`VLAN ID %d is already exists as static VLAN`	Trying to create already existing static VLAN ID.
802.1Q	`Cannot put a message on dot1q msg Queue, Returns:%d`	Failed to send Dot1q message on Dot1q message Queue.
802.1Q	`Invalid dot1q Interface: %s`	Failed to add VLAN to a member of port.
802.1Q	`Cannot set membership for user interface %s on management vlan %d`	Failed to add VLAN to a member of port.
802.1Q	`Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s`	Incorrect tagmode for VLAN tagging.
802.1Q	`Cannot set tagging for interface %d on non existent VLAN %d"`	The VLAN ID does not exist.
802.1Q	`Cannot set tagging for interface %d which is not a member of VLAN %d`	Failure in Setting the tagging configuration for a interface on a range of VLAN.
802.1Q	`VLAN create currently underway for VLAN ID  %d"`	Trying to create the VLAN ID which is already under process of creation.
802.1Q	`VLAN ID %d already exists`	Trying to create the VLAN ID which is already exists.
802.1Q	`Failed to delete, Default VLAN %d cannot be deleted`	Trying to delete Default VLAN ID.
802.1Q	`Failed to delete, VLAN ID %d is not a static VLAN`	Trying to delete Dynamic VLAN ID from CLI.
802.1Q	`Requestor %d attempted to release internal VLAN %d: owned by %d`	-

Table 47. 802.1S Log Messages

Component	Message	Cause
802.1S	`dot1sIssueCmd: Dot1s Msg Queue is full!!!! Event: %u, on interface: %u, for instance: %u`	The message Queue is full.
802.1S	`dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded`	The current conditions (e.g., port is not enabled, or currently not finished processing another BPDU on the same interface) does not allow us to process this BPDU.
802.1S	`dot1sBpduTransmit(): could not get a buffer`	Out of system buffers.

Table 48. Port MAC Locking Log Message

Component	Message	Cause
Port Mac Locking	`pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.`	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 49. Protocol-based VLANs Log Message

Component	Message	Cause
Protocol Based VLANs	`pbVlanCnfgrInitPhase2Process: Unable to register NIM callback`	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol Based VLANs	`pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with VLANs`	Appears when VLANRegisterForChange fails to register pbVlan for VLAN changes.
Protocol Based VLANs	`pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore`	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

QoS

Table 50. ACL Log Messages

Component	Message	Cause
ACL	`Total number of ACL rules (x) exceeds max (y) on intf i.`	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	`ACL name, rule x: This rule is not being logged`	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	`aclLogTask: error logging ACL rule trap for correlator number`	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	`IP ACL number: Forced truncation of one or more rules during config migration`	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 51. CoS Log Message

Component	Message	Cause
COS	`cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults`	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 52. DiffServ Log Messages

Component	Message	Cause
DiffServ	`diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device`	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.
DiffServ	`Policy invalid for service intf: policy name, interface x, direction y`	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

Technologies

Table 53. Error Messages

Component	Message	Cause
Broadcom	`Invalid USP unit = x, slot = x, port = x`	A port was not able to be translated correctly during the receive.
Broadcom	`In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x`	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
Broadcom	`Failed installing mirror action - rest of the policy applied successfully`	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured.
Broadcom	`Policy x does not contain rule x`	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy. Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy.
Broadcom	`ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x`	An issue installing the policy due to a possible duplicate hash.
Broadcom	`ACL x not found in internal table`	Attempting to delete a non-existent ACL.
Broadcom	`ACL internal table overflow`	Attempting to add an ACL to a full table.
Broadcom	`In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x`	Attempting to configure the bandwidth beyond its capabilities.
Broadcom	`USL: failed to put sync response on queue`	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.
Broadcom	`USL: failed to sync ipmc table on unit = x`	Either the transport failed or the message was dropped.
Broadcom	`usl_task_ipmc_msg_send(): failed to send with x`	Either the transport failed or the message was dropped.
Broadcom	`USL: No available entries in the STG table`	The Spanning Tree Group table is full in USL.
Broadcom	`USL: failed to sync stg table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: A Trunk doesn't exist in USL`	Attempting to modify a Trunk that doesn't exist.
Broadcom	`USL: A Trunk being created by bcmx already existed in USL`	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	`USL: A Trunk being destroyed doesn't exist in USL`	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	`USL: A Trunk being set doesn't exist in USL`	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	`USL: failed to sync trunk table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: Mcast entry not found on a join`	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	`USL: Mcast entry not found on a leave`	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	`USL: failed to sync dVLAN data on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: failed to sync policy table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

Table 53. Error Messages (Continued)

Component	Message	Cause
Broadcom	`USL: failed to sync VLAN table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`Invalid LAG id x`	Possible synchronization issue between the BCM driver and HAPI.
Broadcom	`Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x`	Uport not valid from BCM driver.
Broadcom	`Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x`	USP not able to be calculated from the learn event for BCM driver.
Broadcom	`Unable to insert route R/P`	Route *R* with prefix *P* could not be inserted in the hardware route table. A retry will be issued.
Broadcom	`Unable to Insert host H`	Host *H* could not be inserted in hardware host table. A retry will be issued.
Broadcom	`USL: failed to sync L3 Intf table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: failed to sync L3 Host table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: failed to sync L3 Route table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: failed to sync initiator table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: failed to sync terminator table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	`USL: failed to sync ip-multicast table on unit = x`	Could not synchronize unit *x* due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

O/S Support

Table 54. Linux BSP Log Message

Component	Message	Cause
Linux BSP	`rc = 10`	Second message logged at bootup, right after Starting code… Always logged.

Table 55. OSAPI Linux Log Messages

Component	Message	Cause
OSAPI Linux	`osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! or osapiNetlinkDumpOpen: unable to bind socket! errno = XX`	Couldn't open a netlink socket. Make sure "ARP Daemon support" (CONFIG_ARPD) is enabled in the Linux kernel, if the reference kernel binary is not being used.
OSAPI Linux	`ipstkNdpFlush: sending delete failed`	Failed when telling the kernel to delete a neighbor table entry (the message is incorrect).
OSAPI Linux	`unable to open /proc/net/ipv6/conf/default/hop_limit`	IPv6 MIB objects read, but /proc file system is not mounted, or running kernel does not have IPV6 support.
OSAPI Linux	`osapimRouteEntryAdd, errno XX adding 0xYY to ZZ or osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ`	Error adding or deleting an IPv4 route (listed in hex as *YY*), on the interface with Linux name *ZZ*. Error code can be looked up in errno.h.
OSAPI Linux	`l3intfAddRoute: Failed to Add Route` *or* `l3intfDeleteRoute: Failed to Delete Route`	Error adding or deleting a default gateway in the kernel's routing table (the function is really osapiRawMRouteAdd()/Delete()).
OSAPI Linux	`osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ or osapiNetIPSet: ioctl on XX failed: addr: 0x%YY`	Failed trying to set the IP address (in hex as *YY*) of the interface with Linux name *XX*, and the interface does not exist. Sometimes this is a harmless race condition (e.g. trying to set address 0 when DHCPing on the network port (dtl0) at bootup, before it is created using TAP).
OSAPI Linux	`ping: sendto error`	Trouble sending an ICMP echo request packet for the UI ping command. Maybe there was no route to that network.
OSAPI Linux	`Failed to Create Interface`	Out of memory at system initialization time.
OSAPI Linux	`TAP Unable to open XX`	The /dev/tap file is missing, or, if not using the reference kernel binary, the kernel is missing "Universal TUN/TAP device driver support" (CONFIG_TUN).
OSAPI Linux	`Tap monitor task is spinning on select failures` *then* `Tap monitor select failed: XX`	Trouble reading the /dev/tap device, check the error message *XX* for details.
OSAPI Linux	`Log_Init: log file error - creating new log file`	This pertains to the "event log" persistent file in flash. Either it did not exist, or had a bad checksum.
OSAPI Linux	`Log_Init: Flash (event) log full; erasing`	Event log file has been cleared; happens at boot time.
OSAPI Linux	`Log_Init: Corrupt event log; erasing`	Event log file had a non-blank entry after a blank entry; therefore, something was messed up.
OSAPI Linux	`Failed to Set Interface IP Address` *or* `IP Netmask` *or* `Broadcast Address` *or* `Flags` *or* `Hardware Address` *or* `Failed to Retrieve Interface Flags`	Trouble adding VRRP IP or MAC address(es) to a Linux network interface.

Appendix B: Contact Information

Ubiquiti Networks Support

Ubiquiti Support Engineers are located around the world and are dedicated to helping customers resolve software, hardware compatibility, or field issues as quickly as possible. We strive to respond to support inquiries within a 24-hour period.

Online Resources

Support: **support.ubnt.com**

Community: **community.ubnt.com**

Downloads: **downloads.ubnt.com**



Ubiquiti Networks, Inc.
2580 Orchard Parkway
San Jose, CA 95131
www.ubnt.com

©2014-2015 Ubiquiti Networks, Inc. All rights reserved. Ubiquiti, Ubiquiti Networks, the Ubiquiti U logo, the Ubiquiti beam logo, and EdgeSwitch are trademarks or registered trademarks of Ubiquiti Networks, Inc. in the United States and in other countries. All other trademarks are the property of their respective owners.

AI042315