



CLI Reference Guide

Managed Switches

1900003588 REV2.0.0

May 2026

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. All the brands and product names are trademarks or registered trademarks of their respective holders. © 2026 TP-Link

<https://www.omadanetworks.com/>

CONTENTS

Preface	1
Chapter 1 Using the CLI	9
1.1 Accessing the CLI	9
1.1.1 Logon by a console port	9
1.1.2 Logon by Telnet	12
1.1.3 Logon by SSH	13
1.2 CLI Command Modes	20
1.3 Privilege Restrictions	24
1.4 Conventions	24
1.4.1 PoE Disclaimer	24
1.4.2 Format Conventions	24
1.4.3 Special Characters	24
1.4.4 Parameter Format	25
Chapter 2 Line Commands (Only for Certain Devices)	26
2.1 line	26
2.2 media-type rj45	27
Chapter 3 User Interface	28
3.1 enable	28
3.2 service password-encryption	28
3.3 enable password	29
3.4 enable secret	30
3.5 configure	31
3.6 key config-key general key	32
3.7 exit	33
3.8 end	33
3.9 clipaging	34
3.10 history	34
3.11 history clear	35
Chapter 4 User Management Commands	36
4.1 user name (password)	36
4.2 user name (algorithm-type)	37
4.3 user name (secret)	39
4.4 service password-recovery	40

4.5	service passwd-complexity	41
4.6	service passwd-complexity min-length	42
4.7	service passwd-complexity min-class-number	42
4.8	service passwd-complexity max-repeat-number	43
4.9	service passwd-complexity max-keyboard-consecutive-num	44
4.10	service passwd-complexity not-current	45
4.11	service passwd-complexity not-username	45
4.12	service passwd-complexity not-manufacturer-name	46
4.13	service passwd-cycle	47
4.14	show user account-list	48
4.15	show user configuration	48
4.16	show client	49
Chapter 5	System Configuration Commands	50
5.1	system-time manual	50
5.2	system-time ntp	50
5.3	system-time dst predefined	52
5.4	system-time dst date	53
5.5	system-time dst recurring	54
5.6	hostname	55
5.7	location	56
5.8	contact-info	56
5.9	led	57
5.10	ip management-vlan	58
5.11	ip address	59
5.12	ip address-alloc	60
5.13	controller cloud-based	61
5.14	controller inform-url	61
5.15	controller discover	62
5.16	controller dns-adoption	63
5.17	reset	64
5.18	service reset-disable	65
5.19	reboot	65
5.20	reboot-schedule	66
5.21	copy running-config startup-config	67
5.22	copy startup-config tftp	67
5.23	copy tftp startup-config	68
5.24	copy backup-config tftp	69

5.25	copy backup-config startup-config	69
5.26	copy running-config backup-config.....	70
5.27	copy tftp backup-config	70
5.28	ftp get.....	71
5.29	ftp put.....	72
5.30	scp get	73
5.31	scp put	73
5.32	sftp get.....	74
5.33	sftp put.....	75
5.34	copy logging	76
5.35	copy logging tftp	76
5.36	boot application	77
5.37	boot config.....	77
5.38	remove backup-image	78
5.39	firmware upgrade.....	79
5.40	patch load (Only for Certain Devices).....	80
5.41	patch active (Only for Certain Devices).....	80
5.42	patch run (Only for Certain Devices).....	81
5.43	patch deactivate (Only for Certain Devices)	82
5.44	patch uninstall (Only for Certain Devices)	82
5.45	patch delete (Only for Certain Devices)	83
5.46	show patch information (Only for Certain Devices)	83
5.47	mcu-firmware unit upgrade (Only for Certain Devices).....	84
5.48	mcu-firmware type (Only for Certain Devices).....	85
5.49	checkpoint file (Only for Certain Devices)	85
5.50	show checkpoint (Only for Certain Devices).....	86
5.51	rollback running-config file (Only for Certain Devices)	87
5.52	boot autoinstall start	87
5.53	boot autoinstall persistent-mode	88
5.54	boot autoinstall auto-save.....	89
5.55	boot autoinstall auto-reboot.....	89
5.56	boot autoinstall retry-count	90
5.57	show boot autoinstall	90
5.58	show boot autoinstall downloaded-config.....	91
5.59	ping.....	92
5.60	tracert	93
5.61	show system-info.....	94
5.62	show image-info.....	94

5.63	show boot.....	95
5.64	show running-config	95
5.65	show startup-config	96
5.66	show system-time	96
5.67	show system-time dst.....	97
5.68	show system-time ntp.....	97
5.69	show cable-diagnostics interface.....	98
5.70	show cpu-utilization.....	99
5.71	show memory-utilization	99
5.72	show controller.....	100
5.73	show temperature.....	100
5.74	show voltage.....	101
5.75	clear config interface	101
5.76	power backup unit (Only for Certain Devices)	102
5.77	show power (Only for Certain Devices).....	102
Chapter 6	PTP Configuration Commands (Only for Certain Devices).....	104
6.1	ptp enable (Global View)	104
6.2	ptp profile	105
6.3	ptp clock-type	105
6.4	ptp domain	106
6.5	ptp clock-class	107
6.6	ptp priority1	107
6.7	ptp priority2	108
6.8	ptp slave-only	109
6.9	ptp utc-offset.....	109
6.10	ptp virtual-id.....	110
6.11	ptp enable (Interface View).....	111
6.12	ptp announce-interval.....	111
6.13	ptp announce-timeout	112
6.14	ptp sync-interval	113
6.15	ptp delay-req-interval	114
6.16	ptp pdelay-req-interval	114
6.17	ptp clock-step	115
6.18	ptp delay-mechanism	116
6.19	ptp asymmetry-correction	117
6.20	ptp eth-egress.....	117
6.21	ptp udp-egress.....	118

6.22	ptp reset-statistics	119
6.23	show ptp all	120
6.24	show ptp interface	120
Chapter 7 File System Configuration Commands (Only for Certain Devices)		
	122	
7.1	copy.....	122
7.2	cd	122
7.3	dir	123
7.4	pwd	123
7.5	rename.....	124
7.6	delete	124
7.7	ftp.....	125
7.8	open	126
7.9	put.....	126
7.10	get.....	127
7.11	close	127
Chapter 8 Management Port Configuration Commands (Only for Certain Devices)		
	129	
8.1	management-port protocol	129
8.2	management-port ip.....	129
8.3	management-port ipv6 enable	130
8.4	management-port ipv6 address	131
8.5	show management-port	131
Chapter 9 EEE Configuration Commands		
	133	
9.1	eee	133
9.2	show interface eee	133
Chapter 10 SDM Template Commands.....		
	135	
10.1	show sdm prefer dynamic	135
Chapter 11 Time Range Commands		
	136	
11.1	time-range.....	136
11.2	absolute	136
11.3	periodic.....	137
11.4	holiday (time-range mode)	138
11.5	holiday.....	139

11.6	show holiday	139
11.7	show time-range	140
Chapter 12 Interface Configuration Commands		141
12.1	interface.....	141
12.2	interface range	142
12.3	description	143
12.4	shutdown.....	143
12.5	flow-control.....	144
12.6	duplex.....	145
12.7	jumbo-size.....	145
12.8	speed	146
12.9	clear counters.....	147
12.10	mtu.....	147
12.11	ipv6 gateway	148
12.12	ipv6 dnsDynamic.....	148
12.13	show fiber-ports.....	149
12.14	show interface status	150
12.15	show interface counters.....	150
12.16	show interface configuration.....	151
12.17	show onvif ipc-classify.....	152
Chapter 13 Port Isolation Commands		153
13.1	port isolation	153
13.2	show port isolation interface	154
Chapter 14 Loopback Detection Commands		155
14.1	loopback-detection (global).....	155
14.2	loopback-detection interval.....	155
14.3	loopback-detection recovery-time	156
14.4	loopback-detection (interface).....	157
14.5	loopback-detection config process-mode.....	157
14.6	loopback-detection recover	158
14.7	show loopback-detection global	159
14.8	show loopback-detection interface	160
Chapter 15 Stack Commands (Only for Certain Devices).....		161
15.1	switch stack-group.....	161
15.2	group-info.....	162

15.3	interface port	162
15.4	switch priority	163
15.5	switch renumber	163
15.6	switch provision	164
15.7	switch mac-delay	165
15.8	switch mad enable	166
15.9	switch mad disable	166
15.10	switch mad restore	167
15.11	switch mad detect mode direct interface.....	168
15.12	switch mac-delay show.....	168
15.13	show switch mad detail	169
15.14	show switch stack-ports	169
15.15	show switch.....	170
15.16	show switch neighbors	170
Chapter 16 DDM Commands (Only for Certain Devices).....		172
16.1	ddm state enable	172
16.2	ddm shutdown.....	173
16.3	ddm temperature_threshold.....	173
16.4	ddm voltage_threshold.....	174
16.5	ddm bias_current_threshold.....	175
16.6	ddm tx_power_threshold.....	176
16.7	ddm rx_power_threshold.....	177
16.8	show ddm configuration	178
16.9	show ddm status	179
16.10	show fiber-ports.....	179
Chapter 17 Etherchannel Commands		181
17.1	channel-group	181
17.2	port-channel load-balance	182
17.3	lacp system-priority	183
17.4	lacp port-priority	184
17.5	lacp timeout	184
17.6	show etherchannel	186
17.7	show etherchannel load-balance.....	186
17.8	show lacp.....	187
17.9	show lacp sys-id.....	188

Chapter 18 MLAG Commands (Only for Certain Devices) 189

18.1	mlag enable	189
18.2	mlag disable	190
18.3	interface.....	190
18.4	priority	191
18.5	dad interface.....	192
18.6	dad param	192
18.7	dad tx-interval.....	193
18.8	dad timeout	194
18.9	dad enable.....	195
18.10	keep-alive interval.....	195
18.11	keep-alive timeout	196
18.12	mlag	197
18.13	mlag config-consistency-check	198
18.14	mlag config-consistency-check mode	198
18.15	show mlag info.....	199
18.16	show mlag dual-active	200
18.17	show mlag keep-alive.....	200
18.18	show mlag members-info	201
18.19	show mlag config-consistency-check.....	202

Chapter 19 MAC Address Commands..... 203

19.1	mac address-table static.....	203
19.2	no mac address-table dynamic	204
19.3	mac address-table aging-time	204
19.4	mac address-table filtering	205
19.5	mac address-table notification	206
19.6	mac address-table max-mac-count.....	207
19.7	mac address-table notification (interface)	208
19.8	mac address-table security	209
19.9	mac address-table vlan-security	210
19.10	mac-address flapping detection.....	211
19.11	show mac address-table	213
19.12	show mac address-table exclude	213
19.13	show mac address-table include	214
19.14	clear mac address-table.....	214
19.15	show mac address-table aging-time.....	215
19.16	show mac address-table max-mac-count	216

19.17	show mac address-table interface	216
19.18	show mac address-table count.....	217
19.19	show mac address-table address.....	218
19.20	show mac address-table vlan	218
19.21	show mac address-table notification.....	219
19.22	show mac address-table security.....	220
Chapter 20 IEEE 802.1Q VLAN Commands		221
20.1	vlan	221
20.2	name.....	222
20.3	vlan_trunk (globally).....	222
20.4	vlan_trunk (interface).....	223
20.5	switchport general allowed vlan.....	224
20.6	switchport pvid.....	224
20.7	switchport check ingress	225
20.8	switchport acceptable frame.....	226
20.9	show vlan summary	227
20.10	show vlan brief.....	227
20.11	show vlan.....	228
20.12	show interface switchport.....	228
Chapter 21 MAC-based VLAN Commands.....		230
21.1	mac-vlan mac-address	230
21.2	mac-vlan	231
21.3	show mac-vlan.....	231
21.4	show mac-vlan interface	232
21.5	show dot1x mac-vlan	232
21.6	show dot1x vlan.....	233
21.7	show dot1x interface switchport	234
21.8	show dot1x acl.....	234
21.9	show dot1x redirect-message	235
Chapter 22 Protocol-based VLAN Commands		236
22.1	protocol-vlan template	236
22.2	protocol-vlan vlan	237
22.3	protocol-vlan group.....	238
22.4	show protocol-vlan template.....	239
22.5	show protocol-vlan vlan.....	240

Chapter 23 Private VLAN Commands (Only for Certain Devices)	241
23.1 private-vlan primary	241
23.2 private-vlan community	241
23.3 private-vlan isolated	242
23.4 private-vlan association	243
23.5 switchport private-vlan	243
23.6 switchport private-vlan host-association	244
23.7 switchport private-vlan mapping	245
23.8 show vlan private-vlan	246
23.9 show vlan private-vlan interface	246
Chapter 24 VLAN-VPN Commands (Only for Certain Devices)	248
24.1 dot1q-tunnel	248
24.2 switchport dot1q-tunnel tpid	249
24.3 dot1q-tunnel mapping	249
24.4 switchport dot1q-tunnel mode	250
24.5 switchport dot1q-tunnel missdrop (only for certain devices)	251
24.6 switchport dot1q-tunnel use_inner_priority	252
24.7 switchport dot1q-tunnel mapping	252
24.8 switchport dot1q-tunnel replace	253
24.9 switchport dot1q-tunnel replace-out	254
24.10 show dot1q-tunnel	255
24.11 show dot1q-tunnel mapping	256
24.12 show dot1q-tunnel interface	256
Chapter 25 ERPS Commands	258
25.1 erps ring	258
25.2 control-vlan	258
25.3 description	259
25.4 guard-timer	260
25.5 wtr-timer	260
25.6 holdoff-timer	261
25.7 protected-instance	262
25.8 raps-mel	263
25.9 revertive	263
25.10 sub-ring	264
25.11 tc-notify erps	264
25.12 tc-protection interval	265

25.13	tc-protection threshold	266
25.14	version	266
25.15	virtual-channel.....	267
25.16	erps ring rpl	268
25.17	erps ring protect-switch	268
25.18	show erps ring	269
25.19	show erps statistics (only for certain devices)	270
Chapter 26 GVRP Commands.....		271
26.1	gvrp.....	271
26.2	gvrp (interface)	271
26.3	gvrp registration.....	272
26.4	gvrp timer	273
26.5	show gvrp interface.....	274
26.6	show gvrp global	275
Chapter 27 IGMP Snooping Commands.....		276
27.1	ip igmp snooping (global).....	276
27.2	ip igmp snooping version	276
27.3	ip igmp snooping drop-unknown	277
27.4	ip igmp snooping header-validation	278
27.5	ip igmp snooping vlan-config	278
27.6	ip igmp snooping vlan-config (immediate-leave)	280
27.7	ip igmp snooping vlan-config (report-suppression)	281
27.8	ip igmp snooping vlan-config (router-ports-forbidden).....	282
27.9	ip igmp snooping vlan-config (rport interface)	283
27.10	ip igmp snooping vlan-config (static)	283
27.11	ip igmp snooping vlan-config (querier)	284
27.12	ip igmp snooping vlan-config drop-unknown	286
27.13	ip igmp snooping vlan-config route-unknown.....	286
27.14	ip igmp snooping vlan-config ssdp-flood.....	287
27.15	ip igmp snooping vlan-config querier-election	288
27.16	ip igmp snooping querier robustness	289
27.17	ip igmp snooping (interface)	290
27.18	ip igmp snooping max-groups.....	290
27.19	ip igmp snooping immediate-leave.....	292
27.20	ip igmp snooping authentication.....	292
27.21	ip igmp snooping accounting	293

27.22	ip igmp snooping tcn.....	294
27.23	ip igmp snooping tcn flood-query-count.....	294
27.24	ip igmp snooping tcn query-solicit	295
27.25	ip igmp snooping vlan-config tcn-flood.....	296
27.26	ip igmp snooping querier tcn-query-count.....	297
27.27	ip igmp snooping querier tcn-query-interval.....	298
27.28	ip igmp profile.....	299
27.29	deny.....	299
27.30	permit.....	300
27.31	range	300
27.32	ip igmp filter	301
27.33	clear ip igmp snooping statistics	302
27.34	show ip igmp snooping	302
27.35	show ip igmp snooping interface.....	303
27.36	show ip igmp snooping vlan.....	304
27.37	show ip igmp snooping groups	304
27.38	show ip igmp profile.....	305
Chapter 28 Layer 3 IGMP Commands (Only for Certain Devices).....		307
28.1	ip igmp (global).....	307
28.2	ip igmp (on specific ports)	307
28.3	ip igmp header-validation.....	308
28.4	ip igmp join-group.....	309
28.5	ip igmp mroute-proxy.....	309
28.6	ip igmp offlink.....	310
28.7	ip igmp proxy unsolicited-report-interval.....	310
28.8	ip igmp proxy-service.....	311
28.9	ip igmp querier-timeout	311
28.10	ip igmp static-group	312
28.11	ip igmp version	313
28.12	ip igmp last-member-query-count	313
28.13	ip igmp last-member-query-interval.....	314
28.14	ip igmp query-interval	315
28.15	ip igmp query-max-response-time.....	316
28.16	ip igmp robustness	316
28.17	ip igmp startup-query-interval.....	317
28.18	show ip igmp	318
28.19	show ip igmp groups	318

28.20	show ip igmp proxy groups	319
28.21	show ip igmp interface	320
Chapter 29 PIM Commands (Only for Certain Devices).....		321
29.1	ip multicast-routing	321
29.2	ip pim (globally)	321
29.3	ip pim (on specific ports).....	322
29.4	ip pim dense-mode.....	323
29.5	ip pim sparse-mode.....	323
29.6	ip pim anycast-rp	324
29.7	ip pim ignore-rp-set-priority	325
29.8	ip pim register-rate-limit	325
29.9	ip pim register-rp-reachability	326
29.10	ip pim register-source.....	327
29.11	ip pim register-suppression.....	327
29.12	ip pim router-id	328
29.13	ip pim bsr-candidate.....	329
29.14	ip pim rp-candidate.....	329
29.15	ip pim rp-register-kat	330
29.16	ip pim spt-threshold	331
29.17	ip pim rp-address	331
29.18	ip pim ssm	332
29.19	ip pim bsr-border	333
29.20	ip pim exclude-genid	333
29.21	ip pim dr-priority	334
29.22	ip pim hello-holdtime	334
29.23	ip pim hello-interval	335
29.24	ip pim passive	335
29.25	ip pim propagation-delay.....	336
29.26	ip pim state-refresh	337
29.27	ip pim unicast-bsm	337
29.28	ip pim join-prune-interval.....	338
29.29	show ip multicast	338
29.30	show ip mroute	339
29.31	show ip pim	340
29.32	show ip pim interface	340
29.33	show ip pim local-MemberShip	341
29.34	show ip pim mroute	342

29.35	show ip pim neighbor	342
29.36	show ip pim nexthop.....	343
29.37	show ip pim statistic	343
29.38	show ip pim bsr-router	344
29.39	show ip pim rp mapping.....	345
29.40	show ip pim rp-hash	345
29.41	show ip pim ssm	346
Chapter 30 PIM6 Commands (Only for Certain Devices)		347
30.1	ipv6 multicast-routing	347
30.2	ipv6 pim anycast-rp	347
30.3	ipv6 pim bsr-candidate	348
30.4	ipv6 pim dense-mode	349
30.5	ipv6 pim ignore-rp-set-priority	350
30.6	ipv6 pim register-rate-limit.....	350
30.7	ipv6 pim register-rp-reachability.....	351
30.8	ipv6 pim register-source	351
30.9	ipv6 pim register-suppression	352
30.10	ipv6 pim router-id.....	353
30.11	ipv6 pim rp embedded	353
30.12	ipv6 pim rp-address	354
30.13	ipv6 pim rp-candidate	355
30.14	ipv6 pim rp-register-kat.....	355
30.15	ipv6 pim sparse-mode	356
30.16	ipv6 pim spt-threshold.....	357
30.17	ipv6 pim ssm	357
30.18	ipv6 pim (on specific ports)	358
30.19	ipv6 pim bsr-border	358
30.20	ipv6 pim dr-priority	359
30.21	ipv6 pim exclude-genid.....	359
30.22	ipv6 pim hello-holdtime	360
30.23	ipv6 pim hello-interval	361
30.24	ipv6 pim join-prune-interval	361
30.25	ipv6 pim passive.....	362
30.26	ipv6 pim propagation-delay	363
30.27	ipv6 pim state-refresh.....	363
30.28	ipv6 pim unicast-bsm	364
30.29	show ipv6 multicast	364

30.30	show ipv6 pim	365
30.31	show ipv6 pim bsr-router	365
30.32	show ipv6 pim interface.....	366
30.33	show ipv6 pim local-MemberShip.....	367
30.34	show ipv6 pim mroute	367
30.35	show ipv6 pim neighbor.....	368
30.36	show ipv6 pim nexthop	368
30.37	show ipv6 pim rp-hash	369
30.38	show ipv6 pim rp mapping.....	370
30.39	show ipv6 pim ssm.....	370
30.40	show ipv6 pim statistic.....	371
Chapter 31 Static Multicast Routing Commands (Only for Certain Devices) ..		372
31.1	ip mroute	372
31.2	show ip mroute static	373
Chapter 32 VRF Commands (Only for Certain Devices)		374
32.1	vrf.....	374
32.2	address-family.....	375
32.3	exit-address-family.....	375
32.4	vrf forwarding	376
32.5	show vrf	377
Chapter 33 MLD Snooping Commands.....		378
33.1	ipv6 mld snooping (global).....	378
33.2	ipv6 mld snooping drop-unknown	378
33.3	ipv6 mld snooping vlan-config	379
33.4	ipv6 mld snooping vlan-config (immediate-leave)	380
33.5	ipv6 mld snooping vlan-config (report-suppression)	381
33.6	ipv6 mld snooping vlan-config (router-ports-forbidden).....	382
33.7	ipv6 mld snooping vlan-config (rport interface)	383
33.8	ipv6 mld snooping vlan-config (static)	383
33.9	ipv6 mld snooping vlan-config (querier)	384
33.10	ipv6 mld snooping vlan-config drop-unknown.....	386
33.11	ipv6 mld snooping vlan-config route-unknown.....	387
33.12	ipv6 mld snooping (interface)	387
33.13	ipv6 mld snooping max-groups.....	388
33.14	ipv6 mld snooping immediate-leave	389
33.15	ipv6 mld profile	390

33.16	deny	390
33.17	permit	391
33.18	range	391
33.19	ipv6 mld filter	392
33.20	clear ipv6 mld snooping statistics	393
33.21	show ipv6 mld snooping	393
33.22	show ipv6 mld snooping interface	394
33.23	show ipv6 mld snooping vlan	395
33.24	show ipv6 mld snooping groups	395
33.25	show ipv6 mld profile	396
Chapter 34 IPv6 MLD Commands (Only for Certain Devices)		397
34.1	ipv6 mld	397
34.2	ipv6 mld last-member-query-count	397
34.3	ipv6 mld last-member-query-interval	398
34.4	ipv6 mld mroute-proxy	399
34.5	ipv6 mld proxy-service	399
34.6	ipv6 mld querier-timeout	400
34.7	ipv6 mld query-interval	400
34.8	ipv6 mld query-max-response-time	401
34.9	ipv6 mld robustness	401
34.10	ipv6 mld startup-query-count	402
34.11	ipv6 mld startup-query-interval	402
34.12	ipv6 mld static-group	403
34.13	ipv6 mld version	404
34.14	show ipv6 mld groups	404
34.15	show ipv6 mld proxy groups	405
34.16	show ipv6 mld interface	405
34.17	show ipv6 mld	406
Chapter 35 CPP Commands		407
35.1	cpp-policy	407
35.2	rate-limit protocol	408
35.3	rate-limit queue-rate (only for certain devices)	409
35.4	rate-limit cpu-rate (only for certain devices)	410
35.5	cpp-policy-apply default-policy	411
35.6	cpp-policy-apply policy	411
35.7	show cpp all	412

35.8	show cpp default-policy	412
35.9	show cpp policy.....	413
35.10	show cpp statistics all (only for certain devices).....	414
35.11	show cpp statistics protocol (only for certain devices)	414
35.12	show cpp statistics cpu-rate	415
35.13	clear cpp statistics all (only for certain devices).....	416
35.14	clear cpp statistics protocol (only for certain devices).....	416
Chapter 36 MVR Commands		418
36.1	mvr (global).....	418
36.2	mvr group	418
36.3	mvr mode.....	419
36.4	mvr querytime.....	420
36.5	mvr vlan.....	421
36.6	mvr (interface).....	421
36.7	mvr type.....	422
36.8	mvr immediate.....	423
36.9	mvr vlan (group).....	423
36.10	mvr mode dynamic auto-enable	424
36.11	show mvr	425
36.12	show mvr interface	425
36.13	show mvr members	426
Chapter 37 MSTP Commands.....		427
37.1	debug spanning-tree.....	427
37.2	debug spanning-tree port-state	428
37.3	spanning-tree (global)	429
37.4	spanning-tree (interface)	429
37.5	spanning-tree priority	430
37.6	spanning-tree common-config	430
37.7	spanning-tree mode	432
37.8	spanning-tree mst configuration	433
37.9	instance	433
37.10	name.....	434
37.11	revision	435
37.12	spanning-tree mst instance	435
37.13	spanning-tree mst	436
37.14	spanning-tree timer	437

37.15	spanning-tree hold-count	438
37.16	spanning-tree max-hops	439
37.17	spanning-tree bpdufilter	439
37.18	spanning-tree bpduflood	440
37.19	spanning-tree bpduguard	441
37.20	spanning-tree guard loop	441
37.21	spanning-tree guard root	442
37.22	spanning-tree guard tc	443
37.23	spanning-tree mcheck	443
37.24	show spanning-tree active	444
37.25	show spanning-tree bridge	444
37.26	show spanning-tree interface	445
37.27	show spanning-tree vlan	446
37.28	show spanning-tree interface-security	446
37.29	show spanning-tree mst	447
37.30	show spanning-tree instance	448
Chapter 38 Debug Commands		449
38.1	debug feppacket packet-dump cpu-traffic position	449
38.2	debug feppacket packet-dump cpu-traffic dst-mac	450
38.3	debug feppacket packet-dump cpu-traffic src-mac	451
38.4	debug feppacket packet-dump cpu-traffic len-type	451
38.5	debug feppacket packet-dump cpu-traffic ip-protocol	452
38.6	debug feppacket packet-dump cpu-traffic dst-ipv4	453
38.7	debug feppacket packet-dump cpu-traffic src-ipv4	453
38.8	debug feppacket packet-dump cpu-traffic dst-ipv6	454
38.9	debug feppacket packet-dump cpu-traffic src-ipv4	455
38.10	debug feppacket packet-dump cpu-traffic dst-port	456
38.11	debug feppacket packet-dump cpu-traffic src-port	456
38.12	debug feppacket packet-dump cpu-traffic tail	457
38.13	debug feppacket packet-dump cpu-traffic rx-port	458
38.14	debug feppacket packet-dump cpu-traffic tx-port	459
38.15	debug feppacket packet-dump cpu-traffic count limit	459
38.16	debug feppacket packet-dump cpu-traffic dump-to	460
38.17	debug feppacket packet-dump port-rx rx-port dst-mac	461
38.18	debug feppacket packet-dump port-rx rx-port src-mac	462
38.19	debug feppacket packet-dump port-rx rx-port len-type	463
38.20	debug feppacket packet-dump port-rx rx-port ip-protocol	463

38.21	debug feppacket packet-dump port-rx rx-port dst-ipv4.....	464
38.22	debug feppacket packet-dump port-rx rx-port src-ipv4.....	465
38.23	debug feppacket packet-dump port-rx rx-port dst-ipv6.....	466
38.24	debug feppacket packet-dump port-rx rx-port src-ipv4.....	466
38.25	debug feppacket packet-dump port-rx rx-port dst-port.....	467
38.26	debug feppacket packet-dump port-rx rx-port src-port.....	468
38.27	debug feppacket packet-dump port-rx rx-port tail	469
38.28	debug feppacket packet-dump port-rx rx-port count limit.....	469
38.29	debug feppacket packet-dump port-rx rx-port dump-to	470
38.30	debug feppacket packet-dump download-txt-file.....	471
38.31	debug feppacket packet-dump download-pcap-file	472
38.32	debug feppacket packet-dump show-txt-file.....	473
38.33	no debug feppacket packet-dump	473
38.34	debug feppacket packet-print (only for certain devices)	474
38.35	debug spanning-tree.....	475
Chapter 39 LLDP Commands.....		477
39.1	lldp	477
39.2	lldp forward_message.....	477
39.3	lldp hold-multiplier	478
39.4	lldp timer	479
39.5	lldp receive	480
39.6	lldp transmit	480
39.7	lldp snmp-trap	481
39.8	lldp tlv-select	482
39.9	lldp management-address	482
39.10	lldp med-fast-count.....	483
39.11	lldp med-status	484
39.12	lldp med-tlv-select.....	484
39.13	lldp med-location	485
39.14	show lldp.....	486
39.15	show lldp interface.....	486
39.16	show lldp local-information interface.....	487
39.17	show lldp neighbor-information interface	488
39.18	show lldp traffic interface	488
Chapter 40 L2PT Commands (Only for Certain Devices)		490
40.1	l2protocol-tunnel.....	490

40.2	l2protocol-tunnel type	491
40.3	show l2protocol-tunnel global	492
40.4	show l2protocol-tunnel interface	493
40.5	l2protocol-tunnel dst-mac	493
40.6	show l2protocol-tunnel dst-mac.....	494
Chapter 41 PPPoE ID-Insertion Commands (Only for Certain Devices).....		495
41.1	pppoe id-insertion (global)	495
41.2	pppoe circuit-id (interface)	496
41.3	pppoe circuit-id type	496
41.4	pppoe remote-id	497
41.5	show pppoe global	498
41.6	show pppoe interface	498
Chapter 42 Static Routes Commands		500
42.1	ip routing.....	500
42.2	interface vlan	500
42.3	interface loopback.....	501
42.4	switchport	501
42.1	switchport	502
42.2	interface range port-channel.....	503
42.3	description	503
42.4	shutdown.....	504
42.5	interface port-channel	505
42.6	ip route	505
42.7	ipv6 routing	506
42.8	ipv6 route	507
42.9	show interface vlan.....	508
42.10	show ip interface	508
42.11	show ip interface brief.....	509
42.12	show ip route	509
42.13	show ip route specify	510
42.14	show ip route summary.....	511
42.15	show ip route static	511
42.16	show ip route static description	512
42.17	show ipv6 interface	512
42.18	show ipv6 route	513
42.19	show ipv6 route summary	513

42.20	show ipv6 route static	514
42.21	show ipv6 route static description	514
Chapter 43 RIP Configuration Commands (Only for Certain Devices)		516
43.1	router rip	516
43.2	network	516
43.3	version	517
43.4	timer basic	518
43.5	distance	519
43.6	auto-summary	519
43.7	default-metric	520
43.8	redistribute	520
43.9	allow-ecmp	521
43.10	default-information originate	522
43.11	neighbor	522
43.12	passive-interface	523
43.13	ip rip authentication mode	523
43.14	ip rip authentication string	524
43.15	ip rip authentication key-chain	525
43.16	ip rip receive version	526
43.17	ip rip send version	526
43.18	ip rip split-horizon	527
43.19	ip rip v2-broadcast	528
43.20	show ip rip	528
43.21	show ip rip status	529
43.22	clear ip rip	529
Chapter 44 RIPng Configuration Commands (Only for Certain Devices)		531
44.1	router ripng	531
44.2	ipv6 rip enable	532
44.3	timer basic	532
44.4	default-metric	533
44.5	redistribute	534
44.6	allow-ecmp	534
44.7	default-information originate	535
44.8	passive-interface	535
44.9	ipv6 rip split-horizon	536
44.10	ipv6 rip summary-address	537

44.11	show ipv6 rip	537
44.12	show ipv6 rip status.....	538
44.13	clear ipv6 rip.....	538
Chapter 45 OSPF Configuration Commands (Only for Certain Devices)		540
45.1	router ospf.....	540
45.2	router-id.....	541
45.3	network	541
45.4	maximum-paths	542
45.5	redistribute.....	543
45.6	default-metric	544
45.7	default-information originate.....	545
45.8	passive-interface default.....	546
45.9	auto-cost.....	546
45.10	distance	547
45.11	timers throttle spf	548
45.12	compatible rfc1583	548
45.13	area stub.....	549
45.14	area nssa	550
45.15	area default-cost.....	551
45.16	area range	551
45.17	area authentication.....	553
45.18	area virtual-link	553
45.19	area virtual-link authentication	554
45.20	area virtual-link authentication-key	555
45.21	area virtual-link message-digest-key.....	556
45.22	capability opaque.....	557
45.23	graceful-restart	558
45.24	graceful-restart grace-period.....	559
45.25	graceful-restart helper.....	559
45.26	graceful-restart helper planned-only	560
45.27	graceful-restart helper strict-lsa-checking.....	561
45.28	ip ospf area.....	561
45.29	ip ospf cost.....	562
45.30	ip ospf retransmit-interval.....	563
45.31	ip ospf transmit-delay	563
45.32	ip ospf priority.....	564
45.33	ip ospf hello-interval.....	565

45.34	ip ospf dead-interval.....	565
45.35	ip ospf authentication	566
45.36	ip ospf authentication-key	567
45.37	ip ospf message-digest-key	567
45.38	ip ospf network.....	568
45.39	ip ospf mtu-ignore	569
45.40	ip ospf passive.....	569
45.41	clear ip ospf.....	570
45.42	show ip ospf	570
45.43	show ip ospf database	571
45.44	show ip ospf interface.....	572
45.45	show ip ospf neighbor	572
45.46	show ip ospf border-routers.....	573
45.47	show ip ospf route	573
45.48	show ip ospf [process-id] graceful-restart helper	574
Chapter 46 OSPFv3 Configuration Commands (Only for Certain Devices)		575
46.1	ipv6 router ospf	575
46.2	router-id.....	576
46.3	maximum-paths	576
46.4	redistribute.....	577
46.5	default-information originate.....	578
46.6	auto-cost.....	579
46.7	distance	579
46.8	distance ospfv3.....	580
46.9	timers throttle spf	581
46.10	timers lsa arrival	582
46.11	distance ospf	582
46.12	area stub	583
46.13	area nssa	584
46.14	area range	584
46.15	ipv6 ospf area	585
46.16	ipv6 ospf cost.....	586
46.17	ipv6 ospf retransmit-interval.....	587
46.18	ipv6 ospf transmit-delay.....	588
46.19	ipv6 ospf priority	588
46.20	ipv6 ospf hello-interval.....	589
46.21	ipv6 ospf dead-interval.....	590

46.22	ipv6 ospf network	590
46.23	ipv6 ospf mtu-ignore	591
46.24	ipv6 ospf passive	591
46.25	clear ipv6 ospf	592
46.26	show ipv6 ospf.....	593
46.27	show ipv6 ospf database.....	593
46.28	show ipv6 ospf interface	593
46.29	show ipv6 ospf neighbor	594
46.30	show ipv6 ospf border-routers	594
46.31	show ipv6 ospf rib	595
Chapter 47 BFD Configuration Commands (Only for Certain Devices).....		596
47.1	bfd-template	596
47.2	detect-multiplier.....	597
47.3	receive-interval	597
47.4	transmit-interval.....	598
47.5	transmit-interval.....	599
47.6	passive-mode.....	599
47.7	ip ospf bfd.....	600
47.8	ip ospf bfd template	601
47.9	ipv6 ospf bfd	602
47.10	ipv6 ospf bfd	602
47.11	isis bfd	603
47.12	show bfd counters.....	604
47.13	show bfd neighbors.....	605
Chapter 48 BGP Configuration Commands (Only for Certain Devices)		606
48.1	router bgp.....	606
48.2	address-family {ipv4 ipv6} unicast	607
48.3	address-family {ipv4 ipv6} vrf.....	608
48.4	address-family targeted-peer evpn	608
48.5	advertise l2vpn evpn	609
48.6	aggregate-address.....	610
48.7	distance bgp	610
48.8	maximum-paths	611
48.9	network.....	612
48.10	redistribute.....	612
48.11	slow-peer detection	613

48.12	timers bgp	614
48.13	bgp always-compare-med	615
48.14	bgp bestpath as-path confed	616
48.15	bgp bestpath as-path ignore	616
48.16	bgp bestpath as-path multipath-relax.....	617
48.17	bgp bestpath compare-routerid	618
48.18	bgp bestpath med confed.....	618
48.19	bgp bestpath med missing-as-worst	619
48.20	bgp client-to-client reflection.....	620
48.21	bgp cluster-id	621
48.22	bgp confederation identifier	621
48.23	bgp confederation peers.....	622
48.24	bgp dampening	623
48.25	bgp default ipv4-unicast.....	623
48.26	bgp default local-preference	624
48.27	bgp deterministic-med	625
48.28	bgp disable-ebgp-connected-route-check.....	626
48.29	bgp fast-external-failover.....	626
48.30	bgp graceful-restart	627
48.31	bgp graceful-restart restart-time.....	628
48.32	bgp graceful-restart rib-stale-time.....	629
48.33	bgp graceful-restart select-defer-time	629
48.34	bgp graceful-restart stalepath-time	630
48.35	bgp graceful-shutdown	631
48.36	bgp listen limit.....	632
48.37	bgp listen range.....	632
48.38	bgp log-neighbor-changes	633
48.39	bgp max-med administrative	634
48.40	bgp max-med on-startup	634
48.41	bgp network import-check.....	635
48.42	bgp reject-as-sets	636
48.43	bgp router-id.....	636
48.44	no neighbor	637
48.45	neighbor activate	638
48.46	neighbor addpath-tx-all-paths	639
48.47	neighbor addpath-tx-bestpath-per-AS	640
48.48	neighbor advertisement-interval	641
48.49	neighbor allowas-in	642

48.50	neighbor as-override.....	643
48.51	neighbor attribute-unchanged	644
48.52	neighbor bfd.....	646
48.53	neighbor capability dynamic	647
48.54	neighbor dampening	648
48.55	neighbor default-originate	649
48.56	neighbor description	650
48.57	neighbor disable-connected-check.....	651
48.58	neighbor dont-capability-negotiate	652
48.59	neighbor ebgp-multihop	653
48.60	neighbor enforce-first-as	654
48.61	neighbor graceful-restart	654
48.62	neighbor graceful-restart-helper	655
48.63	neighbor local-as	656
48.64	neighbor maximum-prefix	657
48.65	neighbor maximum-prefix-out.....	658
48.66	neighbor next-hop-self	659
48.67	neighbor nexthop-local unchanged	660
48.68	neighbor override-capability	661
48.69	neighbor passive.....	662
48.70	neighbor password.....	663
48.71	neighbor peer-group	664
48.72	neighbor port	664
48.73	neighbor remote-as.....	665
48.74	neighbor remove-private-AS.....	666
48.75	neighbor route-reflector-client	667
48.76	neighbor route-server-client	668
48.77	neighbor sender-as-path-loop-detection.....	669
48.78	neighbor send-community	670
48.79	neighbor shutdown.....	671
48.80	neighbor soft-reconfiguration inbound	672
48.81	neighbor strict-capability-match	673
48.82	neighbor timers	674
48.83	neighbor timers connect	675
48.84	neighbor tracking.....	676
48.85	neighbor ttl-security hops.....	677
48.86	neighbor update-group converge	678
48.87	neighbor update-group independent.....	679

48.88	neighbor update-source.....	680
48.89	neighbor weight.....	681
48.90	show ip bgp	682
48.91	show ip bgp attribute-info	682
48.92	show ip bgp cidr-only	683
48.93	show ip bgp dampening flap-statistics	683
48.94	show ip bgp dampening dampened-paths.....	684
48.95	show ip bgp dampening parameters	684
48.96	show ip bgp {ipv4 ipv6 l2vpn evpn} all	685
48.97	show ip bgp l2vpn evpn rd.....	686
48.98	show ip bgp memory	686
48.99	show ip bgp neighbors.....	687
48.100	show ip bgp neighbors advertised-routes	687
48.101	show ip bgp neighbors bestpath-routes	688
48.102	show ip bgp neighbors dampened-routes	689
48.103	show ip bgp neighbors flap-statistics	689
48.104	show ip bgp neighbors prefix-counts	690
48.105	show ip bgp neighbors received-routes.....	690
48.106	show ip bgp neighbors routes	691
48.107	show ip bgp nexthop	692
48.108	show ip bgp peer-group	692
48.109	show ip bgp statistics.....	693
48.110	show ip bgp statistics-all	693
48.111	show ip bgp summary	694
48.112	show ip bgp update-groups.....	694
48.113	show ip bgp vrfs	695
48.114	clear ip bgp.....	695
48.115	clear ip bgp all.....	696
48.116	clear ip bgp dampening	697
48.117	clear ip bgp external	697
48.118	clear ip bgp peer-group.....	698
Chapter 49 L2VPN Configuration Commands (Only for Certain Devices).....		699
49.1	xconnect vc-id.....	699
49.2	show mpls vc	700
49.3	vsi name vsi-id vpls-id	701
49.4	description	701
49.5	signaling.....	702

49.6	encapsulation.....	703
49.7	peer	703
49.8	shutdown.....	705
49.9	show vpls.....	705
49.10	mac learning.....	706
49.11	mac aging-time.....	707
49.12	mac security.....	707
49.13	mac filtering	708
49.14	mac static	709
Chapter 50 IS-IS Configuration Commands (Only for Certain Devices)		711
50.1	router isis.....	711
50.2	area-password	712
50.3	domain-password	712
50.4	graceful-restart	713
50.5	hostname.....	714
50.6	is-type	715
50.7	log-adjacency-changes.....	716
50.8	lsp-gen-interval	716
50.9	lsp-mtu.....	717
50.10	lsp-refresh-interval.....	718
50.11	max-lsp-lifetime	718
50.12	metric-style	719
50.13	net.....	720
50.14	purge-originator	720
50.15	set-attached-bit	721
50.16	set-overload-bit	722
50.17	spf interval.....	722
50.18	topology.....	723
50.19	clear isis neighbor	723
50.20	redistribute	724
50.21	distance	725
50.22	ip router isis.....	726
50.23	ipv6 router isis	726
50.24	isis bfd	727
50.25	isis circuit-type	728
50.26	isis csnp-interval	728
50.27	isis hello-interval	729

50.28	isis hello-multiplier	730
50.29	isis metric	730
50.30	isis network point-to-point.....	731
50.31	isis passive	732
50.32	isis password-key	732
50.33	isis priority	733
50.34	topology.....	734
50.35	isis three-way-handshake	735
50.36	show isis database.....	735
50.37	show isis graceful-restart.....	736
50.38	show isis hostname	736
50.39	show isis neighbor	737
50.40	show isis route.....	738
50.41	show isis summary.....	738
50.42	show isis interface	739
50.43	show isis topology	739
Chapter 51 URPF Configuration Commands (Only for Certain Devices)		741
51.1	urpf	741
51.2	urpf mode	741
Chapter 52 Tunnel Configuration Commands (Only for Certain Devices).....		743
52.1	interface tunnel	743
52.2	tunnel mode	744
52.3	tunnel ttl.....	745
52.4	tunnel ip address.....	745
52.5	tunnel source.....	746
52.6	tunnel destination	747
52.7	keepalive period retry-times.....	748
52.8	tunnel vlan	748
52.9	shutdown.....	749
52.10	ip route tunnel.....	750
52.11	ipv6 route tunnel	750
52.12	show interface tunnel.....	751
Chapter 53 IPv6 Address Configuration Commands		753
53.1	ipv6 enable	753
53.2	ipv6 address autoconfig.....	753
53.3	ipv6 address autoglobal	754

53.4	ipv6 address link-local	755
53.5	ipv6 address dhcp	755
53.6	ipv6 address ra	756
53.7	ipv6 address eui-64	757
53.8	ipv6 address	757
53.9	ipv6 gateway	758
53.10	ipv6 dnsDynamic.....	759
53.11	show ipv6 interface	759
Chapter 54 ARP Commands.....		761
54.1	arp	761
54.2	clear arp-cache	762
54.3	arp dynamicrenew	762
54.4	arp timeout	763
54.5	gratuitous-arp intf-status-up enable.....	764
54.6	gratuitous-arp dup-ip-detected enable.....	764
54.7	gratuitous-arp learning enable	765
54.8	gratuitous-arp send-interval.....	765
54.9	ip proxy-arp.....	766
54.10	ip local-proxy-arp.....	767
54.11	show arp	768
54.12	show ip arp (interface)	768
54.13	show ip arp summary	769
54.14	show gratuitous-arp	769
54.15	show ip proxy-arp	770
Chapter 55 VRRP Commands (Only for Certain Devices)		771
55.1	ip vrrp vrid.....	771
55.2	ipv6 vrrp vrid	772
55.3	ip vrrp vrid authentication-mode.....	772
55.4	ip vrrp vrid description	773
55.5	ip vrrp vrid preempt-mode	774
55.6	ip vrrp vrid priority	775
55.7	ip vrrp vrid timer-advertise	776
55.8	ip vrrp vrid track	776
55.9	ip vrrp vrid version	777
55.10	ip vrrp vrid virtual-ip.....	778
55.11	ip vrrp vrid virtual-ip secondary.....	779

55.12	ipv6 vrrp vrid address link-local	780
55.13	ipv6 vrrp vrid address.....	781
55.14	show ip vrrp.....	781
55.15	show ip vrrp statistics	782
55.16	clear ip vrrp statistics	783
Chapter 56 DHCP Server Commands.....		784
56.1	service dhcp server	784
56.2	ip dhcp server extend-option capwap-ac-ip	784
56.3	ip dhcp server extend-option vendor-class-id.....	785
56.4	ip dhcp server excluded-address	786
56.5	ip dhcp server pool	787
56.6	ip dhcp server ping timeout	787
56.7	ip dhcp server ping packets.....	788
56.8	ip dhcp client gateway-detect.....	789
56.9	network.....	789
56.10	range	790
56.11	vrf.....	791
56.12	lease	791
56.13	address hardware-address.....	792
56.14	address client-identifier.....	793
56.15	default-gateway	794
56.16	dns-server	794
56.17	ip dns-address.....	795
56.18	ipv6 dns-address	796
56.19	netbios-name-server	796
56.20	netbios-node-type.....	797
56.21	next-server	798
56.22	domain-name.....	798
56.23	bootfile.....	799
56.24	option	800
56.25	show ip dhcp server status	800
56.26	show ip dhcp server statistics	801
56.27	show ip dhcp server extend-option.....	801
56.28	show ip dhcp server pool	802
56.29	show ip dhcp server excluded-address.....	802
56.30	show ip dhcp server manual-binding	803
56.31	show ip dhcp server binding	803

56.32	clear ip dhcp server statistics.....	804
56.33	clear ip dhcp server binding.....	804
Chapter 57 DHCPv6 Server Commands		806
57.1	ipv6 dhcp server	806
57.2	ipv6 dhcp server allow-hint.....	807
57.3	ipv6 dhcp server preference	807
57.4	ipv6 dhcp server rapid-commit.....	808
57.5	ipv6 dhcp server unicast	809
57.6	ipv6 dhcp server pool.....	809
57.7	network.....	810
57.8	prefix-delegation.....	811
57.9	address	812
57.10	description	813
57.11	dns-domain-name	813
57.12	dns-server.....	814
57.13	excluded-address.....	815
57.14	link.....	815
57.15	nis-domain-name.....	816
57.16	nis-server	817
57.17	nisp-domain-name	817
57.18	nisp-server	818
57.19	preferred-lifetime.....	819
57.20	valid-lifetime.....	819
57.21	sip-domain-name.....	820
57.22	sip-server	821
57.23	sntp-server.....	821
57.24	vrf.....	822
57.25	ipv6 dhcp server	823
57.26	ipv6 dhcp server allow-hint.....	823
57.27	ipv6 dhcp server preference	824
57.28	ipv6 dhcp server rapid-commit.....	825
57.29	ipv6 dhcp server unicast	826
57.30	ipv6 dhcp server pool.....	826
57.31	show ipv6 dhcp server binding.....	827
57.32	show ipv6 dhcp server binding summary	828
57.33	show ipv6 dhcp server pool.....	828
57.34	show ipv6 dhcp server statistics.....	829

57.35	show ipv6 dhcp server status	829
57.36	clear ipv6 dhcp server binding	830
57.37	clear ipv6 dhcp server statistics	831
Chapter 58 RA Server Commands.....		832
58.1	ipv6 nd ra suppress	832
58.2	ipv6 nd ra dns-server	833
58.3	ipv6 nd ra dns-suffix	833
58.4	ipv6 nd ra hop-limit	834
58.5	ipv6 nd ra interval.....	835
58.6	ipv6 nd ra lifetime.....	836
58.7	ipv6 nd ra managed-config-flag	836
58.8	ipv6 nd ra other-config-flag	837
58.9	ipv6 nd ra mtu	838
58.10	ipv6 nd ra preference	838
58.11	ipv6 nd ra reachable-time.....	839
58.12	ipv6 nd ra retrans-timer	840
58.13	ipv6 nd ra prefix.....	841
58.14	show ipv6 nd ra.....	842
Chapter 59 DHCP Relay Commands		843
59.1	service dhcp relay.....	843
59.2	ip dhcp relay hops.....	843
59.3	ip dhcp relay time.....	844
59.4	ip helper-address.....	845
59.5	ip dhcp relay information option	845
59.6	ip dhcp relay information strategy	846
59.7	ip dhcp relay information format.....	847
59.8	ip dhcp relay information circuit-id	848
59.9	ip dhcp relay information remote-id	849
59.10	ip dhcp relay default-interface	849
59.11	ip dhcp relay vlan	850
59.12	show ip dhcp relay	851
Chapter 60 DHCPV6 Relay Commands		852
60.1	ipv6 dhcp relay	852
60.2	ipv6 dhcp relay vlan 1 helper-address	852
60.3	ipv6 dhcp relay information option 18	853
60.4	ipv6 dhcp relay information option37	854

60.5	ipv6 dhcp relay information remote-id.....	855
60.6	show ipv6 dhcp relay.....	855
60.7	show ipv6 dhcp relay information	856
60.8	show ipv6 dhcp relay counters.....	856
Chapter 61 DHCP L2 Relay Commands		858
61.1	ip dhcp l2relay	858
61.2	ip dhcp l2relay vlan	858
61.3	ip dhcp l2relay information option	859
61.4	ip dhcp l2relay information strategy.....	860
61.5	ip dhcp l2relay information format.....	861
61.6	ip dhcp l2relay information circuit-id.....	862
61.7	ip dhcp l2relay information remote-id.....	862
61.8	show ip dhcp l2relay	863
61.9	show ip dhcp l2relay interface.....	864
Chapter 62 DHCPV6 L2 Relay Commands		865
62.1	ipv6 dhcp l2relay	865
62.2	ipv6 dhcp l2relay vlan.....	865
62.3	ipv6 dhcp l2relay forwarding-mode.....	866
62.4	ipv6 dhcp l2relay information interface-id	867
62.5	ipv6 dhcp l2relay information option18.....	867
62.6	ipv6 dhcp l2relay information option37	868
62.7	ipv6 dhcp l2relay information remote-id	869
62.8	show ipv6 dhcp l2relay	869
62.9	show ipv6 dhcp l2relay information.....	870
Chapter 63 QoS Commands.....		871
63.1	qos trust mode	871
63.2	qos port-priority	872
63.3	qos cos-map	872
63.4	qos dot1p-remap	873
63.5	qos dscp-map.....	874
63.6	qos dscp-remap.....	875
63.7	qos queue bandwidth.....	876
63.8	qos queue mode	877
63.9	qos localPri.....	878
63.10	qos cosPri.....	879
63.11	qos dscpPri	880

63.12	qos wred-profile	880
63.13	qos wred-bind.....	881
63.14	show qos wred-profile	882
63.15	show qos wred-bind interface	882
63.16	show qos cos-map	883
63.17	show qos dot1p-remap interface	883
63.18	show qos dot1p-remap	884
63.19	show qos dscp-map interface	884
63.20	show qos dscp-map	885
63.21	show qos dscp-remap interface	885
63.22	show qos dscp-remap	886
63.23	show qos port-priority interface	887
63.24	show qos trust interface.....	887
63.25	show qos queue interface	888
63.26	show qos rule.....	888
Chapter 64 Bandwidth Control Commands		890
64.1	storm-control rate-mode	890
64.2	storm-control.....	891
64.3	storm-control exceed	892
64.4	storm-control recover	893
64.5	bandwidth.....	893
64.6	show storm-control.....	894
64.7	show bandwidth	895
Chapter 65 OUI-Based VLAN Commands (Only for Certain Devices).....		896
65.1	voice vlan.....	896
65.2	voice-vlan(interface).....	897
65.3	show voice-vlan	898
Chapter 66 Voice VLAN Commands		899
66.1	voice vlan.....	899
66.2	voice vlan (interface)	899
66.3	voice vlan priority	900
66.4	voice vlan oui	901
66.5	show voice vlan	901
66.6	show voice vlan oui-table	902
66.7	show voice vlan interface	902

Chapter 67	Auto VoIP Commands	904
67.1	auto-voip	904
67.2	auto-voip (interface)	904
67.3	auto-voip dot1p	905
67.4	auto-voip untagged	906
67.5	auto-voip none	906
67.6	no auto-voip (interface)	907
67.7	auto-voip dscp	907
67.8	auto-voip data priority	908
67.9	show auto-voip	908
Chapter 68	Access Control Commands	910
68.1	user access-control ip-based enable	910
68.2	user access-control ip-based	910
68.3	user access-control mac-based enable	911
68.4	user access-control mac-based	912
68.5	user access-control port-based enable	913
68.6	user access-control port-based	913
68.7	user access-control ipv6-based enable	914
68.8	user access-control ipv6-based	915
68.9	user access-control ip-based index	916
68.10	user access-control ipv6-based index	917
68.11	user access-control mac-based index	918
68.12	user access-control port-based index	919
Chapter 69	HTTP and HTTPS Commands	921
69.1	ip http server	921
69.2	ip http port	922
69.3	ip http max-users	922
69.4	ip http session timeout	923
69.5	ip http secure-server	924
69.6	ip http secure-port	924
69.7	ip http secure-protocol	925
69.8	ip http secure-ciphersuite	926
69.9	ip http secure-max-users	927
69.10	ip http secure-subject-alt-name	928
69.11	ip http secure-certification signature-algorithm	928
69.12	ip http secure-session timeout	929

69.13	ip http secure-server download certificate.....	930
69.14	ip http secure-server download key.....	931
69.15	show ip http configuration.....	932
69.16	show ip http secure-server	932
Chapter 70 SSH Commands.....		934
70.1	ip ssh server.....	934
70.2	ip ssh port.....	934
70.3	ip ssh algorithm	935
70.4	ip ssh algorithm compatibility	936
70.5	ip ssh session-timeout.....	936
70.6	ip ssh max-client	937
70.7	ip ssh download.....	938
70.8	remove public-key	938
70.9	show ip ssh.....	939
Chapter 71 Telnet Commands.....		940
71.1	telnet	940
71.2	telnet enable	940
71.3	telnet port.....	941
71.4	show telnet-status	941
Chapter 72 Serial Port Commands.....		943
72.1	serial_port baud-rate.....	943
Chapter 73 AAA Commands		944
73.1	tacacs-server host	944
73.2	show tacacs-server.....	945
73.3	radius-server host	946
73.4	radius-server radsec-profile.....	948
73.5	download ca-certificate.....	949
73.6	download client-certificate	949
73.7	download client-key	950
73.8	show radius-server	951
73.9	show radius-server certificate.....	951
73.10	radius-server load-balance algorithm.....	952
73.11	radius-server load-balance least-outstanding	953
73.12	radius-server dead-count	953
73.13	radius-server dead-cycle	954

73.14	radius-server dead-interval.....	955
73.15	radius-server dead-time.....	955
73.16	radius-server max-unresponsiveinterval	956
73.17	radius-server testuser	957
73.18	radius-server detect-server.....	958
73.19	aaa group.....	959
73.20	server	960
73.21	server-alias.....	960
73.22	show aaa group	961
73.23	aaa authentication login.....	962
73.24	aaa authentication enable	963
73.25	aaa authentication dot1x default.....	964
73.26	aaa accounting dot1x default	965
73.27	show aaa authentication.....	965
73.28	show aaa accounting.....	966
73.29	line telnet	966
73.30	login authentication (telnet).....	967
73.31	line ssh	968
73.32	login authentication (ssh).....	968
73.33	line console	969
73.34	login authentication (console)	970
73.35	enable authentication (telnet)	970
73.36	enable authentication (ssh)	971
73.37	enable authentication (console).....	972
73.38	ip http login authentication.....	973
73.39	ip http enable authentication	974
73.40	show aaa global.....	974
73.41	enable admin password.....	975
73.42	enable admin secret	976
73.43	enable-admin.....	977
Chapter 74 IEEE 802.1x Commands.....		979
74.1	dot1x system-auth-control	979
74.2	dot1x handshake.....	980
74.3	dot1x auth-protocol	980
74.4	dot1x vlan-assignment	981
74.5	dot1x accounting	982
74.6	dot1x mab	983

74.7	dot1x guest-vlan	983
74.8	dot1x timeout quiet-period	984
74.9	dot1x timeout supp-timeout	985
74.10	dot1x max-req	986
74.11	dot1x	986
74.12	dot1x port-control	987
74.13	dot1x port-method	988
74.14	dot1x auth-init	989
74.15	dot1x auth-reauth	989
74.16	show dot1x global	990
74.17	show dot1x interface	991
74.18	show dot1x auth-state interface	991
Chapter 75 Port Security Commands (Only for Certain Devices).....		993
75.1	mac address-table max-mac count	993
75.2	mac address-table sticky mac	994
75.3	mac address-table sticky save-time	995
75.4	mac address-table spoofing-defend	996
Chapter 76 MACsec Commands (Only for Certain Devices)		997
76.1	macsec mka-policy	997
76.2	macsec apply-policy	998
76.3	macsec cipher_suite	998
76.4	macsec confidentiality-offset	999
76.5	macsec desire	1000
76.6	macsec mka	1000
76.7	macsec mka priority	1001
76.8	macsec mka psk	1002
76.9	macsec mka timer	1002
76.10	macsec replay-protection	1003
76.11	macsec validation-mode	1004
Chapter 77 Port Mirroring Commands		1005
77.1	monitor session destination interface	1005
77.2	monitor session source	1006
77.3	monitor session 1 destination remote vlan	1007
77.4	monitor session 1 source remote vlan	1008
77.5	show monitor session	1009

Chapter 78 ACL Commands..... 1010

78.1	access-list create	1010
78.2	access-list packet-content profile	1010
78.3	access-list resequence	1011
78.4	access-list mac	1012
78.5	access-list ip	1013
78.6	access-list combined	1015
78.7	access-list ipv6	1017
78.8	access-list packet-content config.....	1019
78.9	access-list action.....	1021
78.10	access-list mode action-stop.....	1021
78.11	access-list action harddrop	1022
78.12	redirect nexthops ipv4	1023
78.13	redirect nexthops ipv6	1023
78.14	nhtype ecmp	1024
78.15	nhtype standby.....	1024
78.16	vrf	1025
78.17	ip-address	1026
78.18	ipv6-address.....	1026
78.19	s-condition	1027
78.20	s-mirror	1028
78.21	qos-remark.....	1028
78.22	access bind	1029
78.23	show access-list	1030
78.24	show access-list bind.....	1031
78.25	show access-list status	1031
78.26	show access-list counter	1032
78.27	clear access-list	1032

Chapter 79 IPv4 IMPB Commands..... 1034

79.1	ip source binding.....	1034
79.2	no ip source binding interface	1035
79.3	ip dhcp snooping	1036
79.4	ip dhcp snooping vlan	1036
79.5	ip dhcp snooping max-entries.....	1037
79.6	ip dhcp snooping trust	1038
79.7	ip arp scan vlan.....	1038
79.8	ip arp scan apply	1039

79.9	show ip arp scan.....	1040
79.10	show ip source binding	1040
79.11	show ip source binding summary	1041
79.12	show ip dhcp snooping	1041
79.13	show ip dhcp snooping interface.....	1042
Chapter 80 IPv6 IMPB Commands.....		1044
80.1	ipv6 source binding	1044
80.2	no ipv6 source binding interface.....	1045
80.3	ipv6 dhcp snooping	1046
80.4	ipv6 dhcp snooping vlan.....	1046
80.5	ipv6 dhcp snooping max-entries	1047
80.6	ipv6 nd snooping.....	1048
80.7	ipv6 nd snooping vlan	1048
80.8	ipv6 nd snooping max-entries	1049
80.9	show ipv6 source binding.....	1050
80.10	show ipv6 source binding summary	1050
80.11	show ipv6 dhcp snooping.....	1051
80.12	show ipv6 dhcp snooping interface	1051
80.13	show ipv6 nd snooping	1052
80.14	show ipv6 nd snooping interface.....	1053
Chapter 81 IP Verify Source Commands.....		1055
81.1	ip verify source	1055
81.2	ip verify source logging.....	1056
81.3	show ip verify source	1056
81.4	show ip verify source interface	1057
Chapter 82 IPv6 Verify Source Commands		1058
82.1	ipv6 verify source.....	1058
82.2	show ipv6 verify source	1059
82.3	show ipv6 verify source interface	1059
Chapter 83 DHCPv4 Filter Commands		1061
83.1	ip dhcp filter	1061
83.2	ip dhcp filter vlan	1061
83.3	ip dhcp filter (interface)	1062
83.4	ip dhcp filter mac-verify.....	1063
83.5	ip dhcp filter limit rate.....	1063

83.6	ip dhcp filter decline rate	1064
83.7	ip dhcp filter server permit-entry	1065
83.8	show ip dhcp filter	1066
83.9	show ip dhcp filter interface.....	1067
83.10	show ip dhcp filter server permit-entry.....	1067
Chapter 84 DHCPv6 Filter Commands		1069
84.1	ipv6 dhcp filter	1069
84.2	ipv6 dhcp filter (interface).....	1069
84.3	ipv6 dhcp filter limit rate	1070
84.4	ipv6 dhcp filter decline rate.....	1071
84.5	ipv6 dhcp filter server permit-entry.....	1072
84.6	show ipv6 dhcp filter	1073
84.7	show ipv6 dhcp filter interface	1073
84.8	show ipv6 dhcp filter server permit-entry	1074
Chapter 85 Dying Gasp Commands		1075
85.1	dying-gasp enable oam	1075
85.2	dying-gasp enable syslog	1076
85.3	dying-gasp enable snmp	1076
85.4	show dying-gasp status.....	1077
85.5	show dying-gasp packets	1077
Chapter 86 DoS Defend Commands		1079
86.1	ip dos-prevent	1079
86.2	ip dos-prevent type	1079
86.3	show ip dos-prevent.....	1081
Chapter 87 sFlow Commands (Only for Certain Devices).....		1083
87.1	sflow address.....	1083
87.2	sflow enable	1084
87.3	sflow collector collector-ID	1084
87.4	sflow sampler.....	1085
87.5	show sflow global.....	1086
87.6	show sflow collector.....	1087
87.7	show sflow sampler	1087
Chapter 88 Ethernet OAM Commands (Only for Certain Devices)		1088
88.1	ethernet-oam.....	1088

88.2	ethernet-oam mode	1089
88.3	ethernet-oam link-monitor symbol-period.....	1089
88.4	ethernet-oam link-monitor frame	1090
88.5	ethernet-oam link-monitor frame-period	1091
88.6	ethernet-oam link-monitor frame-seconds	1093
88.7	ethernet-oam remote-failure.....	1094
88.8	ethernet-oam remote-loopback received-remote- loopback.....	1095
88.9	ethernet-oam remote-loopback	1096
88.10	clear ethernet-oam statistics	1096
88.11	clear ethernet-oam event-log.....	1097
88.12	show ethernet-oam configuration	1098
88.13	show ethernet-oam event-log.....	1099
88.14	show ethernet-oam statistics.....	1099
88.15	show ethernet-oam status	1100
Chapter 89 MPLS Commands (Only for Certain Devices)		1101
89.1	mpls (global).....	1101
89.2	mpls ttl-mode	1102
89.3	mpls ingress-lsp binding ipv4.....	1103
89.4	mpls transmit-lsp binding ipv4	1104
89.5	mpls egress-lsp binding	1105
89.6	mpls (interface).....	1106
89.7	show mpls	1106
89.8	show mpls ftn.....	1107
89.9	show mpls ilm	1108
89.10	show mpls static-lsp.....	1108
89.11	ping mpls ipv4.....	1109
89.12	tracert mpls ipv4	1110
Chapter 90 LDP Commands (Only for Certain Devices)		1112
90.1	mpls ldp	1112
90.2	lsp-id.....	1113
90.3	transport-address.....	1113
90.4	explicit-null	1114
90.5	timer	1115
90.6	targeted-peer	1116
90.7	pwe3.....	1117
90.8	label control-mode	1117

90.9	mpls ldp	1118
90.10	LDP Interface Timer.....	1119
90.11	show mpls ldp global	1120
90.12	show mpls ldp instance.....	1120
90.13	show mpls ldp fec	1121
90.14	show mpls ldp route	1122
90.15	show mpls ldp adjacency	1122
90.16	show mpls ldp session	1123
90.17	show mpls ldp interface.....	1123
90.18	show mpls ldp upstream.....	1124
90.19	show mpls ldp downstream	1125
90.20	show mpls ldp targeted-peer.....	1126
90.21	show mpls ldp entity	1126
90.22	show mpls ldp label-sapce	1127
90.23	show mpls ldp vc.....	1128
90.24	show mpls ldp vpls.....	1128
Chapter 91 DLDP Commands (Only for Certain Devices)		1130
91.1	dldp (global).....	1130
91.2	dldp interval.....	1130
91.3	dldp shut-mode	1131
91.4	dldp reset (global)	1132
91.5	dldp(interface)	1132
91.6	dldp reset (interface)	1133
91.7	show dldp	1133
91.8	show dldp interface	1134
Chapter 92 SNMP Commands		1135
92.1	snmp-server.....	1135
92.2	snmp-server view	1137
92.3	snmp-server group.....	1137
92.4	snmp-server user.....	1139
92.5	snmp-server community	1141
92.6	snmp-server host.....	1142
92.7	snmp-server source-interface	1144
92.8	snmp-server engineID	1145
92.9	snmp-server traps snmp	1146
92.10	snmp-server traps	1147

92.11	snmp-server traps ddm	1148
92.12	snmp-server traps vlan	1149
92.13	snmp-server traps security	1150
92.14	snmp-server traps security dhcp6-filter	1151
92.15	snmp-server traps acl	1151
92.16	snmp-server traps ip	1152
92.17	snmp-server traps power (Only for Certain Devices)	1152
92.18	snmp-server traps link-status	1154
92.19	rmon history	1154
92.20	rmon event	1155
92.21	rmon alarm	1156
92.22	rmon statistics	1158
92.23	show snmp-server	1159
92.24	show snmp-server view	1159
92.25	show snmp-server group	1160
92.26	show snmp-server user	1160
92.27	show snmp-server community	1160
92.28	show snmp-server host	1161
92.29	show snmp-server engineID	1161
92.30	show rmon history	1162
92.31	show rmon event	1162
92.32	show rmon alarm	1163
92.33	show rmon statistics	1164
Chapter 93 NETCONF Commands (Only for Certain Devices)		1165
93.1	netconf ssh	1165
Chapter 94 PoE Commands (Only for Certain Devices)		1166
94.1	power inline consumption (global)	1166
94.2	power profile	1166
94.3	power inline consumption (interface)	1168
94.4	power inline consumption (unit)	1168
94.5	power inline priority	1169
94.6	power inline supply	1170
94.7	power inline profile	1170
94.8	power inline time-range	1171
94.9	show power inline	1172
94.10	show power inline configuration interface	1172

94.11	show power inline information interface.....	1173
94.12	show power profile	1173
94.13	power recovery status enable	1174
94.14	power recovery status	1174
94.15	show power recovery	1175
94.16	show power recovery interface.....	1176
Chapter 95 ARP Inspection Commands.....		1177
95.1	ip arp inspection.....	1177
95.2	ip arp inspection validate.....	1177
95.3	ip arp inspection vlan	1178
95.4	ip arp inspection vlan logging	1179
95.5	ip arp inspection trust	1180
95.6	ip arp inspection limit-rate.....	1180
95.7	ip arp inspection burst-interval	1181
95.8	ip arp inspection recover.....	1182
95.9	ip arp inspection exceed	1183
95.10	show ip arp inspection	1183
95.11	show ip arp inspection interface	1184
95.12	show ip arp inspection vlan	1185
95.13	show ip arp inspection statistics.....	1185
95.14	clear ip arp inspection statistics	1186
Chapter 96 ND Detection Commands		1187
96.1	ipv6 nd detection	1187
96.2	ipv6 nd detection vlan	1187
96.3	ipv6 nd detection vlan logging.....	1188
96.4	ipv6 nd detection trust.....	1188
96.5	show ipv6 nd detection.....	1189
96.6	show ipv6 nd detection interface.....	1190
96.7	show ipv6 nd detection statistics	1190
96.8	show ipv6 nd detection vlan	1191
Chapter 97 System Log Commands		1192
97.1	logging buffer	1192
97.2	logging buffer level	1192
97.3	logging file flash	1193
97.4	logging file flash frequency	1194
97.5	logging file flash level	1195

97.6	logging host index.....	1195
97.7	logging host verify-peer	1196
97.8	logging host source-interface	1197
97.9	logging host download.....	1198
97.10	logging host remove	1199
97.11	logging console.....	1200
97.12	logging console level.....	1200
97.13	logging monitor	1201
97.14	logging monitor level.....	1202
97.15	clear logging	1203
97.16	show logging local-config	1203
97.17	show logging.....	1204
97.18	show logging loghost	1204
97.19	show logging loghost certificate-files.....	1205
97.20	show logging buffer.....	1206
97.21	show logging flash	1206

Preface

This Guide is intended for network administrator to provide referenced information about CLI (Command Line Interface). The device mentioned in this Guide stands for Managed Switch without any explanation. Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <https://www.omadanetworks.com/>

Overview of this Guide

Chapter 1: Using the CLI

Provide information about how to use the CLI, CLI Command Modes, Security Levels and some Conventions.

Chapter 2: Line Commands (Only for Certain Devices)

Provide information about the commands used to make related configurations for the desired users and set the priority of the console media type.

Chapter 3: User Interface

Provide information about the commands used to switch between five CLI Command Modes.

Chapter 4: User Management Commands

Provide information about the commands used for user management.

Chapter 5: System Configuration Commands

Provide information about the commands used for configuring the System information and System IP, reboot and reset the switch, upgrade the switch system and commands used for cable test.

Chapter 6: PTP Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the PTP (Precision Time Protocol).

Chapter 7: File System Configuration Commands

Provide information about the commands used for configuring the File System.

Chapter 8: Management Port Configuration Commands

Provide information about the commands used for configuring the Management Port.

Chapter 9: EEE Configuration Commands

Provide information about the commands used for configuring EEE (Energy Efficient Ethernet).

Chapter 10: SDM Template Commands

Provide information about the commands used for configuring the SDM templates.

Chapter 11: Time Range Commands

Provide information about the commands used for configuring the time range.

Chapter 12: Interface Configuration Commands

Provide information about the commands used for configuring the Speed, Negotiation Mode, and Flow Control for Ethernet ports.

Chapter 13: Port Isolation Commands

Provide information about the commands used for configuring Port Isolation function.

Chapter 14: Loopback Detection Commands

Provide information about the commands used for configuring the Loopback Detection function.

Chapter 15: Stack Commands (Only for Certain Devices)

Provide information about the commands used for configuring the Stack function.

Chapter 16: DDM Commands (Only for Certain Devices)

Provide information about the commands used for DDM (Digital Diagnostic Monitoring) function.

Chapter 17: Etherchannel Commands

Provide information about the commands used for configuring LAG (Link Aggregation Group) and LACP (Link Aggregation Control Protocol).

Chapter 18: MLAG Commands

Provide information about the commands used for configuring MLAG (Multichassis Link Aggregation Group).

Chapter 19: MAC Address Commands

Provide information about the commands used for Address configuration.

Chapter 20: IEEE 802.1Q VLAN Commands

Provide information about the commands used for configuring IEEE 802.1Q VLAN.

Chapter 21: MAC-based VLAN Commands

Provide information about the commands used for configuring MAC-based VLAN.

Chapter 22: Protocol-based VLAN Commands

Provide information about the commands used for configuring Protocol VLAN.

Chapter 23: Private VLAN Commands (Only for Certain Devices)

Provide information about the commands used for configuring Private VLAN.

Chapter 24: VLAN-VPN Commands (Only for Certain Devices)

Provide information about the commands used for configuring VLAN-VPN (Virtual Private Network) function.

Chapter 25: ERPS Commands

Provide information about the commands used for configuring ERPS (Ethernet Ring Protection Switching) function.

Chapter 26: GVRP Commands

Provide information about the commands used for configuring GVRP (GARP VLAN registration protocol).

Chapter 27: IGMP Snooping Commands

Provide information about the commands used for configuring the IGMP Snooping (Internet Group Management Protocol Snooping).

Chapter 28: Layer 3 IGMP Commands (Only for Certain Devices)

Provide information about the commands used for configuring the layer 3 IGMP Snooping (Internet Group Management Protocol Snooping).

Chapter 29: PIM Commands (Only for Certain Devices)

Provide information about the commands used for configuring the PIM (Protocol Independent Multicast) function.

Chapter 30: PIM6 Commands (Only for Certain Devices)

Provide information about the commands used for configuring the IPv6 PIM (Protocol Independent Multicast) function.

Chapter 31: Static Multicast Routing Commands (Only for Certain Devices)

Provide information about the commands used for configuring the Static Multicast Routing function.

Chapter 32: VRF Commands (Only for Certain Devices)

Provide information about the commands used for configuring the VRF (Virtual Routing and Forwarding) function.

Chapter 33: MLD Snooping Commands

Provide information about the commands used for configuring the MLD Snooping (Multicast Listener Discovery Snooping).

Chapter 34: IPv6 MLD Snooping Commands

Provide information about the commands used for configuring the IPv6 MLD Snooping (Multicast Listener Discovery Snooping).

Chapter 34: IPv6 MLD Snooping Commands

Provide information about the commands used for configuring the CPP (CPU Protect Policy).

Chapter 36: MVR Commands

Provide information about the commands used for configuring the MVR.

Chapter 37: MSTP Commands

Provide information about the commands used for configuring the MSTP (Multiple Spanning Tree Protocol).

Chapter 38: Debug Commands

Provide information about the commands used for configuring the debug function.

Chapter 39: LLDP Commands

Provide information about the commands used for configuring LLDP function.

Chapter 40: L2PT Commands (Only for Certain Devices)

Provide information about the commands used for configuring L2PT (Layer 2 Protocol Tunneling).

Chapter 41: PPPoE ID-Insertion Commands (Only for Certain Devices)

Provide information about the commands used for configuring PPPoE ID-Insertion.

Chapter 42: Static Routes Commands

Provide information about the commands used for configuring the Static Route function.

Chapter 43: RIP Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the RIP (Routing Information Protocol).

Chapter 44: RIPvng Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the RIP (RIP next generation).

Chapter 45: OSPF Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the OSPF (Open Shortest Path First).

Chapter 46: OSPFv3 Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the OSPFv3 (Open Shortest Path First version 3).

Chapter 47: BFD Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring BFD (Bidirectional Forwarding Detection).

Chapter 48: BGP Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring BGP (Border Gateway Protocol).

Chapter 49: L2VPN Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring L2VPN.

Chapter 50: IS-IS Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring IS-IS (Intermediate System to Intermediate System).

Chapter 51: URPF Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring URPF (Unicast Reverse Path Forwarding).

Chapter 52: Tunnel Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring Tunnel

Chapter 53: IPv6 Address Configuration Commands

Provide information about the commands used for configuring the System IPv6 addresses.

Chapter 54: ARP Configuration Commands

Provide information about the commands used for configuring the ARP (Address Resolution Protocol) functions.

Chapter 55: VRRP Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring VRRP (Virtual Router Redundancy Protocol).

Chapter 56: DHCP Server Configuration Commands

Provide information about the commands used for configuring the DHCP Server function.

Chapter 57: DHCPV6 Server Configuration Commands

Provide information about the commands used for configuring the DHCPV6 Server function.

Chapter 58: RA Server Configuration Commands

Provide information about the commands used for configuring the RA Server function.

Chapter 59: DHCP Relay Configuration Commands

Provide information about the commands used for configuring the DHCP Relay function.

Chapter 60: DHCPV6 Relay Configuration Commands

Provide information about the commands used for configuring the DHCPV6 Relay function.

Chapter 61: DHCP L2 Relay Configuration Commands

Provide information about the commands used for configuring the DHCP L2 Relay function.

Chapter 62: DHCPV6 L2 Relay Configuration Commands

Provide information about the commands used for configuring the DHCPV6 L2 Relay function.

Chapter 63: QoS Configuration Commands

Provide information about the commands used for configuring the QoS function.

Chapter 64: Bandwidth Control Configuration Commands

Provide information about the commands used for configuring the Bandwidth Control.

Chapter 65: OUI-Based VLAN Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring OUI-Based VLAN (Organizationally Unique Identifier-Based Virtual Local Area Network).

Chapter 66: Voice VLAN Configuration Commands

Provide information about the commands used for configuring Voice VLAN.

Chapter 67 Auto VoIP Configuration Commands

Provide information about the commands used for configuring Auto VoIP.

Chapter 68: Access Control Configuration Commands

Provide information about the commands used for configuring Access Control.

Chapter 69: HTTP and HTTPS Configuration Commands

Provide information about the commands used for configuring the HTTP and HTTPS logon.

Chapter 70: SSH Configuration Commands

Provide information about the commands used for configuring and managing SSH (Security Shell).

Chapter 71: Telnet Configuration Commands

Provide information about the commands used for configuring and managing SSH (Security Shell).

Chapter 72: Serial Port Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring and managing SSH (Security Shell).

Chapter 73: AAA Configuration Commands

Provide information about the commands used for configuring AAA (authentication, authorization and accounting).

Chapter 74: IEEE 802.1X Configuration Commands

Provide information about the commands used for configuring IEEE 802.1X function.

Chapter 75: Port Security Configuration Commands

Provide information about the commands used for configuring Port Security.

Chapter 76: MACsec Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the MACsec (Media Access Control Security).

Chapter 77: Port Mirroring Configuration Commands

Provide information about the commands used for configuring the Port Mirror function.

Chapter 78: ACL Configuration Commands

Provide information about the commands used for configuring the ACL (Access Control List).

Chapter 79: IPv4 IMPB Configuration Commands

Provide information about the commands used for binding the IP address, MAC address, VLAN and the connected Port number of the Host together.

Chapter 80: IPv6 IMPB Configuration Commands

Provide information about the commands used for binding the IPv6 address, MAC address, VLAN and the connected Port number of the Host together.

Chapter 81: IP Verify Source Configuration Commands

Provide information about the commands used for guarding the IP Source by filtering the IP

packets based on the IP-MAC Binding entries.

Chapter 82: IPv6 Verify Source Configuration Commands

Provide information about the commands used for guarding the IPv6 Source by filtering the IP packets based on the IP-MAC Binding entries.

Chapter 83: DHCPv4 Filter Configuration Commands

Provide information about the commands used for configuring the DHCPv4 Filter.

Chapter 84: DHCPv6 Filter Configuration Commands

Provide information about the commands used for configuring the DHCPv6 Filter.

Chapter 85: Dying Gasp Commands

Provide information about the commands used for configuring the Dying Gasp function.

Chapter 86: DoS Defend Commands

Provide information about the commands used for configuring the DoS (Denial of Service) Defend function.

Chapter 87: sFlow Commands (Only for Certain Devices)

Provide information about the commands used for configuring the sFlow (Sampled Flow) function.

Chapter 88: Ethernet OAM Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the Ethernet OAM (Operation, Administration, and Maintenance) function.

Chapter 89: MPLS Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the MPLS (Multiprotocol Label Switching) function.

Chapter 90: LDP Configuration Commands (Only for Certain Devices)

Provide information about the commands used for configuring the LDP (Label Distribution Protocol) function.

Chapter 91: DLDP Commands Configuration (Only for Certain Devices)

Provide information about the commands used for configuring the DLDP (Device Link Detection Protocol).

Chapter 92: SNMP Configuration Commands

Provide information about the commands used for configuring the SNMP (Simple Network Management Protocol) functions.

Chapter 93: NETCONF Commands Configuration (Only for Certain Devices)

Provide information about the commands used for configuring the NETCONF (Network Configuration Protocol).

Chapter 94: PoE Commands Configuration (Only for Certain Devices)

Provide information about the commands used for configuring PoE function.

Chapter 95: ARP Inspection Configuration Commands

Provide information about the commands used for protecting the switch from the ARP cheating or ARP Attack.

Chapter 96: ND Detection Configuration Commands

Provide information about the commands used for configuring ND detection.

Chapter 97: System Log Configuration Commands

Provide information about the commands used for configuring system log.

Chapter 1 Using the CLI

1.1 Accessing the CLI

You can log on to the switch and access the CLI by the following three methods:

1. Log on to the switch by the console port on the switch.
2. Log on to the switch remotely by a Telnet connection through an Ethernet port.
3. Log on to the switch remotely by an SSH connection through an Ethernet port.

1.1.1 Logon by a console port



Note: Console port is only available on certain devices.

■ Console Port

The switch has two console ports: an RJ-45 console port and a Micro-USB console port.

Console output is active on devices connected to both console ports, but console input is only active on one console port at a time.

The Micro-USB connector takes precedence over the RJ-45 connector. When the switch detects a valid connection on the Micro-USB console port, input from the RJ-45 console port is immediately disabled, and input from the Micro-USB console port is enabled. Removing the Micro-USB connection immediately reenables input from the RJ-45 console connection.

■ USB Console Driver

If you are using the USB port on the MAC OS X or Linux OS for console connection, there is no need to run a USB driver.

If you are using the switch's Micro-USB console port with the USB port of a Windows PC, a driver for the USB port is required. The USB driver is provided on the resource CD. Follow the InstallShield Wizard to accomplish the installation.

The TP-Link USB Console Driver supports the following Windows operating systems:

- 32-bit Windows XP SP3
- 64-bit Windows XP
- 32-bit Windows Vista
- 64-bit Windows Vista
- 32-bit Windows 7

- 64-bit Windows 7
- 32-bit Windows 8
- 64-bit Windows 8
- 32-bit Windows 8.1
- 64-bit Windows 8.1
- 32-bit Windows 10
- 64-bit Windows 10

After the TP-Link USB Console Driver is installed, the PC's USB port will act as RS-232 serial port when the PC's USB port is connected to the switch's Micro-USB console port. And the PC's USB port will act as standard USB port when the PC's USB port is unplugged from the switch.

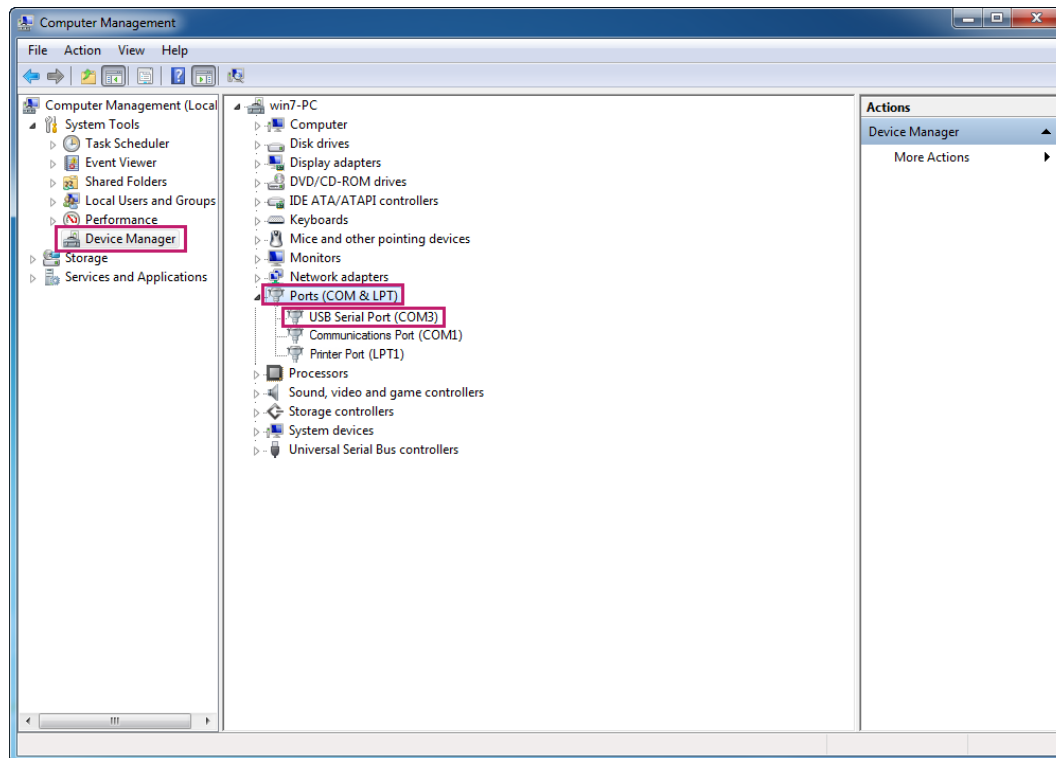
- Logon

Take the following steps to log on to the switch by the console port.

1. Connect the PCs or Terminals to the console port on the switch by the provided cable.
2. Start the terminal emulation program (such as the HyperTerminal, PuTTY, Tera Term) on the PC.
3. Specify the connection COM port in the terminal emulation program. If the Micro-USB Console port is used, you can view which port is assigned to the USB serial port in the following path:

Control Panel -> Hardware and Sound -> Device Manager -> Ports -> USB Serial Port.

Figure 1-1 USB Serial Port Number

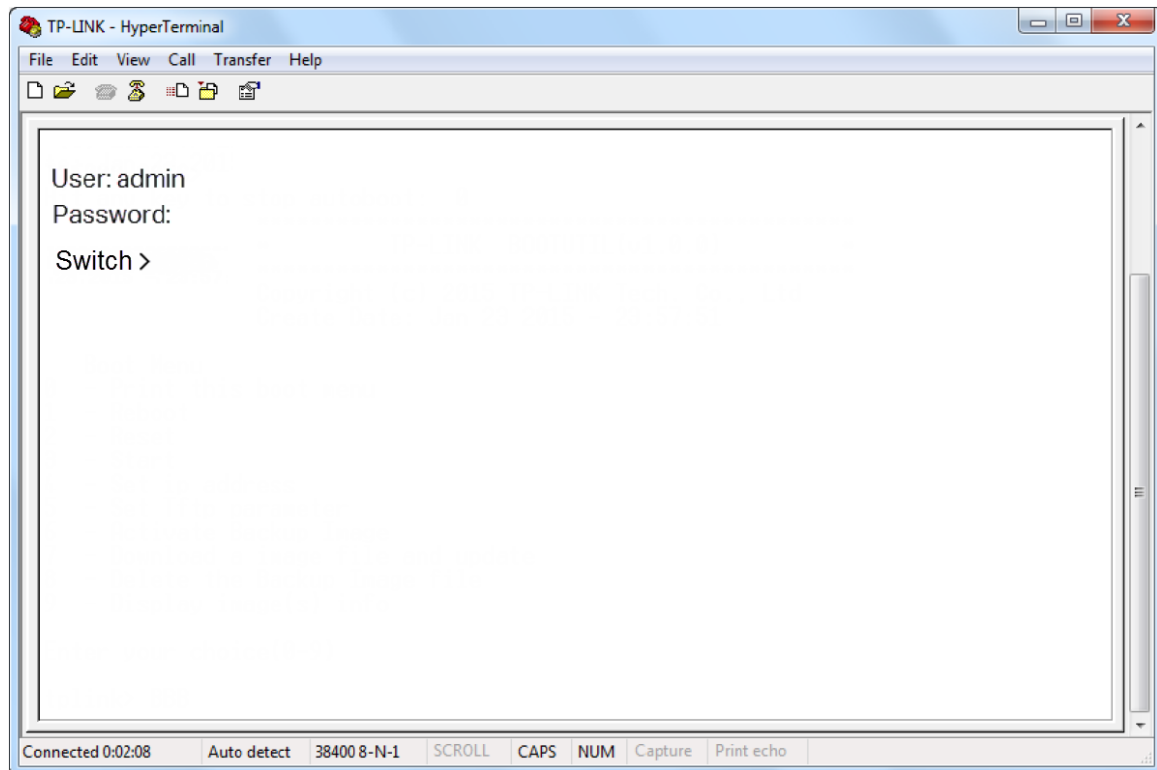


4. Configure the terminal emulation program or the terminal to use the following settings:

- Baud rate: 38400 bps
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

5. Type the Username and Password in the Hyper Terminal window. Press **Enter** in the main window and "Switch>" will appear indicating that you have successfully logged in to the switch and you can use the CLI now.

Figure 1-2 Log in to the Switch



Note: The first time you log in, change the password to better protect your network and devices.

1.1.2 Logon by Telnet

To log on to the switch by a Telnet connection, please take the following steps:

1. Click **Start** and type in **cmd** in the Search programs and files window and press the **Enter** button.

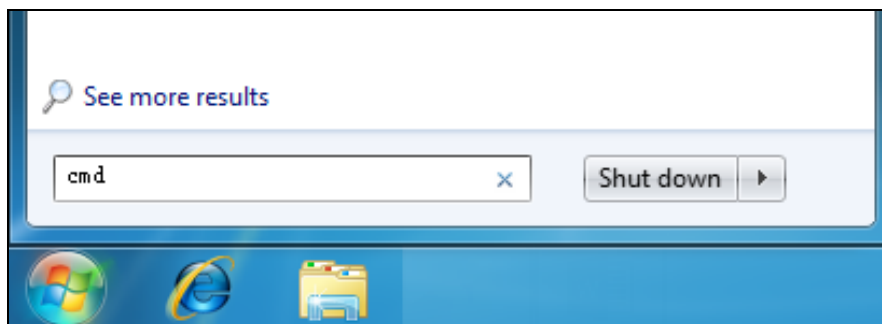


Figure 1-1 Run Window

2. Type in telnet 192.168.0.1 in the cmd window and press **Enter**.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>telnet 192.168.0.1
```

Figure 1-2 Type in the telnet command

3. Type in the login username and password. Press **Enter** and you will enter User EXEC Mode.

```
Telnet 192.168.0.1

***** User Access Login *****

User:admin
Password:

S6500-24GP4XF>
```

Figure 1-2 Log in the Switch

 **Note:** The first time you log in, change the password to better protect your network and devices.

4. Type in **enable** command and you will enter Privileged EXEC Mode. By default, no password is needed. Later you can set a password for users who want to access the Privileged EXEC Mode.

```
Telnet 192.168.0.1

***** User Access Login *****

User:admin
Password:

S6500-24GP4XF>enable

S6500-24GP4XF>
```

Figure 1-3 Enter into Priviledged EXEC Mode

1.1.3 Logon by SSH

To log on by SSH, a Putty client software is recommended. There are two authentication modes to set up an SSH connection:

Password Authentication Mode: It requires username and password.

Key Authentication Mode: It requires a public key for the switch and a private key for the SSH client software. You can generate the public key and the private key through Putty Key Generator.



Note:

1. Before SSH login, please follow the steps shown in Figure 1-4 to enable the SSH function through Telnet connection, which is enabled by default for some models.
2. The first time you log in, change the password to better protect your network and devices.

```
Telnet 192.168.0.1

***** User Access Login *****

User:admin
Password:

S6500-24G>4XF>enable
S6500-24G>4XF#config
S6500-24G>4XF(config)#ip ssh server
```

Figure 1-4 Enable SSH function

■ Password Authentication Mode

1. Open the software to log on to the interface of PuTTY. Enter the IP address of the switch into **Host Name** field; keep the default value 22 in the **Port** field; select **SSH** as the Connection type.

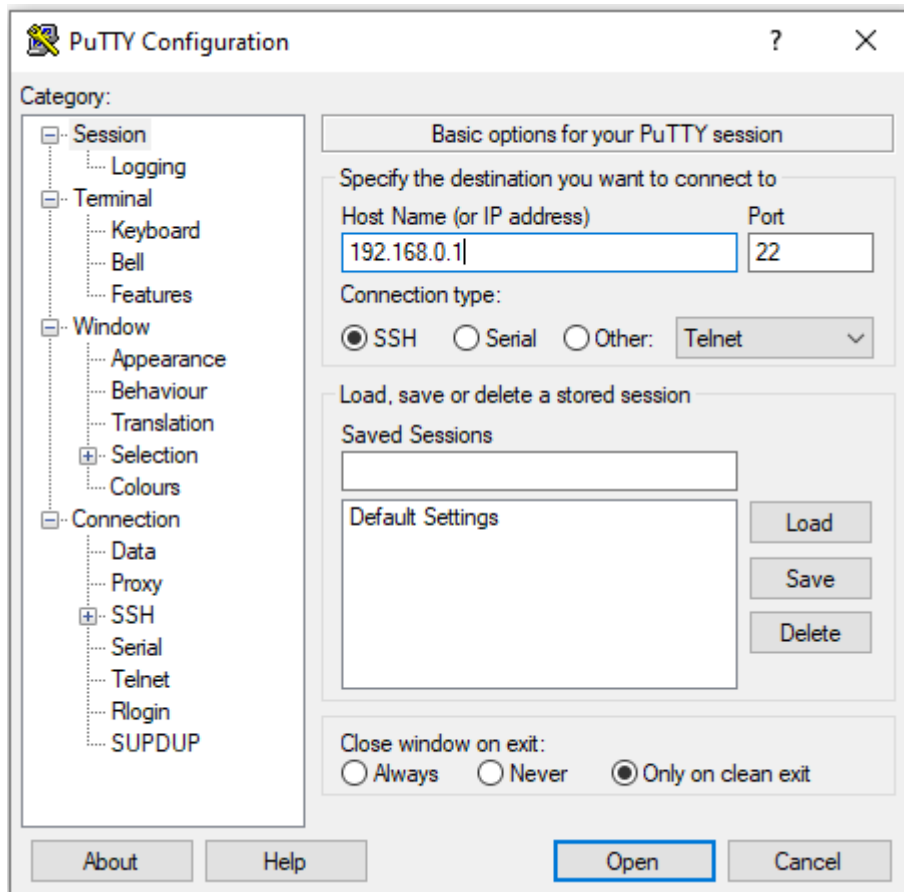


Figure 1-5 SSH Connection Config

2. Click the **Open** button in the above figure to log on to the switch. Enter the login user name and password to log on the switch, and then enter enable to enter Privileged EXEC Mode, so you can continue to configure the switch.

Figure 1-6 Log on the Switch

■ Key Authentication Mode

2. Select the key type and key length, and generate SSH key.

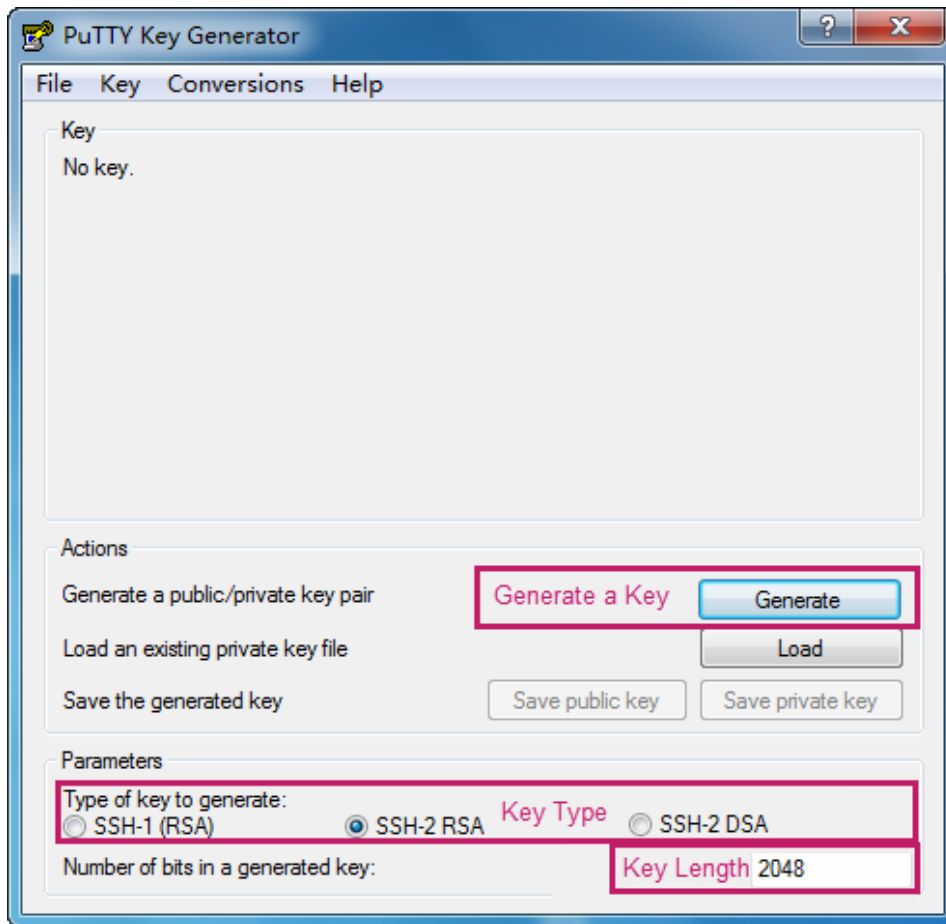


Figure 1-7 Generate SSH Key



Note:

1. The key length is in the range of 512 to 3072 bits.
2. During the key generation, randomly moving the mouse quickly can accelerate the key generation.

3. After the key is successfully generated, please save the public key and private key to a TFTP server.

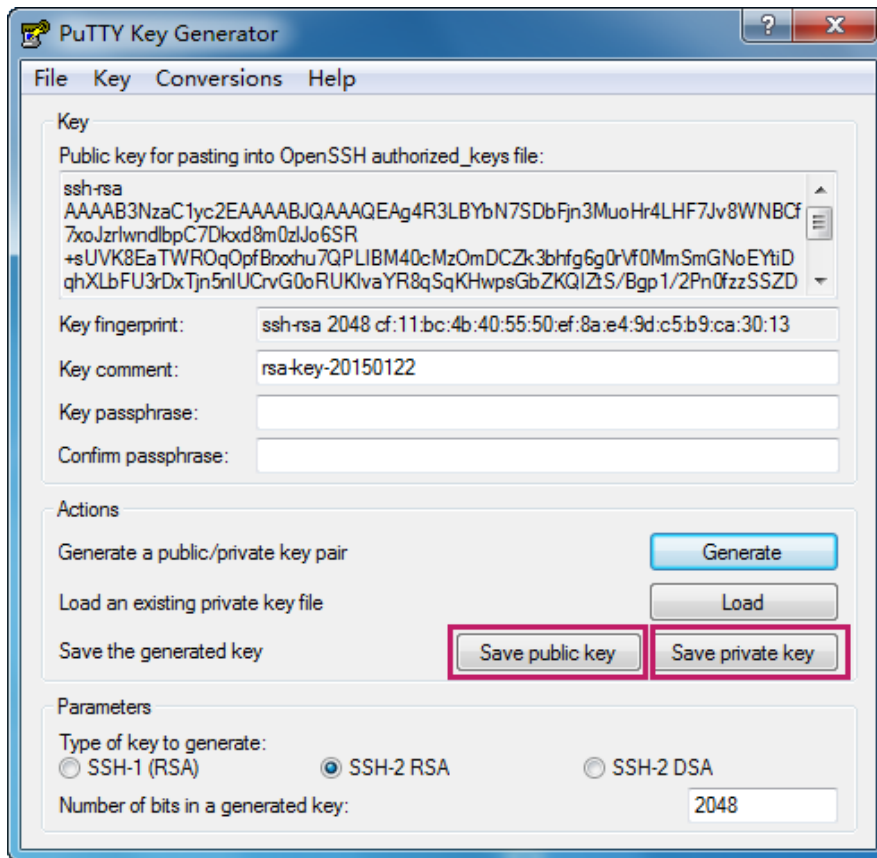


Figure 1-8 Save the Generated Key

4. Log on to the switch by Telnet and download the public key file from the TFTP server to the switch, as the following figure shows:



```
Telnet 192.168.0.1

***** User Access Login *****

User:admin
Password:

S6500-24GP4XF>enable
S6500-24GP4XF#config
S6500-24GP4XF (config)#ip ssh download v2 public ip-address 192.168.0.100
Start to download SSH key file.....
```

The screenshot shows a Telnet session on a switch. The user logs in as 'admin' and enters 'enable' to reach the privileged EXEC mode. Then, the user enters 'config' to enter the configuration mode. The command 'ip ssh download v2 public ip-address 192.168.0.100' is entered, which starts the download of the SSH key file. Red arrows point to 'v2' and '192.168.0.100' in the command, with labels 'The filename of the public key' and 'The IP address of the TFTP server' respectively.

Figure 1-9 Download the Public Key



Note:

1. The key type should accord with the type of the key file.
2. The SSH key downloading cannot be interrupted.

5. After the public key is downloaded, please log on to the interface of PuTTY and enter the IP address for login.

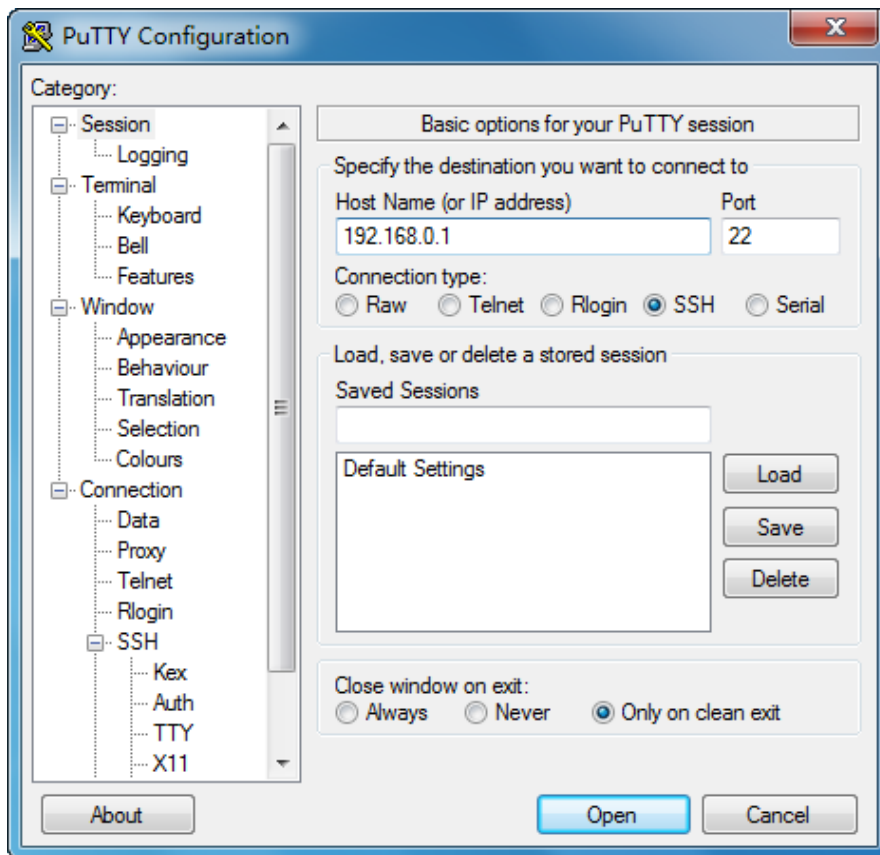


Figure 1-10 SSH Connection Config

- Click **Browse** to download the private key file to SSH client software and click **Open**.

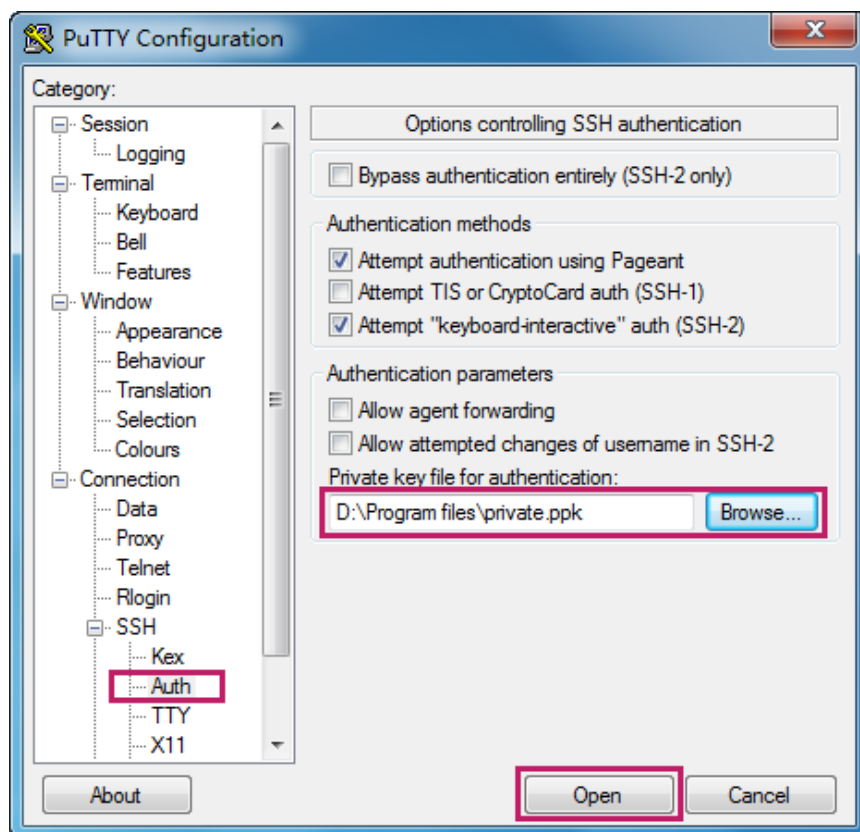


Figure 1-11 Download the Private Key

- After successful authentication, please enter the login user name. If you log on to the switch without entering password, it indicates that the key has been successfully downloaded.

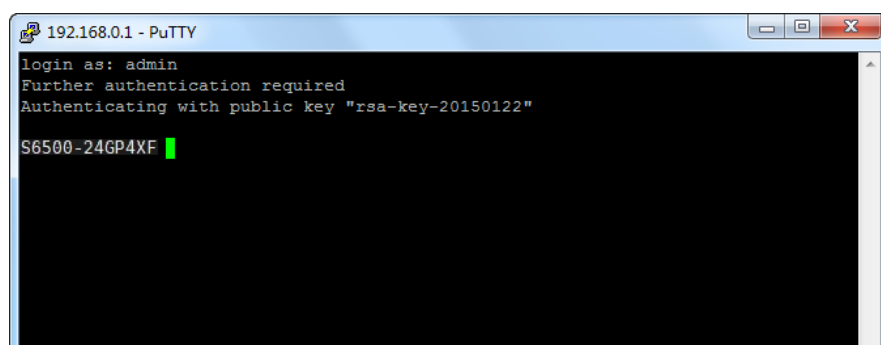


Figure 1-12 Log on the Switch

1.2 CLI Command Modes

The CLI is divided into different command modes: User EXEC Mode, Privileged EXEC Mode, Global Configuration Mode, Interface Configuration Mode and VLAN Configuration Mode.

Interface Configuration Mode can also be divided into Interface Ethernet, Interface link-aggregation and some other modes, which is shown as the following diagram.

The following table gives detailed information about the Accessing path, Prompt of each mode and how to exit the current mode and access the next mode.

Mode	Accessing Path	Prompt	Logout or Access the next mode
User EXEC Mode	Primary mode once it is connected with the switch.	Switch>	Use the exit command to disconnect the switch. Use the enable command to access Privileged EXEC mode.
Privileged EXEC Mode	Use the enable command to enter this mode from User EXEC mode.	Switch#	Enter the disable or the exit command to return to User EXEC mode. Enter configure command to access Global Configuration mode.
Global Configuration Mode	Use the configure command to enter this mode from Privileged EXEC mode.	Switch(config)#	Use the exit or the end command or press Ctrl+Z to return to Privileged EXEC mode. Use the interface gigabitEthernet port or interface range gigabitEthernet port-list command to access interface Configuration mode. Use the vlan vlan-list to access VLAN Configuration mode.
Interface Configuration Mode	Layer 2 Interface: Use the interface gigabitEthernet port , interface port-channel port-channel-id or interface range gigabitEthernet port-list command to enter this mode from Global Configuration mode.	Switch(config-if)# or Switch(config-if-range)#	Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit or the # command to return to Global Configuration mode. A port number must be specified in the interface command.

Mode	Accessing Path	Prompt	Logout or Access the next mode
Interface Configuration Mode	Layer 3 Interface: Use the no switchport command to enter Routed Port mode from Interface Configuration mode. Use the interface vlan <i>vlan-id</i> command to enter VLAN Interface mode from Global Configuration mode. Use the interface loopback <i>id</i> command to enter Loopback Interface mode from Global Configuration mode.	Switch (config-if)# or Switch(config-if-range)#	Use the switchport command to switch to the Layer 2 interface mode. Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit or the # command to return to Global Configuration mode.
Router Configuration Mode	Layer 3 Interface: Use the router rip or router ripng command to enter this mode from Global Configuration mode.	Switch (config-router)	Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit command or the # command to return to Global configuration mode.
VLAN Configuration Mode	Use the vlan <i>vlan-list</i> command to enter this mode from Global Configuration mode.	Switch (config-vlan)#	Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit command or the # command to return to Global configuration mode.



Note:

1. The user is automatically in User EXEC Mode after the connection between the PC and the switch is established by a Telnet/SSH connection.
2. Global Configuration Mode/Interface Configuration Mode/VLAN Configuration Mode is only available in standalone mode.
3. Each command mode has its own set of specific commands. To configure some

commands, you should access the corresponding command mode firstly.

- **Global Configuration Mode:** In this mode, global commands are provided, such as the Spanning Tree, Schedule Mode and so on.
 - **Interface Configuration Mode:** In this mode, users can configure one or several ports, different ports corresponds to different commands
 - a). Interface fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet: Configure parameters for a fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet port, such as Duplex-mode, flow control status.
 - b). Interface range fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet: Configure parameters for several fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet ports.
 - c). Interface link-aggregation: Configure parameters for a link-aggregation, such as broadcast storm.
 - d). Interface range link-aggregation: Configure parameters for multi-trunks.
 - e). Interface vlan: Configure parameters for the vlan-port.
 - **VLAN Configuration Mode:** In this mode, users can create a VLAN and add a specified port to the VLAN.
4. Some commands are global, that means they can be performed in all modes:
- **show:** Display all information of switch, for example: statistic information, port information, VLAN information.
 - **history:** Display the commands history.

1.3 Privilege Restrictions

This switch's security is divided into four privilege levels: User level, Power User level, Operator level and Admin level. You can define username and password pairs, and assign a specific privilege level to each pair. Different privilege levels have access to specified commands, which is illustrated in the **Privilege Requirement** in each command. For details about how to configure username and password pairs, please refer to [user name \(password\)](#) and [user name \(secret\)](#).

Users can enter Privileged EXEC mode from User EXEC mode by using the **enable** command. In default case, no password is needed. In Global Configuration Mode, you can configure password for Admin level by **enable password** command. Once password is configured, you are required to enter it to access Privileged EXEC mode.

1.4 Conventions

1.4.1 PoE Disclaimer

PoE budget calculations are based on laboratory testing. Actual PoE power budget is not guaranteed and will vary as a result of client limitations and environmental factors.

1.4.2 Format Conventions

The following conventions are used in this Guide:

- Items in square brackets [] are optional
- Items in braces { } are required
- Alternative items are grouped in braces and separated by vertical bars. For example:
speed {10 | 100 | 1000 }
- Bold indicates an unalterable keyword. For example: **show logging**
- Normal Font indicates a constant (several options are enumerated and only one can be selected). For example: **mode** {dynamic | static | permanent}
- Italic Font indicates a variable (an actual value must be assigned). For example: **bridge aging-time** *aging-time*

1.4.3 Special Characters

You should pay attentions to the description below if the variable is a character string:

- These six characters " < > , \ & cannot be input.

- If a blank is contained in a character string, single or double quotation marks should be used, for example 'hello world', "hello world", and the words in the quotation marks will be identified as a string. Otherwise, the words will be identified as several strings.

1.4.4 Parameter Format

Some parameters must be entered in special formats which are shown as follows:

- MAC address must be enter in the format of xx:xx:xx:xx:xx:xx.
- One or several values can be typed for a port-list or a vlan-list using comma to separate. Use a hyphen to designate a range of values, for instance, 1/0/1, 1/0/3-5, 1/0/7 indicates choosing port 1/0/1, 1/0/3, 1/0/4, 1/0/5, 1/0/7.

Chapter 2 Line Commands (Only for Certain Devices)



Note: Line Commands are only available on certain devices.

2.1 line

Description

The line command is used to enter the Line Configuration Mode and make related configurations for the desired user(s).

Syntax

```
line { console linenum | vty startlinenum endlinenum }
```

Parameter

linenum — The number of users allowed to login through console port. Its value is 0 in general, for the reason that console input is only active on one console port at a time.

startlinenum — The start serial number of the login user selected to configure the login mode and password, ranging from 0 to 15. 0 means the first login user number, 1 means the second, and the rest can be done on the same manner.

endlinenum — The end serial number of the login user selected to configure the login mode and password, ranging from 0 to 15. 0 means the first login user number, 1 means the second, and the rest can be done on the same manner.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the Console port configuration mode and configure the console port 0:

```
Switch(config)#line console 0
```

Enter the Virtual Terminal configuration mode so as to prepare further configurations such as password and login mode for virtual terminal 0 to 5:

```
Switch(config)#line vty 0 5
```

2.2 media-type rj45

Description

The media-type rj45 command is used to configure the console media type as RJ-45 for input. The switch has two console ports available — an RJ-45 console port and a micro-USB console port. Console input is active on only one console port at a time. By default, the micro-USB connector takes precedence over the RJ-45 connector, which means that, when both the RJ-45 console connection and micro-USB console connection are valid, input from the RJ-45 console is disabled, and input from the micro-USB console is enabled. To return to the default configuration, please use no media-type rj45 command.

Syntax

```
media-type rj45
```

```
no media-type rj45
```

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the RJ-45 console input:

```
Switch(config)# line console 0
```

```
Switch(config-line)# media-type rj45
```

Receive the micro-USB console input prior to the RJ-45 console input:

```
Switch(config)# line console 0
```

```
Switch(config-line)# no media-type rj45
```

Chapter 3 User Interface

3.1 enable

Description

The **enable** command is used to access Privileged EXEC Mode from User EXEC Mode.

Syntax

enable

Command Mode

User EXEC Mode

Privilege Requirement

None.

Example

If you have set the password to access Privileged EXEC Mode from User EXEC Mode:

```
Switch>enable
Enter password:
Switch#
```

3.2 service password-encryption

Description

The **service password-encryption** command is used to enable global password encryption. When passwords are configured or when the configuration is written to the configuration file, password fields are stored in encrypted form to prevent passwords from appearing in clear text in the configuration file. The **type** parameter specifies the password encryption algorithm (for example, aes-128). To disable this function, use the **no service password-encryption** command.

Syntax

service password-encryption [type <encryptType>]
no service password-encryption

Parameter

encryptType — Password encryption type. Currently supported: aes-128.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable global password encryption and specify the encryption type:

```
Switch(config)# service password-encryption type aes-128
```

3.3 enable password

Description

The **enable password** command is used to set or change the password for users to access Privileged EXEC Mode from User EXEC Mode. To remove the password, please use **no enable password** command. This command uses the symmetric encryption.

Syntax

enable password { [0] *password* | 6 *encrypted-password* | 7 *encrypted-password* }
no enable password

Parameter

0 — Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password — A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are !\$%()'*, -./[]_{}. By default, it is empty.

6 — Indicates a symmetric encrypted password with fixed length will follow (AES-128). *encrypted-password* — A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file.

After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

7 — Indicates a symmetric encrypted password with fixed length will follow.

encrypted-password — A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If the password you configured here is unencrypted and the global encryption function is enabled in [service password-encryption](#), the password in the configuration file will be displayed in the symmetric encrypted form.

If both the **enable password** and **enable secret** are defined, only the latest configured password will take effect.

Example

Set the super password as "admin" and unencrypted to access Privileged EXEC Mode from User EXEC Mode:

```
Switch(config)#enable password 0 admin
```

3.4 enable secret

Description

The **enable secret** command is used to set a secret password, which is using an MD5 encryption algorithm, for users to access Privileged EXEC Mode from User EXEC Mode. To return to the default configuration, please use **no enable secret** command. This command uses the MD5 encryption.

Syntax

```
enable secret { [ 0 ] password | 4 encrypted-password | 5  
encrypted-password | 8 encrypted-password | 9 encrypted-password }  
no enable secret
```

Parameter

0 — Specify the encryption type. 0 indicates that an unencrypted password will follow. the password will be encrypted by MD5. By default, the encryption type is 0.

password — A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are !\$%()'*, -./[]_{}. By default, it is empty.

4 — Indicates an SHA256 encrypted password with fixed length will follow.

5 — Indicates an MD5 encrypted password with fixed length will follow.

8 — Indicates a PBKDF2 encrypted password with fixed length will follow.

9 — Indicates a SCRYPT encrypted password with fixed length will follow.

encrypted-password — An/A SHA/MD5/SCRYPT/PBKDF2 encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **enable password** and **enable secret** are defined, only the latest configured password will take effect.

Example

Set the secret password as "admin" and unencrypted to access Privileged EXEC Mode from User EXEC Mode. The password will be displayed in the encrypted form.

```
Switch(config)#enable secret 0 admin
```

3.5 configure

Description

The **configure** command is used to access Global Configuration Mode from Privileged EXEC Mode.

Syntax

configure

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Access Global Configuration Mode from Privileged EXEC Mode:

```
Switch# configure
Switch (config)#
```

3.6 key config-key general key

Description

The **key config-key general key** command is used to configure a private configuration key for general use. This key is used as the source material for deriving encryption keys for features such as configuration file encryption and AES-based password encryption (for example, password-encryption type 6). To remove the configured general key, please use **no key config-key general key** command. This command uses the MD5 encryption.

Syntax

key config-key general key *key-string*
no key config-key general

Parameter

key-string — User defined key, whose length should be 8-63.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

After the general key is configured, if service password-encryption type 6 is enabled, the system will use the keys derived from this general key for AES encryption.

Example

Configure a general configuration key:

```
Switch(config)#key config-key general key mykey12345
```

3.7 exit

Description

The **exit** command is used to return to the previous Mode from the current Mode.

Syntax

exit

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Return to Global Configuration Mode from Interface Configuration Mode, and then return to Privileged EXEC Mode:

```
Switch (config-if)# exit
Switch (config)#exit
Switch#
```

3.8 end

Description

The **end** command is used to return to Privileged EXEC Mode.

Syntax

end

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Return to Privileged EXEC Mode from Interface Configuration Mode:

```
Switch (config-if)#end
Switch #
```

3.9 clipaging

Description

The **clipaging** command is used to enable the pause function for the screen display. If you want to display all the related information of the switch at once when using the show command, please use **no clipaging** command.

Syntax

```
clipaging
no clipaging
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Disable the pause function for the screen display:

```
Switch (config)#no clipaging
```

3.10 history

Description

The **history** command is used to show the latest 20 commands you entered in the current mode since the switch is powered.

Syntax

```
history
```

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

None.

Example

Show the commands you have entered in the current mode:

```
Switch (config)# history  
1 history
```

3.11 history clear

Description

The **history clear** command is used to clear the commands you have entered in the current mode; therefore, these commands will not be shown next time you use the **history** command.

Syntax

history clear

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the commands you have entered in the current mode:

```
Switch (config)#history clear
```

Chapter 4 User Management Commands

User Management commands are used to manage the user's logging information by Web, Telnet or SSH, so as to protect the settings of the switch from being randomly changed.

4.1 user name (password)

Description

The **user name** command is used to add a new user or modify the existed users' information. To delete the existed users, please use **no user name** command. This command uses the symmetric encryption.

Syntax

```
user name name [ privilege admin | operator | power_user | user ] password
{ [ 0 ] password | 6 encrypted-password | 7 encrypted-password }
no user name name
```

Parameter

name —— Type a name for users' login. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.

admin | operator | power_user | user —— Access level. "admin" means that you can edit, modify and view all the settings of different functions. "operator" means that you can edit, modify and view most of the settings of different functions. "power-user" means that you can edit, modify and view some of the settings of different functions. "user" means that you can only view some of the settings of different functions without the right to edit or modify. It is "admin" by default. For more details about privilege restrictions, please refer to the **Privilege Requirement** part in each command.

0 —— Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password —— Users' login password, a string with 6–31 alphanumeric characters (case-sensitive) and symbols. No spaces are allowed.

6 —— Indicates a symmetric encrypted password with fixed length will follow (AES-128). *encrypted-password* —— A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file.

After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

7 — Indicates a symmetric encrypted password with fixed length will follow.

encrypted-password — A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If the password you configured here is unencrypted and the global encryption function is enabled in [service password-encryption](#), the password in the configuration file will be displayed in the symmetric encrypted form.

If both the **user name (password)** and **user name (secret)** are defined, only the latest configured password will take effect.

Example

Add and enable a new admin user named "tplink", of which the password is "admin" and unencrypted:

```
Switch(config)#user name tplink privilege admin password 0 admin
```

4.2 user name (algorithm-type)

Description

The **user name** command is used to add a new user or modify the existed users' information. To delete the existed users, please use **no user name** command. This command uses the symmetric encryption.

Syntax

```
user name name [ privilege admin | operator | power_user | user ]  
algorithm-type { md5 | md5_sha256 | sha256 | scrypt } secret password  
no user name name
```

Parameter

name——Type a name for users' login. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.

admin | operator | power_user | user —— Access level. "admin" means that you can edit, modify and view all the settings of different functions. "operator" means that you can edit, modify and view most of the settings of different functions. "power-user" means that you can edit, modify and view some of the settings of different functions. "user" means that you can only view some of the settings of different functions without the right to edit or modify. It is "admin" by default.

md5 | md5_sha256 | sha256 | scrypt —— algorithm-type. Specify the algorithm to use for hashing the plaintext secret for the user. md5: Encodes the password using the MD5 algorithm; md5_sha256: Encodes the password using the SHA256 hashing algorithm; sha256: Encodes the password using the PBKDF2 hashing algorithm; scrypt: Encodes the password using the SCRYPT hashing algorithm.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If the password you configured here is unencrypted and the global encryption function is enabled in [service password-encryption](#), the password in the configuration file will be displayed in the symmetric encrypted form.

If both the **user name (password)** and **user name (secret)** are defined, only the latest configured password will take effect.

Example

Create an admin user named tplink and set the password to dsaoM#3210, which is encrypted in SCRYPT mode:

```
Switch (config)# user name tplink privilege admin algorithm-type scrypt
secret dsaoM#3210
```

4.3 user name (secret)

Description

The **user name** command is used to add a new user or modify the existed users' information. To delete the existed users, please use **no user name** command. This command uses the MD5 encryption.

Syntax

```
user name name [privilege admin | operator | power_user | user] secret { [ 0 ]  
password | 4 encrypted-password | 5 encrypted-password | 8  
encrypted-password | 9 encrypted-password }  
  
no user name name
```

Parameter

name —— Type a name for users' login. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.

admin | *operator* | *power_user* | *user* —— Access level. "admin" means that you can edit, modify and view all the settings of different functions. "operator" means that you can edit, modify and view most of the settings of different functions. "power-user" means that you can edit, modify and view some of the settings of different functions. "user" means that you can only view some of the settings of different functions without the right to edit or modify. It is "admin" by default.

0 —— Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password —— Users' login password, a string with 6–31 alphanumeric characters (case-sensitive) and symbols. No spaces are allowed.

4 —— Indicates an SHA256 encrypted password with fixed length will follow.

5 —— Indicates an MD5 encrypted password with fixed length will follow.

8 —— Indicates an PBKDF2 encrypted password with fixed length will follow.

9 —— Indicates a SCRYPT encrypted password with fixed length will follow.

encrypted-password —— An/A SHA/MD5/SCRYPT/PBKDF2 encrypted password with fixed length, which you can copy from another switch's configuration file.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **user name (password)** and **user name (secret)** are defined, only the latest configured password will take effect.

Example

Add and enable a new admin user named "tplink", of which the password is "admin". The password will be displayed in the encrypted form.

```
Switch (config)#user name tplink privilege admin secret 0 admin
```

4.4 service password-recovery



Note: This command is only available on certain devices.

Description

The **service password-recovery** command is used to enable the password-recovery feature. To disable the password-recovery feature, please use **no service password-recovery** command.

With password-recovery enabled, you can connect to the switch's console port and delete all your previous set accounts. You need to set a new password before logging into the switch after its startup.

Syntax

service password-recovery

no service password-recovery

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the switch's password-recovery feature:

```
Switch(config)# service password-recovery
```

4.5 service passwd-complexity



Note: This command is only available on certain devices.

Description

The **service passwd-complexity** command is used to enable the global switch of password complexity, which is enabled by default. If the switch is disabled, when the user sets the password, only the password length entered by the user is checked to see if it is between 6 and 64 characters. Other complexity parameters are invalid, and the function of limiting the number of login attempts is disabled. If the switch is enabled, when the user sets the password, the password will be checked according to the parameters set by the user. For specific user settings, see the subsequent command description. At the same time, the login limit will take effect according to the user configuration. To disable this function, please use **no service passwd-complexity** command.

Syntax

service passwd-complexity

no service passwd-complexity

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable global password complexity:

```
Switch(config)# service passwd-complexity
```

4.6 service passwd-complexity min-length



Note: This command is only available on certain devices.

Description

The **service passwd-complexity min-length** command is used to configure the minimum password length, which is 10 by default.

Syntax

service passwd-complexity min-length *min-length*

Parameter

min-length—— minimum password length, the value range is 9~64, the default value is 10.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Set minimum length to 12:

```
Switch(config)#service passwd-complexity min-length 12
```

4.7 service passwd-complexity min-class-number



Note: This command is only available on certain devices.

Description

The **service passwd-complexity min-class-number** command is used to configure the minimum number of character classes (digits, lowercase, uppercase, special characters) required in passwords.

Syntax

service passwd-complexity min-class-number *min-class-number*

Parameter

min-class-number — The minimum character class contained in the password, the value range is 0~4, the default value is 3; if it is set to 0, it means no restriction.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Require all 4 character classes:

```
Switch(config)# service passwd-complexity min-class-number 4
```

4.8 service passwd-complexity max-repeat-number



Note: This command is only available on certain devices.

Description

The **service passwd-complexity max-repeat-number** command is used to configure the maximum allowed consecutive identical characters.

Syntax

service passwd-complexity max-repeat-number *max-repeat-number*

Parameter

max-repeat-number — The maximum number of times the same character can be repeated in a password. The value range is 0 to 16. The default value is 1, which means that the password is not allowed to contain consecutive repeated characters. If it is set to 0, it means there is no limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Allow up to 2 consecutive repeats:

```
Switch(config)# service passwd-complexity max-repeat-number 2
```

4.9 service passwd-complexity max-keyboard-consecutive -num



Note: This command is only available on certain devices.

Description

The **service passwd-complexity max-keyboard-consecutive-num** command is used to configure the maximum consecutive keyboard-aligned characters (case-insensitive, excludes special characters).

Syntax

```
service passwd-complexity max-keyboard-consecutive-num  
max-keyboard-consecutive-num
```

Parameter

max-keyboard-consecutive-num — The maximum number of characters that cannot be included in the password from left to right in the main keyboard area (excluding special characters). Letters are not case sensitive. The value range is 0 to 10. The default value is 4, which means that the password is not allowed to contain consecutive characters such as aSdf and 1234 in the main keyboard area. If it is set to 0, it means there is no limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Block sequences longer than 3 characters (e.g., 123, Asd):

```
Switch(config)#service passwd-complexity  
max-keyboard-consecutive-num 3
```

4.10 service passwd-complexity not-current



Note: This command is only available on certain devices.

Description

The **service passwd-complexity not-current** command is used to configure that a new password cannot be set as the currently active password. When enabled, users cannot configure a new password identical to their current active password. When disabled, users are allowed to set a new password that matches their currently active password. To disable the restriction that prevents newly set passwords from being the same as the current password, use the **no service passwd-complexity not-current** command.

Syntax

service passwd-complexity not-current

no service passwd-complexity not-current

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable check to block reuse of current password:

```
Switch(config)# service passwd-complexity not-current
```

4.11 service passwd-complexity not-username



Note: This command is only available on certain devices.

Description

The **service passwd-complexity not-username** command is used to configure the policy that newly set passwords cannot be the username or its variants (including reversed or case-changed versions). When enabled, newly configured user passwords cannot match the username or its variants; when disabled, users may configure passwords identical to the username or its variants. To disable the restriction preventing new passwords from being username variants, use the **no service passwd-complexity not-username** command.

Syntax

service passwd-complexity not-username

no service passwd-complexity not-username

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Block passwords matching username variants (e.g., Admin@123 → ADMIN@123):

```
Switch(config)# service passwd-complexity not-username
```

4.12 service passwd-complexity not-manufacturer-name



Note: This command is only available on certain devices.

Description

The **service passwd-complexity not-manufacturer-name** command is used to configure that new passwords cannot be set as the manufacturer name or its variants (including reversed or case-altered forms, where manufacturer names include tp-link and tp-link). When enabled, users cannot configure new

passwords using manufacturer names or their variants; when disabled, users are permitted to use manufacturer names and their variants as new passwords. To disable the restriction on using manufacturer names and their variants as new passwords, use the **no service passwd-complexity not-manufacturer-name** command.

Syntax

service passwd-complexity not-manufacturer-name
no service passwd-complexity not-manufacturer-name

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Block manufacturer name variants:

```
Switch(config)# service passwd-complexity not-manufacturer-name
```

4.13 service passwd-cycle



Note: This command is only available on certain devices.

Description

The **service passwd-cycle** command is used to set the time period during which previously used old passwords cannot be reused, determining the cycle before a password becomes available for reuse. If the switch is reset, this configuration will revert to default settings and previous configurations will become invalid.

Syntax

service passwd-cycle *days*

Parameter

days — The time that a used password can be used again, in days, with a value range of 0-356, and a default value of 90, which means that if an old

password is used and a new password is set, the old password cannot be used again within 90 days. 0 means no limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Set reuse cooldown to 120 days:

```
Switch(config)# service passwd-cycle 120
```

4.14 show user account-list

Description

The **show user account-list** command is used to display the information of the current users.

Syntax

show user account-list

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the current users:

```
Switch (config)# show user account-list
```

4.15 show user configuration

Description

The **show user configuration** command is used to display the security configuration information of the users, including access-control, max-number and the idle-timeout, etc.

Syntax

show user configuration

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration information of the users:

```
Switch (config)# show user configuration
```

4.16 show client

Description

The **show client** command is used to display the detailed information about all clients.

Syntax

show client

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the detailed information about all clients:

```
Switch (config)# show client
```

Chapter 5 System Configuration Commands

System Commands can be used to configure the System information and System IP, reboot and reset the switch, upgrade the switch system and other operations.

5.1 system-time manual

Description

The **system-time manual** command is used to configure the system time manually.

Syntax

system-time manual *time*

Parameter

time — Set the date and time manually, MM/DD/YYYY-HH:MM:SS. The valid value of the year ranges from 2000 to 2037.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system mode as manual, and the time is 12/20/2010 17:30:35

```
Switch (config)# system-time manual 12/20/2010-17:30:35
```

5.2 system-time ntp

Description

The **system-time ntp** command is used to configure the time zone and the IP address or hostname for the NTP Server. The switch will get UTC automatically if it has connected to an NTP Server.

Syntax

system-time ntp { *timezone* } { *ntp-server* } { *backup-ntp-server* }
{ *fetching-rate* }

system-time ntp vrf *vrf-name*

Parameter

timezone — Your local time-zone, and it ranges from UTC-12:00 to UTC+13:00.

The detailed information that each time-zone means are displayed as follow:

UTC-12:00 — TimeZone for International Date Line West.

UTC-11:00 — TimeZone for Coordinated Universal Time-11.

UTC-10:00 — TimeZone for Hawaii.

UTC-09:00 — TimeZone for Alaska.

UTC-08:00 — TimeZone for Pacific Time(US Canada).

UTC-07:00 — TimeZone for Mountain Time(US Canada).

UTC-06:00 — TimeZone for Central Time(US Canada).

UTC-05:00 — TimeZone for Eastern Time(US Canada).

UTC-04:30 — TimeZone for Caracas.

UTC-04:00 — TimeZone for Atlantic Time(Canada).

UTC-03:30 — TimeZone for Newfoundland.

UTC-03:00 — TimeZone for Buenos Aires, Salvador, Brasilia.

UTC-02:00 — TimeZone for Mid-Atlantic.

UTC-01:00 — TimeZone for Azores, Cape Verde Is.

UTC — TimeZone for Dublin, Edinburgh, Lisbon, London.

UTC+01:00 — TimeZone for Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna.

UTC+02:00 — TimeZone for Cairo, Athens, Bucharest, Amman, Beirut, Jerusalem.

UTC+03:00 — TimeZone for Kuwait, Riyadh, Baghdad.

UTC+03:30 — TimeZone for Tehran.

UTC+04:00 — TimeZone for Moscow, St.Petersburg, Volgograd, Tbilisi, Port Louis.

UTC+04:30 — TimeZone for Kabul.

UTC+05:00 — TimeZone for Islamabad, Karachi, Tashkent.

UTC+05:30 — TimeZone for Chennai, Kolkata, Mumbai, New Delhi.

UTC+05:45 — TimeZone for Kathmandu.

UTC+06:00 — TimeZone for Dhaka, Astana, Ekaterinburg.

UTC+06:30 — TimeZone for Yangon (Rangoon).

UTC+07:00 — TimeZone for Novosibirsk, Bangkok, Hanoi, Jakarta.

UTC+08:00 — TimeZone for Beijing, Chongqing, Hong Kong, Urumqi, Singapore.

UTC+09:00 — TimeZone for Seoul, Irkutsk, Osaka, Sapporo, Tokyo.

UTC+09:30 — TimeZone for Darwin, Adelaide.

UTC+10:00 — TimeZone for Canberra, Melbourne, Sydney, Brisbane.

UTC+11:00 — TimeZone for Solomon Is., New Caledonia, Vladivostok.

UTC+12:00 — TimeZone for Fiji, Magadan, Auckland, Wellington.

UTC+13:00 — TimeZone for Nuku'alofa, Samoa.

ntp-server — The IP address or domain name for the Primary NTP Server.

backup-ntp-server — The IP address or domain name for the Secondary NTP Server.

fetching-rate — Specify the rate fetching time from NTP server.

vrf-name — VRF instance name (1–15 characters).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system time mode as NTP, the time zone is UTC-12:00, the primary NTP server is 133.100.9.2 and the secondary NTP server is 139.78.100.163, the fetching-rate is 11 hours, and specify the VRF instance named vrf1:

```
Switch(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11
```

```
Switch (config)# system-time ntp vrf vrf1
```

5.3 system-time dst predefined

Description

The **system-time dst predefined** command is used to select a daylight saving time configuration from the predefined mode. The configuration can be used recurrently. To disable DST function, please use **no system-time dst** command.

Syntax

system-time dst predefined [USA /Australia | Europe | New-Zealand]

no system-time dst

Parameter

USA /Australia | Europe | New-Zealand — The mode of daylight saving time. There are 4 options which are USA, Australia, Europe and New-Zealand respectively. The default value is Europe.

Following are the time ranges of each option:

USA — Second Sunday in March, 02:00 – First Sunday in November, 02:00.

Australia — First Sunday in October, 02:00 – First Sunday in April, 03:00.
Europe — Last Sunday in March, 01:00 – Last Sunday in October, 01:00.
New Zealand — Last Sunday in September, 02:00 – First Sunday in April, 03:00.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the daylight saving time as USA standard:

```
Switch(config)#system-time dst predefined USA
```

5.4 system-time dst date

Description

The **system-time dst date** command is used to configure the one-off daylight saving time. The start date is in the current year by default. The time range of the daylight saving time must shorter than one year, but you can configure it spanning years. To disable DST function, please use **no system-time dst** command.

Syntax

system-time dst date {*smonth*} {*sday*} {*stime*} {*syear*} {*emonth*} {*eday*}
{*etime*} {*eyear*} [*offset*]

no system-time dst

Parameter

smonth — The start month of the daylight saving time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

sday — The start day of the daylight saving time, ranging from 1 to 31. Here you should show special attention to February and the differences between a solar month and a lunar month.

stime — The start moment of the daylight saving time, HH:MM.

syear — The start year of the daylight saving time.

emonth — The end month of the daylight saving time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

eday—— The end day of the daylight saving time, ranging from q to 31. Here you should show special attention to February and the differences between a solar month and a lunar month.

etime—— The end moment of the daylight saving time, HH:MM.

eyear—— The end year of the daylight saving time.

offset—— The number of minutes to add during the daylight saving time. It is 60 minutes by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the daylight saving time from zero clock, Apr 1st to zero clock Oct 1st and the offset is 30 minutes in 2015:

```
Switch(config)# system-time dst date Apr 1 00:00 2015 Oct 1 00:00 2015
30
```

5.5 system-time dst recurring

Description

The **system-time dst recurring** command is used to configure the recurring daylight saving time. It can be configured spanning years. To disable DST function, please use **no system-time dst** command.

Syntax

system-time dst recurring {*sweek*} {*sday*} {*smonth*} {*stime*} {*eweeek*} {*eday*}
{*emonth*} {*etime*} [*offset*]

no system-time dst

Parameter

sweek——The start week of the daylight saving time. There are 5 values showing as follows: first, second, third, fourth, last.

sday—— The start day of the daylight saving time. There are 7 values showing as follows: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

smonth—— The start month of the daylight saving time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

stime—— The start moment of the daylight saving time, HH:MM.

eweeek——The end week of the daylight saving time. There are 5 values showing as follows: first, second, third, fourth, last.

eday—— The end day of the daylight saving time. There are 5 values showing as follows: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

emonth—— The end month of the daylight saving time. There are 12 values showing as following: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

etime—— The end moment of the daylight saving time, HH:MM.

offset—— The number of minutes to add during the daylight saving time. It is 60 minutes by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the daylight saving time from 2:00am, the first Sunday of May to 2:00am, the last Sunday of Oct and the offset is 45 minutes:

```
Switch(config)# system-time dst recurring first Sun May 02:00 last Sun Oct
02:00 45
```

5.6 hostname

Description

The **hostname** command is used to configure the system name. To clear the system name information, please use **no hostname** command.

Syntax

hostname [*hostname*]

no hostname

Parameter

hostname—— System Name. The length of the name ranges from 1 to 32 characters. By default, it is the device name, for example "SG6654XHP".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system name as TP-Link

```
Switch(config)# hostname TP-Link
```

5.7 location

Description

The **location** command is used to configure the system location. To clear the system location information, please use **no location** command.

Syntax

location [*location*]

no location

Parameter

location—— Device Location. It consists of 32 characters at most.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system location as Hong Kong:

```
Switch(config)# location Hong Kong
```

5.8 contact-info

Description

The **contact-info** command is used to configure the system contact information. To clear the system contact information, please use **no contact-info** command.

Syntax

contact-info [*contact_info*]

no contact-info

Parameter

contact_info—— Contact Information. It consists of 32 characters at most. It is "www.omadanetworks.com" by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system contact information as www.tp-link.com:

```
Switch(config)# contact-info www.tp-link.com
```

5.9 led



Note: This command is only available on certain devices.

Description

The **led** command is used to control the LEDs.

Syntax

led {on | off}

Parameter

on | off—— The LEDs are configured as on or off. By default, they are on.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the LED as off:

```
Switch(config)# led off
```

5.10 ip management-vlan

Description

The **ip management-vlan** command is used to switch the management VLAN in standalone mode (non-Controller adoption mode). By default, the management VLAN is VLAN 1. After switching the management VLAN, the Controller retains the device-side configurations related to this VLAN, and subsequent communication between the device and the Controller also uses this VLAN (requires Controller version support). Before switching the management VLAN, ensure proper configuration of the VLAN, ports, VLAN interface (VLAN IF), etc., to guarantee normal Controller adoption and management of the device. To restore the management VLAN to the default, please use the **no ip management-vlan** command.

Syntax

ip management-vlan *vlan-id*

no ip management-vlan

Parameter

vlan-id—— The VLAN ID of the management VLAN, ranging from 1 to 4090 (since the Controller only supports VLAN IDs 1–4090).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the switch's management VLAN as VLAN 100 via CLI commands.

(1) Create VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan)# name mgmt-vlan
switch(config-vlan)# exit
```

(2) Add the port to the management VLAN:

```
switch(config)# interface gigabitEthernet 1/0/1
switch(config-if)# switchport general allowed vlan 100 untagged
```

```
switch(config-if)# switchport pvid 100
```

```
switch(config-if)# exit
```

(3) Configure the VLAN 100 interface:

```
switch(config)# interface vlan 100
```

Configure a static IP:

```
switch(config-if)# ip address 192.168.0.1 255.255.255.0
```

Or obtain an IP address via DHCP:

```
switch(config-if)# ip address-alloc dhcp
```

```
switch(config-if)# exit
```

(4) Switch the management VLAN to VLAN 100:

```
switch(config)# ip management-vlan 100
```

(5) Verify the configuration using show running-config.

5.11 ip address

Description

The **ip address** command is used to configure the IP address and IP subnet mask for the specified interface manually. The interface type includes: routed port, port-channel interface, loopback interface and VLAN interface.

Syntax

```
ip address { ip-addr } { mask } [ secondary ]
```

```
no ip address [ ip-addr ] [ mask ]
```

Parameter

ip-addr — The IP address of the Layer 3 interface.

mask — The subnet mask of the Layer 3 interface.

secondary — Specify the interface's secondary IP address. If this parameter is omitted here, the configured IP address is the interface's primary address.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the VLAN interface 2 with the primary IP address as 192.168.1.1/24 and secondary IP address as 192.168.2.1/24:

```
Switch (config)# interface vlan 2
Switch (config-if)# ip address 192.168.1.1 255.255.255.0
Switch (config-if)# ip address 192.168.2.1 255.255.255.0 secondary
```

5.12 ip address-alloc

Description

The **IP address-alloc** command is used to enable the DHCP Client function or the BOOTP Protocol. When this function is enabled, the specified interface will obtain IP from DHCP Server or BOOTP server. To disable the IP obtaining function on the specified interface, please use the **no ip address** command. This command applies to the routed port, the port-channel interface and the VLAN interface.

Syntax

```
ip address-alloc { dhcp | bootp }
no ip address
```

Parameter

dhcp — Specify the Layer 3 interface to obtain IP address from the DHCP Server.

bootp — Specify the Layer 3 interface to obtain IP address from the BOOTP Server.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Client function on the Layer 3 routed port 1/0/1:

```
Switch (config)# interface gigabitEthernet 1/0/1
```

```
Switch (config-if)# no switchport
```

```
Switch (config-if)# ip address-alloc dhcp
```

Disable the IP address obtaining function on the VLAN interface 2:

```
Switch (config)# interface vlan 2
```

```
Switch (config-if)# no ip address
```

5.13 controller cloud-based



Note: This command is only available on certain devices

Description

The **controller cloud-based** command is used to enable Cloud-Based Controller management. When this feature is enabled, you can further add your devices to your Omada Cloud-Based Controller. To disable the feature, use the **no controller cloud-based** command.

Syntax

controller cloud-based

no controller cloud-based

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

5.14 controller inform-url



Note: This command is only available on certain devices

Description

If your switch and Omada SDN Controller are not located on the same subnet, the **controller inform-url** command is used to inform the switch of the controller's URL/IP address. To disable the feature, use the **no controller inform-url** command.

Syntax

```
controller inform-url { controller-url | controller-ip }  
no controller inform-url
```

Parameter

controller-url —— Specify the URL of Omada SDN Controller.

controller-ip —— Specify the IP address of Omada SDN Controller.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Inform the switch of the controller whose IP address is 192.168.1.1:

```
Switch (config)# controller inform-url 192.168.1.1
```

5.15 controller discover



Note: This command is only available on certain devices

Description

The **controller discover** command is used to control whether the device sends out controller discovery broadcast packets. By default, the device sends controller discovery broadcast packets. When the switch is turned off, the device will no longer periodically send broadcast discovery packets, and controllers will be unable to discover the device. However, this setting does not affect the sending of unicast discovery packets. If a controller's address is explicitly specified, that controller can still discover the device. To remove this configuration, please use the **no controller discover** command.

Syntax

controller discover

no controller discover

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the device from sending broadcast discovery packets to controllers:

```
Switch (config)# no controller discover
```

5.16 controller dns-adoption



Note: This command is only available on certain devices

Description

The **controller dns-adoption** command is used to enable the DNS-ADOPTION function. The DNS-ADOPTION function serves as a supplementary method for users to connect to the controller: Users configure the domain name on the DNS server to point to the IP address of the corresponding Omada controller, allowing users to establish a connection to the controller by accessing this domain name. After enabling the DNS-ADOPTION function, the device periodically sends DNS requests for the domain name "omada". If disabled, it will no longer send such DNS requests. This function is enabled by default. To disable this function, please use the **no controller dns-adoption** command.

Syntax

controller dns-adoption

no controller dns-adoption

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DNS-ADOPTION function:

```
Switch (config)# controller dns-adoption
```

5.17 reset

Description

The **reset** command is used to reset the switch's software. After resetting, all configuration of the switch will restore to the factory defaults and your current settings will be lost.

Syntax

```
reset [ except-ip ]
```

Parameter

except-ip — Maintain the IP address when resetting the switch.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Reset all settings of the switch except its IP address:

```
Switch # reset except-ip
```

5.18 service reset-disable

Description

The **service reset-disable** command is used to disable the reset function of the console port or reset button. To enable the reset function, use **no service reset-disable** command. By default, the reset function is enabled.

Syntax

service reset-disable

no service reset-disable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Disable the reset function of console port or reset button:

```
Switch (config)# service reset-disable
```

5.19 reboot

Description

The **reboot** command is used to reboot the Switch. To avoid damage, please don't turn off the device while rebooting.

Syntax

reboot

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Reboot the switch:

```
Switch # reboot
```

5.20 reboot-schedule

Description

This **reboot-schedule** command is used to configure the switch to reboot at a certain time point. To delete the reboot schedule settings, please use the **reboot-schedule cancel** command.

Syntax

reboot-schedule at *time* [*date*] [**save_before_reboot**]

reboot-schedule in *interval* [**save_before_reboot**]

reboot-schedule cancel

Parameter

time —— Specify the time point for the switch to reboot, in the format of hh:mm.

date —— Specify the date for the switch to reboot, in the format of DD:MM:YYYY. The date should be within 30 days.

save_before_reboot —— Save the configuration file before the switch reboots.

interval —— Specify a time period after which the switch reboots. It ranges from 1 to 43200 minutes.

cancel —— Delete the reboot schedule settings.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

In the command **reboot-schedule at** *time* [*date*] [**save_before_reboot**], if no date is specified and the time you set here is later than the time that this command is executed, the switch will reboot later that day; otherwise the switch will reboot at the time point the next day.

Example

Specify the switch to save the configuration files and reboot in 200 minutes:

```
Switch (config)# reboot-schedule in 200 save_before_reboot
```

5.21 copy running-config startup-config

Description

The **copy running-config startup-config** command is used to save the current settings.

Syntax

copy running-config startup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Save current settings:

```
Switch # copy running-config startup-config
```

5.22 copy startup-config tftp

Description

The **copy startup-config tftp** command is used to backup the configuration file to TFTP server.

Syntax

copy startup-config tftp ip-address *ip-addr* filename *name* [vrf *vrf-name*]

Parameter

ip-addr—— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name—— Specify the name for the configuration file which would be backup.

vrf-name—— VRF instance name (1–15 characters).

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Backup the configuration files to TFTP server with the IP 192.168.0.148, name this file config.cfg and specify the VRF instance named vrf1:

```
Switch # copy startup-config tftp ip-address 192.168.0.148 filename config  
vrf vrf1
```

Backup the configuration files to TFTP server with the IP fe80::1234 and name this file config.cfg:

```
Switch # copy startup-config tftp ip-address fe80::1234 filename config
```

5.23 copy tftp startup-config

Description

The **copy tftp startup-config** command is used to download the configuration file to the switch from TFTP server.

Syntax

```
copy tftp startup-config ip-address ip-addr filename name [vrf vrf-name]
```

Parameter

ip-addr—— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name—— Specify the name for the configuration file which would be downloaded.

vrf-name—— VRF instance name (1–15 characters).

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Download the configuration file named as config.cfg to the switch from TFTP server with the IP 192.168.0.148 and specify the VRF instance named vrf1:

```
Switch # copy tftp startup-config ip-address 192.168.0.148 filename config  
vrf vrf1
```

Download the configuration file named as config.cfg to the switch from TFTP server with the IP fe80::1234

```
Switch # copy tftp startup-config ip-address fe80::1234 filename config
```

5.24 copy backup-config tftp

Description

The **copy backup-config tftp** command is used to export the backup configuration file of the switch to TFTP server.

Syntax

```
copy backup-config tftp ip-address ip-addr filename name [vrf vrf-name]
```

Parameter

ip-addr—— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name—— Specify the name for the configuration file which would be exported.

vrf-name—— VRF instance name (1–15 characters).

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Export the backup configuration file of the switch to the TFTP server with the IP 192.168.0.148, name the file config.cfg, and specify the VRF instance named vrf1:

```
Switch # copy backup-config tftp ip-address 192.168.0.148 filename config  
vrf vrf1
```

5.25 copy backup-config startup-config

Description

The **copy backup-config startup-config** command is used to replace the startup configuration file using the backup configuration file.

Syntax

```
copy backup-config startup-config
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Replace the startup configuration file using the backup configuration file.:

```
Switch # copy backup-config startup-config
```

5.26 copy running-config backup-config

Description

The **copy running-config backup-config tftp** command is used to save the current running configuration as the backup configuration file.

Syntax

```
copy running-config backup-config
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Save the current running configuration as the backup configuration file.

```
Switch # copy running-config backup-config
```

5.27 copy tftp backup-config

Description

The **copy tftp backup-config** command is used to download the backup configuration file from a TFTP server.

Syntax

```
Copy tftp backup-config ip-address ip-addr filename name [vrf vrf-name]
```

Parameter

ip-addr—— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name—— Specify the name for the configuration file which would be downloaded.

vrf-name—— VRF instance name (1–15 characters).

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Download the configuration file named config.cfg from the TFTP server with the IP 192.168.0.148 and specify the VRF instance named vrf1:

```
Switch # copy tftp backup-config ip-address 192.168.0.148 filename config  
vrf vrf1
```

5.28 ftp get



Note: This command is only available on certain devices

Description

The **ftp get** command is used to download a file from an FTP server to the switch.

Syntax

```
ftp get srcFileName dstFileName username ip-addr [vrf-name]
```

Parameter

srcFileName —— Source file name on the FTP server.

dstFileName —— Destination file name on the switch.

username —— User name for FTP login.

ip-addr —— FTP server IPv4 or IPv6 address.

vrf-name—— VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download a file to the switch over IPv4:

```
Switch# ftp get srcFile dstFile admin 192.168.0.1 testvrf1
```

5.29 ftp put



Note: This command is only available on certain devices

Description

The **ftp put** command is used to upload a file from the switch to an FTP server.

Syntax

```
ftp put srcFileName dstFileName username ip-addr [vrf-name]
```

Parameter

srcFileName — Source file name on the switch.

dstFileName — Destination file name on the FTP server.

username — User name for FTP login.

ip-addr — FTP server IPv4 or IPv6 address.

vrf-name — VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Upload a file to an FTP server over IPv4:

```
Switch# ftp put srcFile dstFile admin 192.168.0.1 testvrf1
```

5.30 scp get



Note: This command is only available on certain devices

Description

The **scp get** command is used to download a file from an SCP server to the switch.

Syntax

scp get srcFileName dstFileName username ip-addr [*vrf-name*]

Parameter

srcFileName — Source file name on the SCP server (allowed characters: alphanumeric, -_@:/.\[]()).

dstFileName — Destination file name on the switch (allowed characters: alphanumeric, -_@:/.\[]()).

username — SCP login username.

ip-addr — SCP server IPv4 or IPv6 address.

vrf-name — VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download a file to the switch over IPv4:

```
Switch# scp get srcFile dstFile admin 192.168.0.1 testvrf1
```

5.31 scp put



Note: This command is only available on certain devices

Description

The **scp put** command is used to upload a file from the switch to an SCP server.

Syntax

scp put srcFileName dstFileName username ip-addr [*vrf-name*]

Parameter

srcFileName — Source file name on the switch (allowed characters: alphanumeric, -_@:/.[]()).

dstFileName — Destination file name on the SCP server (allowed characters: alphanumeric, -_@:/.[]()).

username — SCP login username.

ip-addr — SCP server IPv4 or IPv6 address.

vrf-name — VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Upload a file to an SCP server over IPv4:

```
Switch# scp put srcFile dstFile admin 192.168.0.1 testvrf1
```

5.32 sftp get



Note: This command is only available on certain devices

Description

The **sftp get** command is used to download a file from an SFTP server to the switch.

Syntax

sftp get srcFileName dstFileName username ip-addr [*vrf-name*]

Parameter

srcFileName — Source file name on the SFTP server.

dstFileName — Destination file name on the switch.

username — User name for SFTP login.

ip-addr — SFTP server IPv4 or IPv6 address.

vrf-name — VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download a file to the switch over IPv4:

```
Switch# sftp get srcFile dstFile admin 192.168.0.1 testvrf1
```

5.33 sftp put



Note: This command is only available on certain devices

Description

The **sftp put** command is used to upload a file from the switch to an SFTP server.

Syntax

sftp put srcFileName dstFileName username ip-addr [*vrf-name*]

Parameter

srcFileName — Source file name on the switch.

dstFileName — Destination file name on the SFTP server.

username — User name for SFTP login.

ip-addr — FTP server IPv4 or IPv6 address.

vrf-name — VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Upload a file to an SFTP server over IPv4:

```
Switch# sftp put srcFile dstFile admin 192.168.0.1 testvrf1
```

5.34 copy logging

Description

The **copy logging** command is used to export system log information to the user file system.

Syntax

copy logging { flash | usbflash1 | usbflash2 } *filename*

Parameter

flash | usbflash1 | usbflash2—— The location of the exported file.

filename—— The name of the exported log file.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Export the log information to flash and name it syslog.log:

```
Switch # copy logging flash syslog.log
```

5.35 copy logging tftp

Description

The **copy logging tftp** command is used to export system log information to a remote end.

Syntax

copy logging tftp *ip-address filename*

Parameter

ip-address—— The destination IP address of the exported file.

filename—— The name of the exported log file.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Export the log information to 192.168.1.255 and name it syslog.log:

```
Switch # copy logging tftp 192.168.1.255 syslog.log.
```

5.36 boot application

Description

The **boot application** command is used to configure the image file as startup image or backup image.

Syntax

```
boot application filename { image1 | image 2 } { startup | backup }  
no boot application
```

Parameter

image1 | image2 — Specify the image file to be configured. By default, the image1.bin is the startup image and the image2.bin is the backup image.

startup | backup — Specify the property of the image, either startup image or backup image.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the image2.bin as the startup image:

```
Switch (config)# boot application filename image2 startup
```

5.37 boot config

Description

The **boot config** command is used to configure the configuration file as startup configuration or backup configuration.

Syntax

boot config filename { config1 | config 2 } { startup | backup }
no boot config

Parameter

config1 | config2 — Specify the configuration file to be configured. By default, the config1.cfg is the startup image and the config2.cfg is the backup image.

startup | backup — Specify the property of the configuration.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the config2.cfg as the startup image:

```
Switch (config)# boot config filename config2 startup
```

5.38 remove backup-image

Description

The **remove backup-image** command is used to delete the backup-image.

Syntax

remove backup-image

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Delete the backup image file:

```
Switch # remove backup-image
```

5.39 firmware upgrade

Description

The **firmware upgrade** command is used to upgrade the switch's backup image file via the TFTP server. The uploaded firmware file will take place of the Backup Image, and user can choose whether to reboot the switch with the Backup Image.

Syntax

firmware upgrade tftp ip-address *ip-addr* filename *name* [vrf *vrf-name*]

Parameter

ip-addr — IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name — Specify the name of the desired firmware file.

vrf-name — VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Upgrade the switch's backup image file with the file firmware.bin in the TFTP server with the IP address 192.168.0.148, and reboot the switch with this firmware:

```
Switch # firmware upgrade tftp ip-address 192.168.0.148 filename  
firmware.bin
```

```
It will only upgrade the backup image. Continue? (Y/N):y
```

```
Operation OK!
```

```
Reboot with the backup image? (Y/N): y
```

Upgrade the switch's backup image file with the file firmware.bin in the TFTP server with the IP address fe80::1234, but do not reboot the switch:

```
Switch # firmware upgrade tftp ip-address fe80::1234 filename  
firmware.bin
```

```
It will only upgrade the backup image. Continue? (Y/N):y
```

```
Operation OK!
```


Reboot with the backup image? (Y/N): n

5.40 patch load (Only for Certain Devices)

Description

This command is used to load a patch file from a TFTP server into the patch area of the system. The patch is in the deactivated state and has not taken effect.

Syntax

patch load ip-address *ip-addr* **filename** *filename* [**vrf** *vrf-name*] [**unit** *unit-id*]

Parameter

ipaddr: IP address of the TFTP server.

filename: Name of the patch file.

vrf-name: VRF instance name (1-15 characters).

unit id: Stack unit ID, ranging from 1 to 4.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Download the patch file named patch.bin from the TFTP server address with IP address 192.168.0.2 and specify the VRF instance named vrf1 on unit 1:

```
Switch# patch load ip-address 192.168.0.146 filename patch.bin vrf vrf1  
unit 1
```

5.41 patch active (Only for Certain Devices)

Description

This command is used to temporarily run a deactivated patch loaded into the system patch area. When a deactivated patch is temporarily run, the patch is activated and takes effect. When the device is restarted, the patch that was

activated before the restart will be deactivated. Users can perform the following three operations on the activated patch.

Syntax

patch active [**unit** *unit-id*]

Parameter

unit id: Stack unit ID, ranging from 1 to 4.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Activate all deactivated patches loaded into the system patch area on unit 1:

```
Switch# patch active unit 1
```

5.42 patch run (Only for Certain Devices)

Description

This command is used to permanently run an activated patch. When an activated patch is permanently run, the patch is in the running state. When the device is restarted, the patch that was in the running state before the restart will remain in the running state and take effect. Users can perform the following two operations on the running patch:

Syntax

patch run [**unit** *unit-id*]

Parameter

unit id: Stack unit ID, ranging from 1 to 4.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Permanently run an activated patch on unit 1:

```
Switch# patch run unit 1
```

5.43 patch deactivate (Only for Certain Devices)

Description

This command is used to deactivate an activated patch:

Syntax

```
patch deactivate [unit unit-id]
```

Parameter

unit id: Stack unit ID, ranging from 1 to 4.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Deactivate an activated patch on unit 1:

```
Switch# patch deactivate unit 1
```

5.44 patch uninstall (Only for Certain Devices)

Description

This command is used to uninstall a running patch and activate it:

Syntax

```
patch uninstall [unit unit-id]
```

Parameter

unit id: Stack unit ID, ranging from 1 to 4.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Uninstall a running patch on unit 1 and activate it:

```
Switch# patch uninstall unit 1
```

5.45 patch delete (Only for Certain Devices)

Description

This command is used to delete a patch in the deactivated, activated, or running state, invalidating the patch and deleting the patch file from the system patch area:

Syntax

```
patch delete [ unit unit-id]
```

Parameter

unit id: Stack unit ID, ranging from 1 to 4.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Delete a patch from unit 1:

```
Switch# patch delete unit 1
```

5.46 show patch information (Only for Certain Devices)

Description

This command is used to view the patch information of the current system:

Syntax

show patch information

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the patch information of the current system:

```
Switch# show patch information
```

5.47 mcu-firmware unit upgrade

(Only for Certain Devices)

Description

The **mcu-firmware unit upgrade** command is used to upgrade the switch's MCU-firmware online.

Syntax

mcu-firmware unit {*unit id*} type {*mcu-type*} upgrade

Parameter

unit id—— Stack unit ID, ranging from 1 to 4.

mcu-type—— MCU device type, which can be pse, crps, fan, monitor.

Command Mode

None

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Upgrade the switch's MCU-firmware online:

```
Switch#mcu-firmware unit 1 type pse upgrade
```

5.48 mcu-firmware type (Only for Certain Devices)

Description

The **mcu-firmware type** command is used to display the MCU version information.

Syntax

mcu-firmware type {*mcu-type*} **version**

Parameter

mcu-type—— MCU device type, which can be pse, crps, fan, monitor.

Command Mode

None

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the MCU firmware version of the PSE:

```
Switch# mcu-firmware type pse version
```

5.49 checkpoint file (Only for Certain Devices)

Description

The **checkpoint file** command is used to create a checkpoint file. When creating a checkpoint file, it snapshots the current configuration. When deleting a checkpoint file, specify the filename for deletion. Note that after performing a device reset operation, all checkpoint files will be cleared. To delete a checkpoint file, please use the **no checkpoint file** command.

Syntax

checkpoint file *filename*

no checkpoint file *fileName*

Parameter

fileName: Checkpoint file name, in the format of letters, numbers, underscores, hyphens and dots, and the length is limited to 1 to 32 characters. For example: hello_2024-01.cfg

Command Mode

Privileged EXEC Mode

Privilege Requirement

Privileged EXEC Mode and Any Configuration Mode

Example

Create a checkpoint file named "hello2024" for the current configuration:

```
Switch#checkpoint file hello2024
```

5.50 show checkpoint (Only for Certain Devices)

Description

The **show checkpoint** command is used to view the names of all existing checkpoint files, or view all configuration information in a specific checkpoint file.

Syntax

show checkpoint

show checkpoint file *fileName*

Parameter

fileName: Checkpoint file name, in the format of letters, numbers, underscores, hyphens and dots, and the length is limited to 1 to 32 characters. *fileName* must be the name of an existing file in the show checkpoint command execution result.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Privileged EXEC Mode and Any Configuration Mode

Example

View the configuration information in the checkpoint file named "hello2024":

```
Switch#show checkpoint file hello2024
```

5.51 rollback running-config file

(Only for Certain Devices)

Description

The **rollback running-config file** command is used to roll back the configuration of the switch to the configuration in an existing checkpoint file.

Syntax

rollback running-config file *fileName*

Parameter

fileName: Checkpoint file name, in the format of letters, numbers, underscores, hyphens and dots, and the length is limited to 1 to 32 characters. *fileName* must be the name of an existing file in the show checkpoint command execution result.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Privileged EXEC Mode and Any Configuration Mode

Example

Roll back the configuration of the switch to the configuration in the checkpoint file named "hello2024":

```
Switch# rollback running-config file hello2024
```

5.52 boot autoinstall start



Note: This command is only available on certain devices.

Description

The **boot autoinstall start** command is used to start Auto Install function. To stop the Auto Install function, use **no boot autoinstall start**.

Syntax

boot autoinstall start [**interface** {fastEthernet | gigabitEthernet | ten-gigabitEthernet | hundred-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan | port-channel port}]

no boot autoinstall start

Parameter

fastEthernet | gigabitEthernet | ten-gigabitEthernet | hundred-gigabitEthernet
| twentyFive-gigabitEthernet | two-gigabitEthernet | vlan | port-channel port:
Specify the interface to be bound for Auto Install.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Start Auto Install function and bind it to interface 1/0/1:

```
Switch(config)# boot autoinstall start interface 1/0/1
```

5.53 boot autoinstall persistent-mode



Note: This command is only available on certain devices.

Description

The **boot autoinstall persistent-mode** command is used to start Auto Install function to next reboot cycle. To disable persistent mode, use **no boot autoinstall persistent-mode**.

Syntax

boot autoinstall persistent-mode
no boot autoinstall persistent-mode

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Start Auto Install function:

```
Switch(config)# boot autoinstall persistent-mode
```

5.54 boot autoinstall auto-save



Note: This command is only available on certain devices.

Description

The **boot autoinstall auto-save** command is used to automatically save the new configuration file that was downloaded by Auto Install function to start-up configuration file Auto Install. To disable auto-save configuration feature use **no boot autoinstall auto-save**.

Syntax

boot autoinstall auto-save

no boot autoinstall auto-save

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure Auto Install function to auto-save new configuration file to start-up configuration file:

```
Switch(config)# boot autoinstall auto-save
```

5.55 boot autoinstall auto-reboot



Note: This command is only available on certain devices.

Description

The **boot autoinstall auto-reboot** command is used to automatically reboot the switch after Auto Install function is completed successfully. To disable auto-reboot feature use **no boot autoinstall auto-reboot**.

Syntax

boot autoinstall auto-reboot

no boot autoinstall auto-reboot

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the switch to auto reboot after Auto Install function completed successfully:

```
Switch(config)# boot autoinstall auto-reboot
```

5.56 boot autoinstall retry-count



Note: This command is only available on certain devices.

Description

The **boot autoinstall retry-count** command is used to configure retry count when Auto Install function uses TFTP to download configuration files in a cycle of Auto Install process. To set retry count to default value use **no boot autoinstall retry-count**.

Syntax

boot autoinstall retry-count *count*

no boot autoinstall retry-count

Parameter

count—— The count of retrying auto install. The value ranges from 1 to 3.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure TFTP retry 2 times when download files failed:

```
Switch(config)# boot autoinstall retry-count 2
```

5.57 show boot autoinstall



Note: This command is only available on certain devices.

Description

The **show boot autoinstall** command is used to display the configuration of Auto Install function.

Syntax

show boot autoinstall

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Auto Install function:

```
Switch# show boot autoinstall
```

5.58 show boot autoinstall downloaded-config



Note: This command is only available on certain devices.

Description

The **show boot autoinstall downloaded-config** command is used to display the configuration file which downloaded by Auto Install.

Syntax

show boot autoinstall downloaded-config

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration file which downloaded by Auto Install:

```
Switch# show boot autoinstall downloaded-config
```

5.59 ping

Description

The **ping** command is used to test the connectivity between the switch and one node of the network.

Syntax

```
ping [ ip | ipv6 ] { ip_addr } [ -n count ] [ -l size ] [ -i interval ] [ -vrf vrf-name ] [ -a src-addr ] [ -s interface { fastEthernet | gigabitEthernet | ten-gigabitEthernet | hundred-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan | port-channel port } ]
```

Parameter

ip — The type of the IP address for ping test should be IPv4.

ipv6 — The type of the IP address for ping test should be IPv6.

ip_addr — The IP address of the destination node for ping test. If the parameter *ip/ipv6* is not selected, both IPv4 and IPv6 addresses are supported, for example 192.168.0.100 or fe80::1234.

count — The amount of times to send test data during Ping testing. It ranges from 1 to 10. By default, this value is 4.

size — The size of the sending data during ping testing. It ranges from 1 to 1500 bytes. By default, this value is 64.

interval — The interval to send ICMP request packets. It ranges from 100 to 1000 milliseconds. By default, this value is 1000.

vrf-name — VRF instance name (1-15 characters).

src-addr — Source IP address for the ping packets (IPv4 or IPv6).

interface { fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | vlan | port-channel } port — Source interface used to send ping packets.

Command Mode

Privileged EXEC Mode

Privilege Requirement

None.

Example

Test connectivity to 192.168.0.131 in VRF vrf1, using source address 192.168.0.10 and source interface GigabitEthernet 1/0/1:

```
Switch # ping 192.168.0.131 -vrf vrf1 -a 192.168.0.10 -s interface
gigabitEthernet 1/0/1
```

5.60 tracert

Description

The **tracert** command is used to test the connectivity of the gateways during its journey from the source to destination of the test data.

Syntax

```
tracert [ ip | ipv6 ] ip_addr [ maxHops ] [-vrf vrf-name] [-a src-addr] [-s
interface{fastEthernet | gigabitEthernet | ten-gigabitEthernet |
hundred-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet |
vlan | port-channel port}]
```

Parameter

ip — The type of the IP address for tracert test should be IPv4.

ipv6 — The type of the IP address for tracert test should be IPv6.

ip_addr — The IP address of the destination device. If the parameter *ip/ipv6* is not selected, both IPv4 and IPv6 addresses are supported, for example 192.168.0.100 or fe80::1234.

maxHops — The maximum number of the route hops the test data can pass through. It ranges from 1 to 30. By default, this value is 4.

vrf-name — VRF instance name (1-15 characters).

src-addr — Source IP address for the tracert packets (IPv4 or IPv6).

interface{ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | vlan | port-channel } port — Source interface used to send tracert packets.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Trace the route to 192.168.0.131 in VRF vrf1, using source address 192.168.0.10 and source interface GigabitEthernet 1/0/1:

```
Switch # tracert 192.168.0.131 20 -vrf vrf1 -a 192.168.0.10 -s interface  
gigabitEthernet 1/0/1
```

5.61 show system-info

Description

The **show system-info** command is used to display System Description, Device Name, Device Location, System Contact, Hardware Version, Firmware Version, System Time, Run Time and so on.

Syntax

```
show system-info
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the system information:

```
Switch # show system-info
```

5.62 show image-info

Description

The **show image-info** command is used to display the information of image files in the system.

Syntax

```
show image-info
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system image files' information:

```
Switch# show image-info
```

5.63 show boot

Description

The **show boot** command is used to display the boot configuration of the system.

Syntax

```
show boot
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system boot configuration information:

```
Switch# show boot
```

5.64 show running-config

Description

The **show running-config** command is used to display the current operating configurations of the whole system, a specified unit, or a specified port.

Syntax

```
show running-config [unit{all || [exclude keyword] [include keyword] |  
interface {fastEthernet | gigabitEthernet | ten-gigabitEthernet} port} ]  
show running-config [all || [exclude keyword] [include keyword] | interface  
{fastEthernet | gigabitEthernet | ten-gigabitEthernet} port]
```

Parameter

unit—— Specify the unit number of a switch to show the unit's operating configurations. By default, it is 1.

all—— Display all the operating configurations of the whole system or a specified unit.

|—— Enable filter to filtrate the configurations. You can use **exclude** and **include** to set the filter rule.

keyword—— The filter conditions, such as interface, vlan, and user.

port—— Specify the number of the port to show the port's operating configurations.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the current operating configurations only related to the user:

```
Switch# show running-config | include user
```

5.65 show startup-config

Description

The **show startup-config** command is used to display the current configuration saved in the switch. These configuration settings will not be lost the next time you reboot the switch.

Syntax

```
show startup-config
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the saved configuration:

```
Switch# show startup-config
```

5.66 show system-time

Description

The **show system-time** command is used to display the time information of the switch.

Syntax

show system-time

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the time information of the switch

```
Switch# show system-time
```

5.67 show system-time dst

Description

The **show system-time dst** command is used to display the DST information of the switch.

Syntax

show system-time dst

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DST information of the switch

```
Switch# show system-time dst
```

5.68 show system-time ntp

Description

The **show system-time ntp** command is used to display the NTP mode configuration information.

Syntax

show system-time ntp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the NTP mode configuration information of the switch:

```
Switch# show system-time ntp
```

5.69 show cable-diagnostics interface

Description

The **show cable-diagnostics interface** command is used to display the cable diagnostics of the connected Ethernet Port., which facilitates you to check the connection status of the cable connected to the switch, locate and diagnose the trouble spot of the network.

Syntax

```
show cable-diagnostics interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Parameter

port—— The number of the port which is selected for Cable test.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Show the cable-diagnostics of port 3:

```
Switch# show cable-diagnostics interface gigabitEthernet 1/0/3
```

5.70 show cpu-utilization

Description

The **show cpu-utilization** command is used to display the system's CPU utilization in the last 5 seconds/1minute/5minutes.

Syntax

show cpu-utilization

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the CPU utilization information of the switch:

```
Switch# show cpu-utilization
```

5.71 show memory-utilization

Description

The **show memory-utilization** command is used to display the current system's memory utilization in the last 5 seconds/1minute/5minutes.

Syntax

show memory-utilization

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the memory utilization information of the switch:

```
Switch# show memory-utilization
```

5.72 show controller



Note: This command is only available on certain devices.

Description

The **show controller** command is used to display the current controller settings and status.

Syntax

show controller

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the current controller settings and status:

```
Switch# show controller
```

5.73 show temperature



Note: This command is only available on certain devices.

Description

The **show temperature** command is used to display the temperature of switch.

Syntax

show temperature

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the temperature information of the switch:

```
Switch-DC# show temperature
```

5.74 show voltage



Note: This command is only available on certain devices.

Description

The **show voltage** command is used to display the voltage of DC power board.

Syntax

```
show voltage
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the voltage information of the switch:

```
Switch # show voltage
```

5.75 clear config interface

Description

The **clear config interface** command is used to clear all configurations of a specified port.

Syntax

```
clear config interface [fastEthernet | gigabitEthernet |  
two-gigabitEthernet | ten-gigabitEthernet | port-channel ] port
```

Parameter

port—— The port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Clear all configurations of gigabitEthernet port 1/0/3:

```
Switch(config)# clear config interface gigabitEthernet 1/0/3
```

5.76 power backup unit (Only for Certain Devices)

Description

The **power backup unit** command is used to configure the power backup mode.

Syntax

power backup unit *{unit id}* *{power}* **mode** *{mode}*

Parameter

unit id—— Stack unit ID, ranging from 1-4.

power—— power supply module number.

mode—— Power backup mode

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the power backup mode of stack unit 1:

```
Switch(config)#power backup unit 1 pwr1 mode enable
```

5.77 show power (Only for Certain Devices)

Description

The **show power** command is used to display the power details.

Syntax

show power [detail]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the power details:

```
Switch#show power
```


Chapter 6 PTP Configuration Commands (Only for Certain Devices)

The Precision Time Protocol (PTP) in network measurement and control systems is a protocol for synchronizing time (phase) and frequency across standard Ethernet devices. It is also known as IEEE 1588 (defined by IEEE) or 1588 for short. Its primary goal is to achieve high-precision clock synchronization within Local Area Networks (LAN) or Wide Area Networks (WAN) to meet the requirements of applications such as communication networks, industrial control, financial trading, and audio/video transmission.

PTP defines the basic paradigm for network clock synchronization and imposes no strict requirements on the network environment, ensuring broad adaptability. Based on PTP, derived protocols such as 802.1as (also known as gPTP), G.8265.1, G.8275.1, G.8275.2, SMPTE, and AES67 have been developed. These protocols impose restrictions on network environments and PTP parameters for specific domains and can be seen as functional subsets of PTP (achievable through PTP's profile mechanism).

6.1 ptp enable (Global View)

Description

The **ptp enable** command is used to enable the PTP function globally. To disable this function globally, use the **no ptp enable** command. By default, PTP is disabled.

Syntax

ptp enable
no ptp enable

Parameter

None

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the PTP function globally:

```
Switch(config)# ptp enable
```

6.2 ptp profile

Description

The **ptp profile** command is used to specify the PTP protocol standard. To restore the default protocol standard (1588v2), use the **no ptp profile** command.

Syntax

ptp profile { *1588v2* / *8021as* }

no ptp profile

Parameter

1588v2 / *8021as*—— Specify the protocol standard (default: 1588v2).

Note

Changing the protocol standard will clear all existing configurations under the previous standard and reset PTP parameters to their default values for the new standard. The global ptp enable state is retained.

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the protocol to 802.1as:

```
Switch(config)# ptp profile 8021as
```

6.3 ptp clock-type

Description

The **ptp clock-type** command is used to configure the PTP node type. To remove the configuration, use the **no ptp clock-type** command. No node type is set by default.

Syntax

ptp clock-type { *bc* / *oc* / *e2etc* / *p2ptc* }

no ptp clock-type

Parameter

Node types vary by protocol:

1588v2: *bc, oc, e2etc, p2ptc*

802.1as: *bc, oc, p2ptc*

Note

Ensure compatibility with the configured protocol standard.

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the node type to bc under 1588v2:

```
Switch(config)# ptp clock-type bc
```

6.4 ptp domain

Description

The **ptp domain** command is used to specify the PTP clock domain. To restore the default domain for the current protocol, use the **no ptp domain** command. Only devices in the same domain can synchronize.

Syntax

ptp domain *domain*

no ptp domain

Parameter

domain—— Domain ID (integer). Default varies by protocol.

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the domain to 1:

```
Switch(config)# ptp domain 1
```

6.5 ptp clock-class

Description

The **ptp clock-class** command is used to set the clock quality class (lower values indicate higher priority in master election). Default: 248.

Syntax

ptp clock-class *clock-class*

no ptp clock-class

Parameter

clock-class—— Integer (smaller values = higher priority).

Note

If <clock-class> < 128, the device cannot act as a slave. Configure carefully to avoid synchronization issues.

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set clock class to 200:

```
Switch(config)# ptp clock-class 200
```

6.6 ptp priority1

Description

The **ptp priority1** command is used to set Priority1 for master election (lower values = higher priority). Defaults vary by protocol.

Syntax

ptp priority1 *priority1*

no ptp priority1

Parameter

priority1—— Integer (specific range depends on protocol).

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set Priority1 to 129:

```
Switch(config)# ptp priority1 129
```

6.7 ptp priority2

Description

The **ptp priority2** command is used to set Priority2 for master election (lower values = higher priority). Defaults vary by protocol.

Syntax

ptp priority2 *priority1*

no ptp priority2

Parameter

priority2—— Integer (specific range depends on protocol).

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set Priority2 to 129:

```
Switch(config)# ptp priority2 129
```

6.8 ptp slave-only

Description

The **ptp slave-only** command is used to OC-type ports to operate as slave-only. To restore the default behavior (master/member allowed), use the **no ptp slave-only** command.

Syntax

ptp slave-only

no ptp slave-only

Parameter

None

Note

Only applicable to OC node types.

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure slave-only mode for OC under 1588v2:

```
Switch (config)# ptp profile 1588v2
```

```
Switch (config)# ptp clock-type oc
```

```
Switch (config)# ptp slave-only
```

6.9 ptp utc-offset

Description

The **ptp utc-offset** command is used to correct the deviation between UTC time and TAI time. Its **no** command is used to restore utc-offset to the default value. By default, the value of utc-offset is 37 seconds.

Syntax

ptp utc-offset *utc-offset*

no ptp utc-offset

Parameter

utc-offset—— Specify the offset between UTC time and TAI time, in integer form, in seconds, with a default value of 37 seconds.

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the offset to 40 seconds:

```
Switch (config)# ptp utc-offset 40
```

6.10 ptp virtual-id

Description

The **ptp virtual-id** command is used to configure the virtual clock ID of the ptp device. Its no command is used to restore the default clock ID. The clock ID is unique and is used to distinguish other clock devices in the domain. By default, the clock ID is composed of the mac address of the device and 0xfffe.

Syntax

ptp virtual-id *xxxxxx.xxxx.xxxxxx*

no ptp virtual-id

Parameter

xxxxxx.xxxx.xxxxxx—— Hexadecimal ID.

Command Mode

Global Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set virtual ID to 112233.4455.aabbcc:

```
Switch (config)# ptp virtual-id 112233.4455.aabbcc
```

6.11 ptp enable (Interface View)

Description

The **ptp enable** command is used to PTP functionality on a port, turning it into a PTP port. The no form disables PTP on the port. By default, PTP is disabled on ports.

Syntax

ptp enable

no ptp enable

Parameter

None

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable PTP on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp enable
```

6.12 ptp announce-interval

Description

The **ptp announce-interval** command is used to configure the announce message transmission rate on a port. The no form restores the protocol-standard default. The default is protocol-specific.

Syntax

ptp announce-interval *announce-interval*

no ptp announce-interval

Parameter

announce-interval — Transmission interval in seconds, calculated as 2 times the announce-interval in seconds.

Notes

Announce messages are used for clock source election and master-slave synchronization. Excessive rates may consume bandwidth and degrade synchronization. Configure this value carefully.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set announce messages to 1 per second on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
Switch (config-if)# ptp announce-interval 0
```

6.13 ptp announce-timeout

Description

The **ptp announce-interval** command is used to configure the maximum allowed missed announce messages before triggering clock source re-election. The no form restores the default value 3.

Syntax

ptp announce-timeout *announce-timeout*

no ptp announce-timeout

Parameter

announce-timeout—— Timeout threshold (number of intervals).

Notes

Ensure compatibility between announce-timeout and announce-interval. Overly frequent intervals or low timeout values may cause instability.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set timeout to 4 on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp announce-timeout 4
```

6.14 ptp sync-interval

Description

The **ptp sync-interval** command is used to configure the sync message transmission rate. The no form restores the protocol-standard default.

Syntax

ptp sync-interval *sync-interval*

no ptp sync-interval

Parameter

sync-interval — Specify the sync message sending rate on this port. The sending interval is 2 times the sync-interval in seconds.

Notes

Sync messages affect synchronization accuracy. Balance precision and bandwidth usage.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set sync messages to 2 per second on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp sync-interval -1
```

6.15 ptp delay-req-interval

Description

The **ptp delay-req-interval** command is used to configure the minimum interval for sending delay_req packets on a port. The no command is used to restore the default value of the current protocol standard. By default, the default value is used.

Syntax

ptp delay-req-interval *delay-req-interval*

no ptp delay-req-interval

Parameter

delay-req-interval—— Specify the minimum interval for sending delay-req packets on this port. The interval is 2 times the delay-req-interval in seconds.

Notes

Used in request-response mode for path delay calculation. Balance accuracy and bandwidth.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set delay_req rate to 2 per second on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp delay-req-interval -1
```

6.16 ptp pdelay-req-interval

Description

The **ptp pdelay-req-interval** command is used to configure the minimum interval for sending pdelay_req packets on a port. The no command is used to restore the default value of the current protocol standard. By default, the default value is used.

Syntax

ptp delay-req-interval *pdelay-req-interval*

no ptp delay-req-interval

Parameter

pdelay-req-interval—— Specify the minimum interval for sending pdelay-req packets on this port. The interval is 2 times the pdelay-req-interval in seconds.

Notes

Used in peer-to-peer delay mechanism. Balance accuracy and bandwidth.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set pdelay_req rate to 2 per second on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp pdelay-req-interval-1
```

6.17 ptp clock-step

Description

The **ptp clock-step** command is used to configure the timestamp carrying mode of the message on the port. The no command is used to restore the default value under the current protocol standard.

Syntax

ptp clock-step {*one-step* / *two-step*}

no ptp clock-step

Parameter

None

Notes

Not applicable for E2ETC/P2PTC node types.

Unavailable under IEEE 802.1AS.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set timestamp mode to two-step on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp clock-step two-step
```

6.18 ptp delay-mechanism

Description

The **ptp delay-mechanism** command is used to configure the delay measurement mechanism used by the port. The no command is used to restore the default value under the current protocol standard.

Syntax

ptp delay-mechanism {e2e / p2p}

no ptp delay-mechanism

Parameter

None

Notes

Not applicable for E2ETC/P2PTC node types.

Unavailable under IEEE 802.1AS.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set delay mechanism to P2P on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp delay-mechanism p2p
```

6.19 ptp asymmetry-correction

Description

The **ptp asymmetry-correction** command is used to configure the asymmetric delay correction time for the port to send ptp messages. The **no** command is used to cancel the asymmetric delay correction time for the port to send ptp messages. By default, it is not configured.

Syntax

ptp asymmetry-correction *asymmetry-correction*

no ptp asymmetry-correction

Parameter

asymmetry-correction—— Specify the correction time in nanoseconds.

Notes

Corrects synchronization errors caused by unequal transmit/receive path delays.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set correction to 200 ns on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp asymmetry-correction 200
```

6.20 ptp eth-egress

Description

The **ptp eth-egress** command is used to configure the layer 2 encapsulation for PTP messages. The **no** command is used to reset settings.

Syntax

ptp mac-egress {**destination-mac** *destination-mac* /**vlan** *vlan-id* [**priority** *priority*]}
priority}}

no ptp mac-egress { destination-mac /vlan }

Parameter

destination-mac—— Destination MAC address of the packet in Layer 2 encapsulation.

vlan-id—— VLAN ID of the packet in Layer 2 encapsulation.

priority—— 802.1p priority of the VLAN.

Notes

Invalid MACs (e.g., multicast) are rejected.

Disable UDP encapsulation first if configured.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set destination MAC to aa:bb:cc:11:22:33:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
```

```
Switch (config-if)# ptp mac-egress aa:bb:cc:11:22:33
```

6.21 ptp udp-egress

Description

The **ptp udp-egress** command is used to configure Layer 3 UDP encapsulation for PTP messages. The no command is used to reset settings.

Syntax

```
ptp udp-egress {source-ip ip-address /destination-ip ip-address |  
destination-mac destination-mac /vlan vlan-id[priority priority]}  
  
no ptp udp-egress {source-ip /destination-ip | destination-mac /vlan }
```

Parameter

source-ip —— Source IP address of the Layer 3 packet encapsulation

destination-ip —— Destination IP address of the Layer 3 packet encapsulation

destination-mac — Destination MAC address of the Layer 3 packet encapsulation.

vlan-id — VLAN ID of the Layer 3 packet encapsulation.

priority — 802.1p priority of the VLAN.

Notes

When configuring UDP encapsulation, you need to configure the source IP address first.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the source IP address of UDP encapsulation to 192.168.1.5 on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
Switch (config-if)# ptp udp-egress source-ip 192.168.1.5
```

6.22 ptp reset-statistics

Description

The **ptp reset-statistics** command is used to clear the statistics of the port's message transmission and reception.

Syntax

ptp reset-statistics

Parameter

None

Notes

Once the message transmission and reception statistics are cleared, they cannot be restored.

Command Mode

Interface Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear message statistics on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# interface ten-gigabitEthernet 1/0/1
Switch (config-if)# ptp reset-statistics
```

6.23 show ptp all

Description

The **show ptp all** command is used to view the running status of the PTP protocol.

Syntax

show ptp all

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the the running status of the PTP protocol:

```
Switch (config)# show ptp all
```

6.24 show ptp interface

Description

The **show ptp interface** command is used to view the running status and statistics of the PTP port.

Syntax

show ptp all

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the running status and statistics of the PTP port on Ten-GigabitEthernet 1/0/1:

```
Switch (config)# show ptp interface ten-gigabitEthernet 1/0/1
```

Chapter 7 File System Configuration Commands

(Only for Certain Devices)

File System Commands can be used to configure the File System.

7.1 copy

Description

The **copy** command is used to copy the specified file.

Syntax

copy {flash|usbflash1|usbflash2} {filename} {destination}

Parameter

flash|usbflash1|usbflash2 — The flash type of the source file.

filename — File name.

destination — Copied file path.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Copy the specified file:

```
Switch#copy flash test.txt usbflash1
```

7.2 cd

Description

The **cd** command is used to change the current file path.

Syntax

cd {filename|flash|usbflash1|usbflash2} [filename]

Parameter

filename|flash|usbflash1|usbflash2 — The path that needs to be switched. If you enter filename, the file will be found in the current path by default.

filename — Specify the file in the corresponding flash.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Change the current file path:

```
Switch# cd usbflash1 test
```

7.3 dir

Description

The **dir** command is used to list files and subdirectories contained in the specified working directory.

Syntax

dir [flash|usbflash1|usbflash2] [filename]

Parameter

flash|usbflash1|usbflash2 — Specify path.

filename — Specify the file in the corresponding flash.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

List files and subdirectories contained in the specified working directory:

```
Switch#dir flash
```

7.4 pwd

Description

The **pwd** command is used to display the absolute path name of the current working directory.

Syntax

pwd

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the absolute path name of the current working directory:

```
Switch#pwd
```

7.5 rename

Description

The **rename** command is used to rename a file.

Syntax

rename {srcFilename} {dstFilename}

Parameter

srcFilename — Source file name.

dstFilename — Renamed file name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Rename a file:

```
Switch#rename test1 test2
```

7.6 delete

Description

The **delete** command is used to delete a file.

Syntax

delete {filename|flash|usbflash1|usbflash2} [filename]

Parameter

filename|flash|usbflash1|usbflash2 — The file that needs to be deleted. If you enter filename, the file will be found in the current working path by default.

filename — Specify the file in the corresponding flash.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete a file:

```
Switch# delete text.txt
```

7.7 ftp

Description

The **ftp** command is used to enter the FTP (File Transfer Protocol) view.

Syntax

ftp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enter the FTP view:

```
Switch#ftp
```

7.8 open

Description

The **open** command is used to connect to FTP server.

Syntax

open [ipv6] {hostIp}

Parameter

ipv6—— Specify the FTP server type as IPv6.

hostIp —— FTP server IP.

Command Mode

FTP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Connect to FTP server:

```
Switch(ftp)#open 192.168.0.146
```

7.9 put

Description

The **put** command is used to upload files to FTP server.

Syntax

put {srcFilename} {dstFilename}

Parameter

srcFilename —— Source file name.

dstFilename —— Destination file name.

Command Mode

FTP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Upload files to FTP server:

```
Switch(ftp)#put src.c dst.c
```

7.10 get

Description

The **get** command is used to download files from FTP server.

Syntax

```
get {srcFilename} {dstFilename}
```

Parameter

srcFilename —— Source file name.

dstFilename —— Destination file name.

Command Mode

FTP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download files from FTP server:

```
Switch(ftp)#get src.c dst.c
```

7.11 close

Description

The **close** command is used to close current FTP connection.

Syntax

```
close
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Close current FTP connection:

```
Switch#close
```

Chapter 8 Management Port Configuration

Commands (Only for Certain Devices)

8.1 management-port protocol

Description

The **management-port protocol** command is used to enable or disable the IPv4 DHCP function on the management port.

Syntax

management-port protocol {*dhcp*|*none*}

Parameter

dhcp——Enable the DHCP function

none——Disable the DHCP function

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IPv4 DHCP function on the management port:

```
Switch(config)#management-port protocol dhcp
```

8.2 management-port ip

Description

The **management-port ip** command is used to configure the IPv4 address of the management port. To delete the address, please use the **no management-port ip** command.

Syntax

management-port ip {*ip-addr*}{*mask*}

no management-port ip

Parameter

ip-addr——IPv4 address

mask—— IP mask

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the IPv4 address of the management port:

```
Switch(config)#management-port ip 192.168.10.1 255.255.255.0
```

8.3 management-port ipv6 enable

Description

The **management-port ipv6 enable** command is used to enable the management-port ipv6 function. To disable the function, please use the **no management-port ipv6 enable** command.

Syntax

management-port ipv6 enable

no management-port ipv6 enable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the management-port ipv6 function:

```
Switch(config)#management-port ipv6 enable
```

8.4 management-port ipv6 address

Description

The **management-port ipv6 address** command is used to configure the IPv6 address of the management port. To delete the address, please use the **no management-port ipv6 address** command.

Syntax

management-port ipv6 address {*ipv6-addr*} [*eui64*]

no management-port ipv6 address {*ipv6-addr*} [*eui64*]

Parameter

ipv6-addr—— IPv6 address, you need to specify the prefix length.

eui64—— Create the address in eui64 mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the IPv6 address of the management port:

```
Switch(config)#management-port ipv6 address 2001::1/64 eui64
```

8.5 show management-port

Description

The **show management-port** command is used to display the configuration information of the management port.

Syntax

show management-port

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of the management port:

```
Switch# show management-port
```

Chapter 9 EEE Configuration Commands

EEE (Energy Efficient Ethernet) is used to save power consumption of the switch during periods of low data activity. You can simply enable this feature on ports to allow power reduction.

9.1 eee

Description

The **eee** command is used to enable EEE on the port. To disable EEE on the port, please use **no eee** command.

Syntax

eee

no eee

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable EEE on port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#eee
```

9.2 show interface eee

Description

The **show interface eee** command is used to display the EEE configuration on each port.

Syntax

**show interface eee [fastEthernet *port* | gigabitEthernet *port* |
two-gigabitEthernet *port* | ten-gigabitEthernet *port*]**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the EEE configuration of each port

```
Switch# show interface eee
```

Chapter 10 SDM Template Commands

This chapter describes how to configure the Switch Database Management (SDM) templates to allocate hardware resources on the switch for different uses.

10.1 **show sdm prefer dynamic**

Description

The **show sdm prefer dynamic** command is used to display dynamic resource allocation of the current SDM template in use, or the SDM templates that can be used.

Syntax

show sdm prefer dynamic

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the resource allocation of the template currently in use:

```
Switch(config)#show sdm prefer dynamic
```


Chapter 11 Time Range Commands

With this feature, you can configure a time range and bind it to a PoE port or an ACL rule.

11.1 time-range

Description

The **time-range** command is used to create time-range entry for the switch and enter Time-range Create Configuration Mode. After a time-range entry is created, you need to specify the date and time. A time-range can implement multiple time-ranges simultaneously as long as they do not conflict with each other. To delete the corresponding time-range configuration, please use **no time-range** command.

Syntax

time-range *name*

no time-range *name*

Command Mode

Global Configuration Mode

Parameter

name — The time-range name, ranging from 1 to 16 characters.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a time-range named "tRange1" for the switch:

```
Switch(config)# time-range tRange1
```

11.2 absolute

Description

The **absolute** command is used to create an absolute time-range for the time-range of the switch. To delete the corresponding absolute time-range configuration, please use **no absolute** command.

Syntax

absolute from *start-date* **to** *end-date*

no absolute [*index*]

Parameter

start-date—— The start date in Absoluteness Mode, in the format of MM/DD/YYYY.

end-date—— The end date in Absoluteness Mode, in the format of MM/DD/YYYY.

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an absolute time-range for the switch and specify the date extending from May 5th, 2017 through Oct. 5th, 2017:

```
Switch(config)#time-range tRange1
```

```
Switch(config-time-range)#absolute from 05/05/2017 to 10/05/2017
```

11.3 periodic

Description

The **periodic** command is used to create a periodic mode time-range for the time-range of the switch. To delete the corresponding periodic mode time-range configuration, please use **no periodic** command.

Syntax

periodic start *start-time* **end** *end-time* **day-of-the-week** *week-day*

no periodic [*index*]

Parameter

start-time——Specify the start time in the format of HH:MM

end-time——Specify the end time in the format of HH:MM

week-day——In the format of 1-3, 6, daily, off-day, or working-day. For example, 1-3,6 represents Monday, Tuesday, Wednesday and Saturday; daily represents every day; off-day represents the weekends; working-day represents the working days.

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time-range tSeg1 with time from 8:30 to 12:00 at weekends:

```
Switch(config)#time-range tSeg1
Switch(config-time-range)#periodic start 08:30 end 12:00
day-of-the-week 6-7
```

11.4 holiday (time-range mode)

Description

The **holiday** command is used to create holiday mode time-range for the time-range of the switch. When the holiday which is excluded from time-range occurs, the switch will not supply power.

Syntax

```
holiday { exclude | include }
```

Parameter

exclude — The time range will not take effect on holiday.

include — The time range will take effect on holiday.

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a time-range entry named "tRange3" and configure time-range to exclude the holiday:

```
Switch(config)#time-range tRange3
Switch(config-time-range)#holiday exclude
```

11.5 holiday

Description

The **holiday** command is used to create holiday for the switch. To delete the corresponding holiday configuration, please use **no holiday** command.

Syntax

holiday *name* **start-date** *start-date* **end-date** *end-date*

no holiday *name*

Parameter

name — The holiday name, ranging from 1 to 16 characters.

start-date — The start date of the holiday, in the format of MM/DD, for instance, 05/01.

end-date — The end date of the holiday, in the format of MM/DD, for instance, 05/01.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a holiday named "holiday1" and configure the start date as October 1st and the end date as October 3rd:

```
Switch(config)# holiday holiday1 start-date 10/01 end-date 10/03
```

11.6 show holiday

Description

The **show holiday** command is used to display the defined holiday.

Syntax

show holiday

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined holiday:

```
Switch# show holiday
```

11.7 show time-range

Description

The **show time-range** command is used to display the defined time-range.

Syntax

```
show time-range [ time-range-name ]
```

Parameter

time-range-name—— Specify the time range name with 1 to 16 characters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined time-range:

```
Switch# show time-range
```

Chapter 12 Interface Configuration Commands

Ethernet Configuration Commands can be used to configure the Bandwidth Control, Negotiation Mode and Storm Control for Ethernet ports.

12.1 interface

Description

The **interface** command is used to enter the Interface Configuration Mode and configure the corresponding port.

Syntax

interface *fastEthernet / gigabitEthernet / two-gigabitEthernet / ten-gigabitEthernet* *port*

Parameter

fastEthernet port—— The 100M Ethernet port number.

gigabitEthernet port—— The Gigabit Ethernet port number.

ten-gigabitEthernet port—— The 10-Gigabit Ethernet port number.

two-gigabitEthernet port—— The 2.5-Gigabit Ethernet port number.

port-channel num—— The Ethernet channel number.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

To enter the Interface gigabitEthernet Configuration Mode and configure port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
```

12.2 interface range

Description

The **interface range** command is used to enter the interface range Configuration Mode and configure multiple Ethernet ports at the same time.

Syntax

interface range fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet *port-list*

Parameter

fastEthernet port—— The 100M Ethernet port number.

gigabitEthernet port—— The Gigabit Ethernet port number.

ten-gigabitEthernet port—— The 10-Gigabit Ethernet port number.

two-gigabitEthernet port —— The 2.5-Gigabit Ethernet port number.

port-list—— The list of Ethernet ports.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Command in the **Interface Range gigabitEthernet** Mode is executed independently on all ports in the range. It does not affect the execution on the other ports at all if the command results in an error on one port.

Example

To enter the Interface range gigabitEthernet Configuration Mode, and configure ports 1, 2, 3, 6, 7 and 9 at the same time by adding them to one port-list:

```
Switch(config)# interface range gigabitEthernet 1/0/1-3,1/0/6-7,1/0/9
```

12.3 description

Description

The **description** command is used to add a description to the Ethernet port. To clear the description of the corresponding port, please use **no description** command.

Syntax

description *string*
no description

Parameter

string—— Content of a port description, ranging from 1 to 16 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a description Port_5 to port 1/0/5:

```
Switch(config)# interface gigabitEthernet 1/0/5  
Switch(config-if)# description Port_5
```

12.4 shutdown

Description

The **shutdown** command is used to disable an Ethernet port. To enable this port again, please use **no shutdown** command.

Syntax

shutdown
no shutdown

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# shutdown
```

12.5 flow-control

Description

The **flow-control** command is used to enable the flow-control function for a port. To disable the flow-control function for this corresponding port, please use **no flow-control** command. With the flow-control function enabled, the Ingress Rate and Egress Rate can be synchronized to avoid packet loss in the network.

Syntax

flow-control

no flow-control

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the flow-control function for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# flow-control
```

12.6 duplex

Description

The **duplex** command is used to configure the Duplex Mode for an Ethernet port. To return to the default configuration, please use **no duplex** command.

Syntax

duplex { auto | full | half }

no duplex

Parameter

auto | full | half — The duplex mode of the Ethernet port. There are three options: auto-negotiation mode, full-duplex mode and half-duplex mode. By default, the Gigabit Ethernet port is auto-negotiation mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the Duplex Mode as full-duplex for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
```

```
Switch(config-if)# duplex full
```

12.7 jumbo-size

Description

The **jumbo-size** command is used to specify the size of jumbo frames.

Syntax

jumbo-size *size*

Parameter

size — The value of jumbo frames. It ranges from 1518 to 9216 bytes, and the default is 1518 bytes.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Globally configure the size of jumbo frames as 9216:

```
Switch(config)# jumbo-size 9216
```

12.8 speed

Description

The **speed** command is used to configure the Speed Mode for an Ethernet port. To return to the default configuration, please use **no speed** command.

Syntax

speed { 10 | 100 | 1000 | 2500 | 5000 | 10000 | auto }

no speed

Parameter

10 | 100 | 1000 | 2500 | 5000 | 10000 | auto — The speed mode of the Ethernet port. There are seven options: 10Mbps, 100Mbps, 1000Mbps, 2500Mbps, 5000Mbps, 10000Mbps and Auto negotiation mode (default).

Command Mode

Interface Configuration Mode (interface fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet / interface range fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the Speed Mode as 100Mbps for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
```

```
Switch(config-if)# speed 100
```

12.9 clear counters

Description

The **clear counters** command is used to clear the statistics information of all the Ethernet ports and port channels.

Syntax

```
clear counters  
clear counters interface [ fastEthernet | gigabitEthernet |  
two-gigabitEthernet | ten-gigabitEthernet port] [ port-channel  
port-channel-id]
```

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Clear the statistic information of all ports and port channels:

```
Switch(config)# clear counters
```

12.10 mtu

Description

The **mtu** command is used to configure the MTU on an interface to limit the maximum size of IP packets forwarded on the interface. The configurable range is from 512 to the currently configured jumbo-size. A maximum of six custom MTU configurations are allowed system-wide. To restore to the default setting, please use **no mtu** command.

Syntax

```
mtu mtu-value
```

Parameter

mtu-value—— MTU value for the interface. Valid values are 512 to the currently configured jumbo-size.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the MTU to 1024:

```
Switch(config-if)# mtu 1024
```

12.11 ipv6 gateway

Description

The **ipv6 gateway** command is used to manually configure the IPv6 gateway address on an interface. To restore to the default setting, please use **no ipv6 gateway** command.

Syntax

ipv6 gateway *gateway-address*

no ipv6 gateway *gateway-address*

Parameter

gateway-address —— IPv6 gateway address.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the interface gateway to 2000::1:

```
Switch (config-if)# ipv6 gateway 2000::1
```

12.12 ipv6 dnsDynamic

Description

The **ipv6 dnsDynamic** command is used to enable dynamic IPv6 DNS acquisition on an interface. When enabled, the interface can learn IPv6 DNS

server information from RA messages or DHCPv6. To disable this feature, please use **no ipv6 dnsDynamic** command.

Syntax

ipv6 dnsDynamic

no ipv6 dnsDynamic

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable dynamic DNS on the interface:

```
Switch(config-if)# ipv6 dnsDynamic
```

12.13 show fiber-ports



Note: This command is only available on certain devices.

Description

The **show fiber-ports** command is used to display the information of all optical modules.

Syntax

show fiber-ports

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all fiber ports:

```
Switch(config)# show fiber-ports
```

12.14 show interface status

Description

The **show interface status** command is used to display the connection status of the Ethernet port/port channel.

Syntax

```
show interface status [ fastEthernet port] [ gigabitEthernet port]  
[ two-gigabitEthernet port] [ ten-gigabitEthernet port] [ port-channel  
port-channel-id]
```

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel..

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the connection status of all ports and port channels:

```
Switch(config)# show interface status
```

Display the connection status of port 1/0/1:

```
Switch(config)# show interface status gigabitEthernet 1/0/1
```

12.15 show interface counters

Description

The **show interface counters** command is used to display the statistics information of all ports/port channels.

Syntax

```
show interface counters [ fastEthernet | gigabitEthernet |  
two-gigabitEthernet | ten-gigabitEthernet port] [ port-channel  
port-channel-id]
```

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics information of all Ethernet ports and port channels:

```
Switch(config)# show interface counters
```

Display the statistics information of port 1/0/2:

```
Switch(config)# show interface counters gigabitEthernet 1/0/2
```

12.16 show interface configuration

Description

The **show interface configuration** command is used to display the configurations of all ports and port channels, including Port-status, Flow Control, Negotiation Mode and Port-description.

Syntax

```
show interface configuration [ fastEthernet | gigabitEthernet |  
two-gigabitEthernet | ten-gigabitEthernet port] [ port-channel  
port-channel-id]
```

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of all Ethernet ports and port channels:

```
Switch(config)# show interface configuration
```

Display the configurations of port 1/0/2:

```
Switch(config)# show interface configuration gigabitEthernet 1/0/2
```


12.17 show onvif ipc-classify

Description

The **show onvif ipc-classify** command is used to display whether a port is in a direct connection state (has only learned one MAC address), the current traffic identification status, and traffic identification results. The identification results are used to indicate whether the device connected to the port is an IPC. There are two possible displays for the result (IPC and Other).

Syntax

show onvif ipc-classify

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the current port traffic identification results:

```
Switch(config)# show onvif ipc-classify
```

Chapter 13 Port Isolation Commands

Port Isolation provides a method of restricting traffic flow to improve the network security by forbidding the port to forward packets to the ports that are not on its forwarding port list.

13.1 port isolation

Description

The **port isolation** command is used to configure the forward port/port channel list of a port/port channel, so that this port/port channel can only communicate with the ports/port channels on its list. To delete the corresponding configuration, please use **no port isolation** command.

Syntax

```
port isolation { [fa-forward-list fa-forward-list] [gi-forward-list gi-forward-list] [tw-forward-list tw-forward-list] [te-forward-list te-forward-list] } [po-forward-list po-forward-list]
```

```
no port isolation
```

Parameter

fa-forward-list / *gi-forward-list* / *tw-forward-list* / *te-forward-list* — The list of Ethernet ports.

po-forward-list — The list of port channels.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set port 1, 2, 4 and port channel 2 to the forward list of port 1/0/5:

```
Switch(config)# interface gigabitEthernet 1/0/5
Switch(config-if)# port isolation gi-forward-list 1/0/1-2,1/0/4
po-forward-list 2
```

Set all Ethernet ports and port channels to forward list of port 1/0/2, namely restore to the default setting:

```
Switch(config)# interface gigabitEthernet 1/0/2
```

13.2 show port isolation interface

Description

The **show port isolation interface** command is used to display the forward port list of a port/port channel.

Syntax

```
show port isolation interface [fastEthernet port| gigabitEthernet port|  
two-gigabitEthernet port| ten-gigabitEthernet port| port-channel  
port-channel-id]
```

Parameter

port — The number of Ethernet port you want to show its forward port list, in the format of 1/0/2.

port-channel-id — The ID of port channel you want to show its forward port list, ranging from 1 to 6.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the forward-list of port 1/0/2:

```
Switch# show port isolation interface gigabitEthernet 1/0/2
```

Display the forward-list of all Ethernet ports and port channels:

```
Switch# show port isolation interface
```

Chapter 14 Loopback Detection Commands

With loopback detection feature enabled, the switch can detect loops using loopback detection packets. When a loop is detected, the switch will display an alert or further block the corresponding port according to the configuration.

14.1 loopback-detection (global)

Description

The **loopback-detection** command is used to enable the loopback detection function globally. To disable it, please use **no loopback detection** command.

Syntax

loopback-detection
no loopback-detection

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the loopback detection function globally:

```
Switch(config)# loopback-detection
```

14.2 loopback-detection interval

Description

The **loopback-detection interval** command is used to define the interval of sending loopback detection packets from switch ports to network, aiming at detecting network loops periodically.

Syntax

loopback-detection interval *interval-time*

Parameter

interval-time—— The interval of sending loopback detection packets. It ranges from 1 to 1000 seconds. By default, this value is 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the interval-time as 50 seconds:

```
Switch(config)# loopback-detection interval 50
```

14.3 loopback-detection recovery-time

Description

The **loopback-detection recovery-time** command is used to configure the time after which the blocked port would automatically recover to normal status.

Syntax

loopback-detection recovery-time *recovery-time*

Parameter

recovery-time — The time after which the blocked port would automatically recover to normal status, and the loopback detection would restart. It ranges from 2 to 1000000 seconds. By default, this value is 90.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the recovery-time as 70 seconds:

```
Switch(config)# loopback-detection recovery-time 70
```

14.4 loopback-detection (interface)

Description

The **loopback-detection** command is used to enable the loopback detection function of the specified port. To disable it, please use **no loopback-detection** command.

Syntax

loopback-detection
no loopback-detection

Command Mode

Interface Configuration Mode (interface fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet / interface range fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the loopback detection function of ports 1-3:

```
Switch(config)# interface range gigabitEthernet 1/0/1-3
Switch(Config-if-range)# loopback-detection
```

14.5 loopback-detection config process-mode

Description

The **loopback-detection config process-mode** command is used to configure the process-mode for the ports by which the switch copes with the detected loops. You also need to configure the recovery mode to remove the block status of the port or VLAN when the process-mode is Port Based or VLAN Based.

Syntax

```
loopback-detection config process-mode { alert | port-based | vlan-based }  
recovery-mode { auto | manual }
```

Parameter

alert — When a loop is detected, the switch will send a trap message and generate an entry on the log file. It is the default setting.

port-based — When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the port on which the loop is detected and no packets can pass through the port.

vlan-based — When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the VLAN in which the loop is detected and only the packets of the blocked VLAN cannot pass through the port.

auto — Block status can be automatically removed after recovery time.

manual — Block status can only be removed manually.

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the loopback detection process-mode as port-based, and configure the recovery mode as manual for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2  
Switch(config-if)# loopback-detection config process-mode port-based  
recovery-mode manual
```

14.6 loopback-detection recover

Description

The **loopback-detection recover** command is used to remove the block status of selected ports, recovering the blocked ports to normal status,

Syntax

loopback-detection recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Recover the blocked port 1/0/2 to normal status:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# loopback-detection recover
```

14.7 show loopback-detection global

Description

The **show loopback-detection global** command is used to display the global configuration of loopback detection function such as loopback detection global status, loopback detection interval and loopback detection recovery time.

Syntax

show loopback-detection global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of loopback detection function:

```
Switch# show loopback-detection global
```


14.8 show loopback-detection interface

Description

The **show loopback-detection interface** command is used to display the configuration of loopback detection function and the status of the specified Ethernet port.

Syntax

```
show loopback-detection interface [ fastEthernet port | gigabitEthernet port | two-gigabitEthernet port | ten-gigabitEthernet port | port-channel lagid ] [ detail ]
```

Parameter

port — The Ethernet port number.

lagid — The number of LAG, ranging from 1 to 14.

detail — Displays the loop status and block status of the VLAN which the specified port belongs to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of loopback detection function and the status of all ports:

```
Switch# show loopback-detection interface
```

Display the configuration of loopback detection function and the status of port 5:

```
Switch# show loopback-detection interface gigabitEthernet 1/0/5
```

Chapter 15 Stack Commands (Only for Certain Devices)

Stack is a device virtualization technology that connects two and above switches supporting stack features via cables through their stack ports, which logically virtualize them to one device as a whole to forward data in the network in Layer 2 and Layer 3 protocols. Through this feature, switches can be stacked to improve reliability, expand port numbers, increase bandwidth, simplify networking, and etc.

In a stack system, the switches can be categorized mainly into two roles: Master Switch and Member Switch. The master switch manages and controls devices in the whole stack system while the member switch only forwards data as a standby device of the master switch.

As the following figure shows, the switches are connected to form a stack which works as a unified system that enables multiple devices to collaborate under the management of the master switch as a whole.

15.1 switch stack-group

Description

The **switch stack-group** command is used to access the viewing page of a specified stack port group configuration of the specified device.

Syntax

switch {*unitid*} stack-group {*groupid*}

Parameter

unitid—— Device ID in the stack system, ranging from 1-8.

groupid—— ID of the stack port group, ranging from 1-12.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enter the viewing page of a stack port group 1 on switch 1:

```
Switch(config)#switch 1 stack-group 1
```

15.2 group-info

Description

The **group-info** command is used to view the specified stack port group configuration of the specified device.

Syntax

group-info

Parameter

group-info — Display the information of the stack group.

Command Mode

Stack-Group Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the information of the stack port group 1 on switch 2.

```
Switch(config)# switch 2 stack-group 1
```

```
Switch(stack-group)#group-info
```

15.3 interface port

Description

The **interface port** command is used to enable the stack function for a specified slot. To disable this function, please use the **no interface port** command.

Syntax

interface *port*

no interface *port*

Parameter

port — Port which the stack function to be enabled/disabled on

Command Mode

Stack-Group Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure 2/0/28 as a stack port and join stack-group 1 of unit 2:

```
Switch(config)# switch 2 stack-group 1
Switch(stack-group)# interface 2/0/28
```

15.4 switch priority

Description

The **switch priority** command is used to configure the stack priority of the device with specified unit ID.

Syntax

switch {*unitid*} priority {*priority*}

Parameter

unitid—— Device ID in the stack system, ranging from 1 to 8.

Priority—— Stack priority. The higher the priority, the more likely the device is to become the master device. The value ranges from 1 to 255.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the stack priority of unit 1 as 5:

```
Switch(config)#switch 1 priority 5
```

15.5 switch renumber

Description

The **switch renumber** command is used to modify the stack unit ID of a specified device, which will take effect after the switch reboots.

Syntax

switch {*unitid*} renumber {*new-unitid*}

Parameter

unitid—— ID in the stack system, ranging from 1 to 8.

new-unitid—— New device ID to be configured, ranging from 1 to 12.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Renumber the stack unit ID of unit 1 as 2:

```
Switch(config)# switch 1 renumber 2
```

```
WARNING: Changing the Unit number may result in a configuration change for  
that unit. The interface configuration associated with the old unit number will  
remain as a provisioned configuration. Do you want to continue?[Y/N] y
```

```
Changing Unit Number 1 to Unid Number 1. New Unit Number will be effective  
after next reboot
```

15.6 switch provision

Description

The **switch provision** command is used to create a preconfigured entry specifying unitid and device-type. After creation, you can use other configuration commands to configure the unit. The configuration will take effect after the stack is connected. To delete the entry, please use the **no switch provision** command.

Syntax

```
switch {unitid} provision {device-type}
```

```
no switch {unitid} provision {device-type}
```

Parameter

unitid—— Unit ID. Valid values are 1 to 8.

device-type—— Device type. The provision device needs to be of the same type as the connected device.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure provision entries:

```
Switch(config)#switch 1 provision 3
```

15.7 switch mac-delay

Description

The **switch mac-delay** command is used to enable or disable the virtual MAC feature. To disable this feature, please use the parameter "immediately".

Syntax

```
switch mac-delay { delay-time | immediately }
```

Parameter

delay-time: The delay time for virtual MAC switching(in minutes), ranging from 0-60 minutes. 0 indicates never switching the stack MAC. The default value is 10 minutes. If the original master switch in the stacking system temporarily leaves and returns within the switching time, the stack MAC address will not change. However, if the master switch does not return to the stacking system within the switching time, the stacking system will use the MAC address of the current master switch as the new MAC address.

immediately: When the stacking system changes, the stacking system MAC changes immediately, that is, the virtual MAC feature is not enabled.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the virtual MAC switching time to 5 minutes:

```
Switch(config)# switch mac-delay 5
```

15.8 switch mad enable

Description

The **switch mad enable** command is used to enable Multi-Active Detection (MAD) globally. MAD is a protocol for detecting and handling stack splits, primarily used in stack systems to monitor operational status, detect stack splits, resolve conflicts, and recover from faults, thereby minimizing service disruption. It is a sub-feature of the stacking module, with configuration and display commands located under the stacking module.

When the management channel of a stack system fails, the stack splits. The original logical device divides into multiple devices, which may retain identical system parameters and cause conflicts. To prevent this, split devices will "self-terminate" by erroring down all service ports except stacking member ports, reserved ports, and MAD-configured ports.

Syntax

switch mad enable

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MAD globally:

```
Switch(config)# switch mad enable
```

15.9 switch mad disable

Description

The **switch mad disable** command is used to disable MAD globally. The retain-config parameter preserves MAD-related configurations while disabling the feature.

Syntax

switch mad disable { retain-config }

Parameter

retain-config — Disables MAD but retains all related configurations.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MAD globally:

```
Switch(config)# switch mad disable
```

15.10 switch mad restore



Note: After the Recovery state switch is enabled, multiple hosts may be discovered again in the network. Please ensure that the switch in Detect status has also failed or been removed from the network, or that you are restoring the network.

Description

The **switch mad restore** command is used to restore a stack system in recovery state by re-enabling error-down ports.

Syntax

switch mad restore

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Restore a stack system in recovery state by re-enabling error-down ports:

```
Switch(config)# switch mad restore
```


15.11 switch mad detect mode direct interface

Description

The **switch mad detect mode direct interface** command is used to configure direct ports for MAD detection. MAD ports are blocked and cannot carry service traffic.

Syntax

switch mad detect mode direct interface { *portList* }

no switch mad detect mode direct interface

Parameter

portList—— Physical ports of the switch, e.g. (1/0/1-2, 2/0/1). The MAD port will be blocked and services cannot be performed. Please avoid performing other configurations on this port. The LAG port cannot be configured and is mutually exclusive with the stack port. That is, the stack port cannot be configured as a MAD port, and the MAD port cannot be configured as a stack port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure port 1/0/1 for MAD detection:

```
Switch(config)# switch mad detect mode direct interface 1/0/1
```

15.12 switch mac-delay show

Description

The **switch mac-delay show** command is used to display the MAC-delay switching time of the current stacking system.

Syntax

switch mac-delay show

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the MAC-delay switching time of the current stacking system:

```
Switch# switch mac-delay show
```

15.13 show switch mad detail

Description

The **show switch mad detail** command is used to display the relevant configuration of the MAD function and the current status of the switch.

Syntax

```
show switch mad detail
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the relevant configuration of the MAD function and the current status of the switch:

```
Switch# show switch mad detail
```

15.14 show switch stack-ports

Description

The **show switch stack-ports** command is used to display the stack port information of all members of the stack group.

Syntax

```
show switch stack-ports
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the stack port information of all members of the stack group:

```
Switch#show switch stack-ports
```

15.15 show switch

Description

The **show switch** command is used to display the information of all devices in the stack system.

Syntax

```
show switch [ unit-id ]
```

Parameter

unitid: Device ID in the stack system, ranging from 1 to 8.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the information of member switch 2:

```
Switch#show switch 2
```

15.16 show switch neighbors

Description

The **show switch neighbors** command is used to display the group ID of the stack port and the unit ID of its neighboring member device in the current stack system.

Syntax

```
show switch neighbors
```

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the unit ID of the current stack system:

```
Switch#show switch neighbors
```

Chapter 16 DDM Commands (Only for Certain Devices)



Note: DDM commands are only available on certain devices.

The DDM (Digital Diagnostic Monitoring) function allows the user to monitor the status of the SFP modules inserted into the SFP ports on the switch. The user can choose to shut down the monitoring SFP port automatically when specified parameter exceeds the alarm threshold or warning threshold. The monitoring parameters include: Temperature, Voltage, Bias Current, Tx Power and Rx Power.

16.1 ddm state enable

Description

The **ddm state enable** command is used to enable the DDM function on the specified SFP port.

Use the **no ddm state enable** command to disable the DDM function on this port.

Syntax

ddm state enable

no ddm state enable

Default Setting

Enabled on all the SFP ports.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Enable DDM function on port 1/0/25:

```
Switch(config)#interface gigabitEthernet 1/0/25
```

```
Switch(config-if)#ddm state enable
```

16.2 ddm shutdown

Description

The **ddm shutdown** command is used to configure whether to shut down the port when an exceeding alarm threshold or warning threshold event is encountered.

Syntax

ddm shutdown { none | warning | alarm }

Parameter

none — The port will never be shut down regardless of the exceeding alarm threshold and warning threshold events.

warning — Shut down the port when an exceeding warning threshold event is encountered.

alarm — Shut down the port when an exceeding alarm threshold event is encountered.

Default Setting

none, which means the port will never be shut down regardless of the exceeding alarm threshold and warning threshold events.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Shut down the port 1/0/25 when an exceeding warning threshold event is encountered:

```
Switch(config)#interface gigabitEthernet 1/0/25
```

```
Switch(config-if)#ddm shutdown warning
```

16.3 ddm temperature_threshold

Description

The **ddm temperature_threshold** command is used to configure the threshold of the DDM temperature value.

Syntax

ddm temperature_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in Celsius.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM temperature on the port 1/0/25 as 5:

```
Switch(config)#interface gigabitEthernet 1/0/25
Switch(config-if)#ddm temperature_threshold high_alarm 5
```

16.4 ddm voltage_threshold

Description

The **ddm voltage_threshold** command is used to configure the threshold of the DDM voltage value.

Syntax

ddm voltage_threshold { high_alarm | high_warning | low_alarm |
low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value—— Enter the threshold value in Volt.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM voltage on the port 1/0/25 as 5:

```
Switch(config)#interface gigabitEthernet 1/0/25
Switch(config-if)#ddm voltage_threshold high_alarm 5
```

16.5 ddm

bias_current_threshold

Description

The **ddm bias_current_threshold** command is used to configure the threshold of the DDM Bias Current value.

Syntax

ddm bias_current_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm — Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning — Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm — Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning — Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value — Enter the threshold value in mA.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Bias Current on the port 1/0/25 as 5:

```
Switch(config)#interface gigabitEthernet 1/0/25
Switch(config-if)#ddm bias_current_threshold high_alarm 5
```

16.6 ddm tx_power_threshold

Description

The **ddm tx_power_threshold** command is used to configure the threshold of the DDM Tx Power value.

Syntax

```
ddm tx_power_threshold { high_alarm | high_warning | low_alarm |  
low_warning } value
```

Parameter

high_alarm — Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning — Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm — Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning — Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value — Enter the threshold value in mW.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Tx Power on the port 1/0/25 as 5:

```
Switch(config)#interface gigabitEthernet 1/0/25  
Switch(config-if)#ddm tx_power_threshold high_alarm 5
```

16.7 ddm rx_power_threshold

Description

The **ddm rx_power_threshold** command is used to configure the threshold of the DDM Rx Power value.

Syntax

```
ddm rx_power_threshold { high_alarm | high_warning | low_alarm |  
low_warning } value
```

Parameter

high_alarm — Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning — Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm — Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning — Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value — Enter the threshold value in mW.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Rx Power on the port 1/0/25 as 5:

```
Switch(config)#interface gigabitEthernet 1/0/25
Switch(config-if)#ddm rx_power_threshold high_alarm 5
```

16.8 show ddm configuration

Description

The **show ddm configuration** command is used to display the DDM configuration.

Syntax

```
show ddm configuration { state | temperature | voltage | bias_current |  
tx_power | rx_power | tx_rx_power }
```

Parameter

state — Display the DDM configuration state.

temperature — Displays the threshold of the DDM temperature value.

voltage — Displays the threshold of the DDM Voltage value.

bias_current — Displays the threshold of the DDM Bias Current value.

tx_power — Displays the threshold of the DDM Tx Power value.

rx_power — Displays the threshold of the DDM Rx Power value.

tx_rx_power — Displays the threshold of the DDM Tx and Rx Power value.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

View the DDM configuration state:

```
Switch(config)#show ddm configuration state
```

View the threshold of the DDM Voltage value:

```
Switch(config)#show ddm configuration voltage
```

16.9 show ddm status

Description

The **show ddm status** command is used to display the DDM status, which is the digital diagnostic monitoring status of SFP modules inserting into the switch's SFP ports.

Syntax

show ddm status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

View the DDM status:

```
Switch(config)#show ddm status
```

16.10 show fiber-ports



Note: This command is only available on certain devices.

Description

The **show fiber-ports** command is used to display the information of all fiber ports.

Syntax

show fiber-ports

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all fiber ports:

```
Switch(config)# show fiber-ports
```

Chapter 17 Etherchannel Commands

Etherchannel Commands are used to configure LAG and LACP function.

LAG (Link Aggregation Group) is to combine a number of ports together to make a single high-bandwidth data path, which can highly extend the bandwidth. The bandwidth of the LAG is the sum of bandwidth of its member port.

LACP (Link Aggregation Control Protocol) is defined in IEEE802.3ad and enables the dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. The switch can dynamically group similarly configured ports into a single logical link, which will highly extend the bandwidth and flexibly balance the load.

17.1 channel-group

Description

The **channel-group** command is used to add a port to the EtherChannel Group and configure its mode. To delete the port from the EtherChannel Group, please use **no channel-group** command.

Syntax

channel-group *num* **mode** { on | active | passive }

no channel-group

Parameter

num — The number of the EtherChannel Group, which ranges from 1 to 8 for L2/L2+ switches, 1 to 64 for L3 access switches, and 1 to 120 for L3 aggregation switches.

on — Enable the static LAG.

active — Enable the active LACP mode.

passive — Enable the passive LACP mode.

Command Mode

Interface Configuration Mode (interface fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet / interface range fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add ports 2-4 to EtherChannel Group 1 and enable the static LAG:

```
Switch(config)# interface range gigabitEthernet 1/0/2-4
```

```
Switch(config-if-range)# channel-group 1 mode on
```

17.2 port-channel load-balance

Description

The **port-channel load-balance** command is used to configure the Aggregate Arithmetic for LAG. To return to the default configurations, please use **no port-channel load-balance** command.

Syntax

```
port-channel load-balance { src-mac | dst-mac | src-dst-mac | src-ip | dst-ip |  
src-dst-ip }
```

```
no port-channel load-balance
```

Parameter

src-mac — The source MAC address. When this option is selected, the Aggregate Arithmetic will be based on the source MAC address of the packets.

dst-mac — The destination MAC address. When this option is selected, the Aggregate Arithmetic will be based on the destination MAC address of the packets.

src-dst-mac — The source and destination MAC address. When this option is selected, the Aggregate Arithmetic will be based on the source and destination MAC addresses of the packets. The Aggregate Arithmetic for LAG is "src-dst-mac" by default.

src-ip — The source IP address. When this option is selected, the Aggregate Arithmetic will be based on the source IP address of the packets.

dst-ip — The destination IP address. When this option is selected, the Aggregate Arithmetic will be based on the destination IP address of the packets.

src-dst-ip — The source and destination IP address. When this option is selected, the Aggregate Arithmetic will be based on the source and destination IP addresses of the packets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Aggregate Arithmetic for LAG as "src-dst-ip":

```
Switch(config)# port-channel load-balance src-dst-ip
```

17.3 lacp system-priority

Description

The **lacp system-priority** command is used to configure the LACP system priority globally. To return to the default configurations, please use **no lacp system-priority** command.

Syntax

lacp system-priority *pri*

no lacp system-priority

Parameter

pri — The system priority, ranging from 0 to 65535. It is 32768 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the LACP system priority as 1024 globally:

```
Switch(config)# lacp system-priority 1024
```


17.4 lacp port-priority

Description

The **lacp port-priority** command is used to configure the LACP port priority for specified ports. To return to the default configurations, please use **no lacp port-priority** command.

Syntax

```
lacp port-priority pri  
no lacp port-priority
```

Parameter

pri—— The port priority, ranging from 0 to 65535. It is 32768 by default.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the LACP port priority as 1024 for ports 1-3:

```
Switch(config)# interface range gigabitEthernet 1/0/1-3  
Switch(config-if-range)# lacp port-priority 1024
```

Configure the LACP port priority as 2048 for port 4:

```
Switch(config)# interface gigabitEthernet 1/0/4  
Switch(config-if)# lacp port-priority 2048
```

17.5 lacp timeout

Description

The **lacp timeout** command is used to modify the LACP keepalive packet timeout period for all ports or selected ports. It will overwrite any existing configuration based on the order of application. The default value is long. For this configuration to affect the keepalive packet transmission interval of the

peer device, at least one of the two aggregated devices must be operating in LACP Active mode. To restore the default value, please use the **no lacp timeout** command.

Syntax

lacp timeout {*long* / *short*}

no lacp timeout

Parameter

long / *short*—— The LACP keepalive packet timeout control value for all or selected ports on this device. long specifies a long timeout, short specifies a short timeout.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

This option can only be configured on ports where LACP is enabled, and it will be visible under the corresponding interface section in show running-config.

If the port is removed from an LACP group or converted to a static LAG member port after a timeout type is configured, its timeout type will revert to the default.

If batch configuration is performed via interface range, the configuration will only be applied to ports that have LACP enabled.

Additionally, this option cannot be configured within the Port-channel view; attempting to do so will result in an error.

Example

Configure the LACP keepalive packet timeout period to short on interface GE1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
```

```
Switch(config-if)# lacp timeout short
```

Restore the LACP keepalive packet timeout period to the default value (long) on interface GE1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
```

```
Switch(config-if)# no lacp timeout
```

17.6 show etherchannel

Description

The **show etherchannel** command is used to display the EtherChannel information.

Syntax

```
show etherchannel [ channel-group-num ] { detail | summary }
```

Parameter

channel-group-num — The EtherChannel Group number, which ranges from 1 to 8 for L2/L2+ switches, 1 to 64 for L3 access switches, and 1 to 120 for L3 aggregation switches. By default, it is empty, and will display the information of all EtherChannel Groups.

detail — The detailed information of EtherChannel.

summary — The EtherChannel information in summary.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the detailed information of EtherChannel Group 1:

```
Switch(config)# show etherchannel 1 detail
```

17.7 show etherchannel load-balance

Description

The **show etherchannel load-balance** command is used to display the Aggregate Arithmetic of LAG.

Syntax

```
show etherchannel load-balance
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Aggregate Arithmetic of LAG:

```
Switch(config)# show etherchannel load-balance
```

17.8 show lacp

Description

The **show lacp** command is used to display the LACP information for a specified EtherChannel Group.

Syntax

```
show lacp [ channel-group-num ] { internal / neighbor }
```

Parameter

channel-group-num — The EtherChannel Group number, which ranges from 1 to 8 for L2/L2+ switches, 1 to 64 for L3 access switches, and 1 to 120 for L3 aggregation switches. By default, it is empty, and will display the information of all LACP groups.

internal — The internal LACP information.

neighbor — The neighbor LACP information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the internal LACP information of EtherChannel Group 1:

```
Switch(config)# show lacp 1 internal
```

17.9 show lacp sys-id

Description

The **show lacp sys-id** command is used to display the LACP system priority globally.

Syntax

show lacp sys-id

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LACP system priority:

```
Switch(config)# show lacp sys-id
```

Chapter 18 MLAG Commands (Only for Certain Devices)

MLAG (Multi-Chassis Link Aggregation) enables two network switches to act as a single logical entity, bonding their physical links into a shared aggregated connection. This setup enhances redundancy and bandwidth while preventing traffic disruption if one switch fails. Commonly used in data centers, MLAG ensures seamless failover, simplifies network management, and avoids single points of failure without requiring complex protocols like stacking.

18.1 mlag enable

Description

The **mlag enable** command is used to enable and configure the MLAG domain name.

Syntax

mlag enable {*domainName*}

Parameter

domainName — The MLAG group domain name, *domainName*, is used to uniquely identify an MLAG system. An MLAG system can only be established between two devices if they share the same *domainName*. The allowed range for this parameter is a string of 1 to 31 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MLAG and configure the domain name as 1:

```
Switch(config)# mlag enable 1
```

18.2 mlag disable

Description

The **mlag disable** command is used to disable the MLAG function.

Syntax

mlag disable *retain-mlag-config*

Parameter

retain-mlag-config—— Indicates whether to retain MLAG-related configurations. If the retain-mlag-config parameter is specified, existing MLAG parameters will be preserved; otherwise, all MLAG-related configurations will be cleared, including MLAG member ports (while aggregation groups will remain intact). By default, configurations will not be retained.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the MLAG function:

```
Switch(config)# mlag disable
```

18.3 interface

Description

The **interface** command is used to configure the peer-link port for the internal control link of MLAG.

Syntax

interface *{peer-link-port}*

Parameter

peer-link-port—— Specifies the peer-link port list. Only the highest-rate optical ports are allowed to be configured as peer-links. Multiple ports can be configured to form a peer-link group when specified collectively.

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the peer-link port of 1/0/29-30:

```
Switch(config)#mlag domain 1
Switch(mlag-domain)#interface 1/0/29-30
```

18.4 priority

Description

The **priority** command is used to configure the device's priority during MLAG pairing. A higher priority increases the likelihood of becoming the primary device.

Syntax

priority {*priority*}

Parameter

priority—— The priority value. The default is 5, with a higher value being more likely to become the primary device. The valid range is 1 to 255.

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the device's priority as 100:


```
Switch(config)#mlag domain 1
Switch(mlag-domain)# priority 100
```

18.5 dad interface

Description

The **dad interface** command is used to configure the DAD interface.

Syntax

```
dad interface {dadInterface}
```

Parameter

dadInterface—— MLAG dual-primary detection interface. Only one physical port can be configured as the dad-interface. To replace the existing configuration, you must first delete the existing configuration before adding a new one.

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DAD interface 1/0/29:

```
Switch(config)#mlag domain 1
Switch(mlag-domain)# dad interface 1/0/29
```

18.6 dad param

Description

The **dad param** command is used to configure DAD intercommunication parameters. The MLAG dual-active detection function operates at Layer 3, therefore IP addresses and related parameters need to be configured for this feature. Ensure DAD IP addresses between peer devices reside in the same subnet and can communicate, and avoid conflicts with other interface subnets.

Syntax

dad param peer-ip-address {*peerIpAddr*} src-ip-address {*localIpAddr*} port {*l4Port*}

Parameter

peerIpAddr—— DAD-IP address of the MLAG peer device (IPv4). Must be in the same subnet as the local DAD IP with connectivity, and must not conflict with other interface subnets.

localIpAddr—— Local DAD-IP address for this MLAG device (IPv4). Must be in the same subnet as the peer DAD IP with connectivity, and must not conflict with other interface subnets.

l4Port—— (Optional) Communication port for MLAG DAD. Valid range: 50000-60000. Default: 50000 when unconfigured.

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DAD intercommunication parameters:

```
Switch(config)#mlag domain 1
Switch(mlag-domain)# dad param peer-ip-address 192.168.2.1
src-ip-address 192.168.2.2 port 60000
```

18.7 dad tx-interval

Description

The **dad tx-interval** command is used to configure the DAD message transmission interval. Both devices in the MLAG domain must use the same value; otherwise, DAD may malfunction if one device's transmission interval is shorter than the peer's timeout duration.

Syntax

dad tx-interval {*intervalTime*}

Parameter

intervalTime—— The interval for MLAG dual-active detection messages, in milliseconds (ms). Default: 3000 ms. Configurable range: 3s to 10s (note: the interval must not exceed the DAD timeout).

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DAD message transmission interval as 3000ms:

```
Switch(config)#mlag domain 1
Switch(mlag-domain)# dad tx-interval 3000
```

18.8 dad timeout

Description

The **dad timeout** command is used to configure the DAD timeout duration. Both devices in the MLAG domain must use the same value; otherwise, DAD may malfunction if one device's transmission interval is shorter than the peer's timeout.

Syntax

dad timeout { *timeoutTime* }

Parameter

timeoutTime—— The timeout duration for MLAG dual-active detection, in milliseconds (ms). Default: 4000 ms. Configurable range: 4s to 15s (note: the message interval must not exceed the DAD timeout).

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DAD timeout duration as 4000ms:

```
Switch(config)#mlag domain 1
Switch(mlag-domain)# dad timeout 4000
```

18.9 dad enable

Description

The **dad enable** command is used to enable the DAD function. DAD-interface and DAD parameters must be fully configured before enabling DAD. To disable this function, please use the **no dad enable** command.

Syntax

dad enable
no dad enable

Parameter

None

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the DAD function

```
Switch(config)#mlag domain 1
Switch(mlag-domain)# no dad enable
```

18.10 keep-alive interval

Description

The **keep-alive interval** command is used to configure the keep-alive message interval (must be less than 1/3 of the KA timeout).

Syntax

keep-alive interval {*kaInterval*}

Parameter

kaInterval—— Keep-alive message interval, in milliseconds (ms). Default: 500 ms. Configurable range: 300 to 5000.

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the keep-alive message interval as 500ms:

```
Switch(config)#mlog domain 1
Switch(mlog-domain)# keep-alive interval 500
```

18.11 keep-alive timeout

Description

The **keep-alive timeout** command is used to configure the keep-alive timeout (must be greater than 3× the KA interval).

Syntax

keep-alive timeout {*kaTimeout*}

Parameter

kaTimeout—— Keep-alive timeout duration, in milliseconds (ms). Default: 7000 ms. Configurable range: 900 to 15000, with the timeout being at least 3× the interval.

Command Mode

MLAG-domain Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the timeout as 7000ms:

```
Switch(config)#mlag domain 1
Switch(mlag-domain)# keep-alive timeout 7000
```

18.12 mlag

Description

The **mlag** command is used to configure a regular aggregation group as an MLAG member port. Only MLAG member ports support cross-device link aggregation. MLAG systems pair identical aggregation groups (same lagid) from both devices into the same MLAG member group. To add/remove ports, use standard aggregation group commands. Use `no mlag` to revert an MLAG member group to a regular aggregation group.

Prerequisites: 1. MLAG is enabled. 2. The aggregation group is configured.

Syntax

mlag

Parameter

None

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure interface 1 as an MLAG member port:

```
Switch(config)# interface port-channel 1
Switch(mlag-domain)# mlag
```

18.13 mlag

config-consistency-check

Description

The **mlag config-consistency-check** command is used to enable MLAG configuration consistency checks. This function is enabled by default. A 120-second log silence period applies after MLAG pairing to suppress consistency alerts; users should resolve any mismatches promptly. To disable this function, use the **no mlag config-consistency-check** command. If disabled, users must manually ensure configuration consistency.

Syntax

mlag config-consistency-check
no mlag config-consistency-check

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MLAG configuration consistency checks:

```
Switch(config)# mlag config-consistency-check
```

18.14 mlag

config-consistency-check mode

Description

The **mlag config-consistency-check mode** command is used to enable the MLAG configuration consistency check feature, which is enabled by default. A 120-second alert log suppression period for consistency checks begins

immediately after MLAG pairing is completed. Users must promptly adjust configurations on both ends if inconsistencies are detected. To disable this feature, use the **mlag config-consistency-check mode** command. If the MLAG configuration consistency check is disabled, users are solely responsible for manually ensuring configuration consistency between both devices.

Syntax

mlag config-consistency-check mode

no mlag config-consistency-check mode

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# mlag config-consistency-check
```

18.15 show mlag info

Description

The **show mlag info** command is used to view the basic MLAG domain information.

Syntax

show mlag info

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the basic MLAG domain information:

```
Switch(config)# show mlag info
```

18.16 show mlag dual-active

Description

The **show mlag dual-active** command is used to view the MLAG dual-active detection details.

Syntax

```
show mlag dual-active
```

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the MLAG dual-active detection details:

```
Switch(config)# show mlag dual-active
```

18.17 show mlag keep-alive

Description

The **show mlag keep-alive** command is used to view the MLAG keep-alive heartbeat status.

Syntax

```
show mlag keep-alive
```

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the MLAG keep-alive heartbeat status:

```
Switch(config)# show mlag keep-alive
```

18.18 show mlag members-info

Description

The **show mlag members-info** command is used to view the MLAG member port details.

Syntax

```
show mlag members-info
```

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the MLAG member port details:

```
Switch(config)# show mlag members-info
```

18.19 show mlag config-consistency-check

Description

The **show mlag config-consistency-check** command is used to view the MLAG configuration consistency check status.

Syntax

show mlag config-consistency-check

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the MLAG configuration consistency check status:

```
Switch(config)# show mlag config-consistency-check
```

Chapter 19 MAC Address Commands

MAC Address configuration can improve the network security by configuring the Port Security and maintaining the address information by managing the Address Table.

19.1 mac address-table static

Description

The **mac address-table static** command is used to add the static MAC address entry. To remove the corresponding entry, please use **no mac address-table static** command. The static address can be added or removed manually, independent of the aging time. In the stable networks, the static MAC address entries can facilitate the switch to reduce broadcast packets and enhance the efficiency of packets forwarding remarkably.

Syntax

```
mac address-table static {mac-addr vid vid interface { fastEthernet port | gigabitEthernet port | two-gigabitEthernet port | ten-gigabitEthernet port | hundred-gigabitEthernet port }}
```

```
no mac address-table static { mac-addr [vid vid] | vid vid | interface { fastEthernet port | gigabitEthernet port | hundred-gigabitEthernet port | ten-gigabitEthernet port | twentyFive-gigabitEthernet port | two-gigabitEthernet port }}
```

Parameter

mac-addr——The MAC address of the entry you desire to add.

vid—— The VLAN ID number of your desired entry. It ranges from 1 to 4094.

port—— The Ethernet port number of your desired entry.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a static Mac address entry to bind the MAC address 00:02:58:4f:6c:23, VLAN1 and port 1 together:

```
Switch(config)# mac address-table static 00:02:58:4f:6c:23 vid 1 interface
gigabitEthernet 1/0/1
```

19.2 no mac address-table dynamic

Description

The **no mac address-table dynamic** command is used to delete the specified dynamic MAC address, or dynamic MAC addresses based on the VLAN or the port.

Syntax

```
no mac address-table dynamic { mac-addr | vid vid | interface {fastEthernet
port | gigabitEthernet port | two-gigabitEthernet port | ten-gigabitEthernet
port}}
```

Parameter

mac-addr——The MAC address you desire to delete.

vid——The VLAN ID on which you desire to delete MAC addresses.

port——The Ethernet port on which you desire to delete MAC addresses.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete the MAC addresses on VLAN 1:

```
Switch(config)# no mac address-table dynamic vid 1
```

19.3 mac address-table aging-time

Description

The **mac address-table aging-time** command is used to configure aging time for the dynamic address. To return to the default configuration, please use **no mac address-table aging-time** command.

Syntax

mac address-table aging-time *aging-time*

no mac address-table aging-time

Parameter

aging-time—— The aging time for the dynamic address. The value of it can be 0 or ranges from 10 to 630 seconds. When 0 is entered, the Auto Aging function is disabled. It is 300 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the aging time as 500 seconds:

```
Switch(config)# mac address-table aging-time 500
```

19.4 mac address-table filtering

Description

The **mac address-table filtering** command is used to add the filtering address entry. To delete the corresponding entry, please use **no mac address-table filtering** command. The filtering address function is to forbid the undesired package to be forwarded. The filtering address can be added or removed manually, independent of the aging time.

Syntax

mac address-table filtering *mac-addr* **vid** *vid*

no mac address-table filtering [*mac-addr*] [**vid** *vid*]

Parameter

mac-addr—— The MAC address to be filtered.

vid—— The corresponding VLAN ID of the MAC address. It ranges from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a filtering address entry of which VLAN ID is 1 and MAC address is 00:1e:4b:04:01:5d:

```
Switch(config)# mac address-table filtering 00:1e:4b:04:01:5d vid 1
```

19.5 mac address-table notification



Note: This command is only available on certain devices.

Description

The **mac address-table notification** command is used to configure global settings of MAC address table notification.

Syntax

```
mac address-table notification { [ global-status enable | disable ]  
[ table-full-status enable | disable ] [ interval time ] }
```

Parameter

global-status enable | disable — Enable/Disable the notification function globally.

table-full-status enable | disable — Enable/Disable the MAC threshold notification. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the threshold of the switch's MAC address table is reached or exceeded.

interval *time* — Specify the notification trap interval between each set of traps that are generated to the NMS. The interval ranges from 1 to 1000 seconds, and it's 1 second by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the global MAC address notification and table full notification, specify the notification sending interval as 2 seconds:

```
Switch(config)# mac address-table notification global-status enable
table-full-status enable interval 2
```

19.6 mac address-table max-mac-count

Description

The **mac address-table max-mac-count** command is used to configure the Port Security. To return to the default configurations, please use **no mac address-table max-mac-count** command. Port Security is to protect the switch from the malicious MAC address attack by limiting the maximum number of the MAC addresses that can be learned on the port. The port with Port Security feature enabled will learn the MAC address dynamically. When the learned MAC address number reaches the maximum, the port will stop learning. Therefore, the other devices with the MAC address unlearned cannot access to the network via this port.

Syntax

```
mac address-table max-mac-count { [ max-number num ] [ mode { dynamic | static | permanent } ] [ status { forward | drop | disable } ]  
[ exceed-max-learned enable | disable ] }  
no mac address-table max-mac-count [ max-number | mode | status ]
```

Parameter

num — The maximum number of MAC addresses that can be learned on the port. It ranges from 0 to 64. By default, this value is 64.

dynamic | static | permanent — Learn mode for MAC addresses. There are three modes, including Dynamic mode, Static mode and Permanent mode. When Dynamic mode is selected, the learned MAC address will be deleted automatically after the aging time. When Static mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. When permanent mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually too. However, the learned entries will be saved even the switch is rebooted.

status — Select the action to be taken when the number of the MAC addresses reaches the maximum learning number on the port. By default, this function is disabled.

- forward: The packets will be forward but not be learned when learned MAC number exceeds the maximum MAC address number on this port.
- drop: The packets will be dropped when learned MAC number exceeds the maximum MAC address number on this port.
- disable: The MAC address threshold on this port is disabled.

exceed-max-learned enable | disable — Enable/Disable the new-mac-learned notification on this port. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the port learns a new MAC address.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable Port Security function for port 1/0/1, select Static mode as the learn mode, and specify the maximum number of MAC addresses that can be learned on this port as 30. When the number of MAC address entries reaches 30 on this port, new entry will be dropped:

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# mac address-table max-mac-count max-number 30
mode static status drop
```

19.7 mac address-table notification (interface)



Note: This command is only available on certain devices.

Description

The **mac address-table notification** command is used to configure the MAC change notification on port.

Syntax

```
mac address-table notification { [ learn-mode-change enable | disable ]  
[ new-mac-learned enable | disable ] [ exceed-max-learned enable |  
disable ] }
```

Parameter

learn-mode-change enable | disable — Enable/Disable the learn-mode-change notification. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the learning mode of this port changes. To configure the learning mode configuration, please refer to [mac address-table max-mac-count](#).

new-mac-learned enable | disable — Enable/Disable the new-mac-learned notification on this port. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the port learns a new MAC address.

exceed-max-learned enable | disable — Enable/Disable the new-mac-learned notification on this port. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the port learns a new MAC address.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the learn-mode-change notification on port 1/0/2:

```
Switch(config)# mac address-table notification global-status enable  
Switch(config)# interface gigabitEthernet 1/0/2  
Switch(config-if)# mac address-table notification learn-mode-change  
enable
```

19.8 mac address-table security



Note: This command is only available on certain devices.

Description

The **mac address-table security** command is used to configure the maximum number of MAC address can be learned in specified VLANs.

Syntax

mac address-table security vid *vid* **max-learn** *number* { forward | drop }

Parameter

vid—— Specify the VLAN ID to configure its MAC address table.

number—— Configure the threshold of the MAC address table in this VLAN. It ranges from 0 to 16383.

forward | drop | disable —— Choose the mode when learned MAC number exceeds the threshold of the MAC address table in this VLAN.

- Drop: The packets will be dropped when learned MAC number exceeds the threshold of the MAC address table in this VLAN.
- Forward: The packets will be forward but not be learned when learned MAC number exceeds the threshold of the MAC address table in this VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the max learned MAC address number is VLAN 2 as 1000, and drop the packets that have no match in the MAC address table:

```
Switch(config)# mac address-table security vid 2 max-learn 1000 drop
```

19.9 mac address-table vlan-security



Note: This command is only available on certain devices.

Description

The **mac address-table security** command is used to configure the maximum number of MAC address can be learned in specified VLANs.

Syntax

mac address-table vlan-security { vid *vid* max-learn *number* | mode { forward | drop } }

Parameter

vid—— Specify the VLAN ID to configure its MAC address table.

number—— Configure the threshold of the MAC address table in this VLAN. It ranges from 0 to 16383.

forward | drop | disable —— Choose the mode when learned MAC number exceeds the threshold of the MAC address table in this VLAN.

- Drop: The packets will be dropped when learned MAC number exceeds the threshold of the MAC address table in this VLAN.

- Forward: The packets will be forward but not be learned when learned MAC number exceeds the threshold of the MAC address table in this VLAN.

- Disable: The threshold of the MAC address table is disabled.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the max learned MAC address number is VLAN 2 as 1000:

```
Switch(config)# mac address-table vlan-security vid 2 max-learn 1000
```

19.10 mac-address flapping detection



Note: This command is only available on certain devices.

Description

The **mac-address flapping detection** command is used to enable and configure MAC address flapping detection globally. When enabled, the switch tracks MAC moves within the specified aging time. If the number of MAC changes reaches the configured threshold, the switch performs the configured action. By default, MAC address flapping detection is disabled. To

disable the feature globally, please use the **no mac-address flapping detection** command.

Syntax

```
mac-address flapping { [ action { alert | port-down | vlan-quit } ] [ aging-time time ] [ detection [ { changed-time changed-time | exclude vlan-id } ] ] [ revertime revertime ] }
```

```
no mac-address flapping detection
```

Parameter

alert | *port-down* | *vlan-quit*—— Action taken when the MAC flapping count reaches changed-time within time.

- alert: Generate an alert only. (Default)
- port-down: Block the port.
- vlan-quit: Remove the port from its VLAN.

time—— Aging time for MAC flapping detection. If two MAC flapping events occur within time, the flapping counter increments by 1 and the aging timer is reset. If no flapping occurs within time, the flapping counter for the MAC entry is cleared. Valid values are 30 to 900 seconds, in multiples of 10. Default is 30 seconds.

changed-time—— Threshold for the flapping counter. When the flapping count reaches this value, MAC flapping is considered to have occurred and the configured action is triggered. Valid values are 3 to 50. Default is 10.

vlan-id—— VLAN allowlist. MAC flapping within this VLAN is not detected. Valid values are 1 to 4094.

revertime—— Recovery time after an action is triggered. After revertime, the switch restores the original state (unblocks the port or returns the port to its original VLAN). Valid values are 60 to 900 seconds, in multiples of 10. Default is 90 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MAC address flapping detection globally:

```
Switch(config)# mac-address flapping detection
```

19.11 show mac address-table

Description

The **show mac address-table** command is used to display the information of all address entries.

Syntax

show mac address-table [{ dynamic | static | filtering }]

Parameter

dynamic | static | filtering — The type of your desired entry. By default, all the entries are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all address entries:

```
Switch(config)# show mac address-table
```

19.12 show mac address-table | exclude

Description

The **show mac address-table | exclude** command is used to exclude lines containing specific information from the show mac address-table output, such as certain MAC addresses or ports.

Syntax

show mac address-table | exclude "*text*"

Parameter

text — The text to match for exclusion. Supports up to eighty matching conditions, separated by |.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Filter the show mac address-table output to exclude entries associated with ports 1/0/1 and 1/0/9:

```
Switch(config)# show mac address-table | exclude "1/0/1 |1/0/9"
```

19.13 show mac address-table | include

Description

The **show mac address-table | include** command is used to include only lines containing specific information in the show mac address-table output, such as certain MAC addresses or ports.

Syntax

```
show mac address-table | include "text"
```

Parameter

text — The text to match for inclusion. Supports up to eighty matching conditions, separated by |.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display only entries in the show mac address-table output associated with ports 1/0/1 and 1/0/9:

```
Switch(config)# show mac address-table | include "1/0/1 |1/0/9"
```

19.14 clear mac address-table

Description

The **show mac address-table** command is used to clear the specified address entries.

Syntax

```
clear mac address-table { dynamic | static | filtering }
```

Parameter

dynamic | static | filtering — The type of your desired entry.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the information of all static address entries:

```
Switch(config)# clear mac address-table static
```

19.15 show mac address-table aging-time

Description

The **show mac address-table aging-time** command is used to display the Aging Time of the MAC address.

Syntax

```
show mac address-table aging-time
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Aging Time of the MAC address:

```
Switch(config)# show mac address-table aging-time
```


19.16 show mac address-table max-mac-count

Description

The **show mac address-table max-mac-count interface gigabitEthernet** command is used to display the security configuration of all ports or the specified port.

Syntax

```
show mac address-table max-mac-count { all | interface { fastEthernet port |  
gigabitEthernet port | hundred-gigabitEthernet port | port-channel  
port-channel-id | ten-gigabitEthernet port | twentyFive-gigabitEthernet port |  
two-gigabitEthernet port } }
```

Parameter

all — Displays the security information of all the Ethernet ports.
port — The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration of all ports:

```
Switch(config)# show mac address-table max-mac-count all
```

Display the security configuration of port 1/0/1:

```
Switch(config)# show mac address-table max-mac-count interface  
gigabitEthernet 1/0/1
```

19.17 show mac address-table interface

Description

The **show mac address-table interface** command is used to display the address configuration of the specified port/port channel.

Syntax

```
show mac address-table interface { fastEthernet port | gigabitEthernet  
port | hundred-gigabitEthernet port | port-channel port-channel-id |  
ten-gigabitEthernet port | twentyFive-gigabitEthernet port |  
two-gigabitEthernet port }
```

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the address configuration of port 1/0/1:

```
Switch(config)# show mac address-table interface gigabitEthernet 1/0/1
```

19.18 show mac address-table count

Description

The **show mac address-table count** command is used to display the total amount of MAC address table.

Syntax

```
show mac address-table count [ vlan vlan-id ]
```

Parameter

vlan-id —— Specify the VLAN which the MAC entries belong to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the total MAC entry information in different VLANs:

```
Switch(config)# show mac address-table count
```

19.19 show mac address-table address

Description

The **show mac address-table address** command is used to display the information of the specified MAC address.

Syntax

show mac address-table address *mac-addr* [**interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **port-channel** *port-channel-id* } | **vid** *vlan-id*]

Parameter

mac-addr——The specified MAC address.

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

vlan-id—— Specify the VLAN which the entry belongs to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the MAC address 00:00:00:00:23:00 in VLAN 1:

```
Switch(config)#show mac address-table address 00:00:00:00:23:00 vid 1
```

19.20 show mac address-table vlan

Description

The **show mac address-table vlan** command is used to display the MAC address configuration of the specified vlan.

Syntax

show mac address-table vlan *vid*

Parameter

vid——The specified VLAN id.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MAC address configuration of vlan 1:

```
Switch(config)# show mac address-table vlan 1
```

19.21 show mac address-table notification



Note: This command is only available on certain devices.

Description

The **show mac address-table notification** command is used to display the MAC notification configuration globally or on the specified port.

Syntax

```
show mac address-table notification all
```

Parameter

all — Displays the notification information globally and of all the Ethernet ports.

port — Displays the notification information on the specified port.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the notification configuration of all the ports:

```
Switch(config)# show mac address-table notification all
```

19.22 show mac address-table security



Note: This command is only available on certain devices.

Description

The **show mac address-table security** command is used to display the MAC address security configuration globally or of the specified VLAN.

Syntax

show mac address-table security [vid *vid*]

Parameter

vid——The specified VLAN id.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MAC address security configuration of VLAN 1:

```
Switch(config)# show mac address-table security vid 1
```

Chapter 20 IEEE 802.1Q VLAN Commands

VLAN (Virtual Local Area Network) technology is developed for the switch to divide the LAN into multiple logical LANs flexibly. Hosts in the same VLAN can communicate with each other, regardless of their physical locations. VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

20.1 vlan

Description

The **vlan** command is used to create IEEE 802.1Q VLAN and enter VLAN Configuration Mode. To delete the IEEE 802.1Q VLAN, please use **no vlan** command.

Syntax

vlan *vlan-list*
no vlan *vlan-list*

Parameter

vlan-list—— Specify IEEE 802.1Q VLAN ID list, ranging from 2 to 4094, in the format of 2-3, 5. It is multi-optional.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VLAN 2-10 and VLAN 100:

```
Switch(config)# vlan 2-10,100
```

Delete VLAN 2:

```
Switch(config)# no vlan 2
```

20.2 name

Description

The **name** command is used to assign a description to a VLAN. To clear the description, please use **no name** command.

Syntax

name *descript*

no name

Parameter

descript——String to describe the VLAN, which contains 16 characters at most.

Command Mode

VLAN Configuration Mode(VLAN)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the name of VLAN 2 as "group1":

```
Switch(config)# vlan 2
```

```
Switch(config-vlan)# name group1
```

20.3 vlan_trunk (globally)

Description

The **vlan_trunk** command is used to enable VLAN Trunk globally. When enabled, the switch will automatically create all VLANs (2-4094). To disable VLAN Trunk, use the **no vlan_trunk** command.

Syntax

vlan_trunk

no vlan_trunk

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable VLAN Trunk globally:

```
Switch(config)#vlan_trunk
```

20.4 vlan_trunk (interface)

Description

The **vlan_trunk** command is used to enable VLAN Trunk for the desired port. When enabled, all packets in VLANs can pass through this port. For VLANs that have been added through switchport general allowed vlan command, data will be forwarded according to the configured egress rule. For VLANs that have not been manually added, data will be forwarded through the egress rule "tagged". To disable VLAN Trunk, use the **no vlan_trunk** command. By default, it is disabled.

Syntax

```
vlan_trunk  
no vlan_trunk
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable VLAN Trunk for port 1/0/3:

```
Switch(config)#interface gigabitEthernet 1/0/3  
Switch(config-if)#vlan_trunk
```


20.5 switchport general allowed vlan

Description

The **switchport general allowed vlan** command is used to add the desired port to IEEE 802.1Q VLAN, or to remove a port from the corresponding VLAN.

Syntax

switchport general allowed vlan *vlan-list* { tagged | untagged }

no switchport general allowed vlan *vlan-list*

Parameter

vlan-list — VLAN ID list, ranging from 1 to 4094, in the format of 2-3, 5. It is multi-optional. "all" can also be entered to indicate all configured VLANs.

tagged | untagged — egress-rule. When the *vlan-list* is entered with "all", the egress-rule is "tagged" by default and cannot be modified.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure Gigabit Ethernet port 1/0/4 whose link type is "general" to VLAN 2 and its egress-rule as "tagged":

```
Switch(config)#interface gigabitEthernet 1/0/4
```

```
Switch(config-if)#switchport general allowed vlan 2 tagged
```

20.6 switchport pvid

Description

The **switchport pvid** command is used to configure the PVID for the switch ports.

Syntax

switchport pvid *vlan-id*

Parameter

vlan-id—— VLAN ID, ranging from 1 to 4094.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the PVID of port 1/0/2 as 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# switchport pvid 2
```

20.7 switchport check ingress

Description

The **switchport check ingress** command is used to enable the Ingress Checking function for the switch ports. With this function enabled, the port will accept the packet of which the VLAN ID is in the port's VLAN list and discard others. With this function disabled, the port will forward the packet directly. To disable this function, please use **no switchport check ingress** command.

Syntax

switchport check ingress
no switchport check ingress

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable Ingress Checking on the port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# switchport check ingress
```

20.8 switchport acceptable frame

Description

The **switchport acceptable frame** command is used to specify the acceptable frame type for the switch ports and the ports will perform this operation before Ingress Checking. To restore to the default setting, please use **no switchport acceptable frame** command.

Syntax

```
switchport acceptable frame { all | tagged }
no switchport acceptable frame
```

Parameter

all | tagged — the acceptable frame type.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the acceptable frame type of Gigabit Ethernet port 1/0/4 as "tagged":

```
Switch(config)#interface gigabitEthernet 1/0/4
Switch(config-if)#switchport acceptable frame tagged
```

20.9 show vlan summary

Description

The **show vlan summary** command is used to display the summarized information of IEEE 802.1Q VLAN.

Syntax

```
show vlan summary
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summarized information of IEEE 802.1Q VLAN:

```
Switch(config)# show vlan summary
```

20.10 show vlan brief

Description

The **show vlan brief** command is used to display the brief information of IEEE 802.1Q VLAN.

Syntax

```
show vlan brief
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the brief information of IEEE 802.1Q VLAN:

```
Switch(config)# show vlan brief
```

20.11 show vlan

Description

The **show vlan** command is used to display the information of IEEE 802.1Q VLAN.

Syntax

show vlan [*id vlan-id*]

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094. It is multi-optional. Using the **show vlan** command without parameter displays the detailed information of all VLANs.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of vlan 5:

```
Switch(config)# show vlan id 5
```

20.12 show interface switchport

Description

The **show interface switchport** command is used to display the IEEE 802.1Q VLAN configuration information of the specified port/port channel.

Syntax

show interface switchport [*fastEthernet port* | *gigabitEthernet port* | *ten-gigabitEthernet port* | *port-channel port-channel-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the VLAN configuration information of all ports and port channels:

```
Switch(config)# show interface switchport
```

Chapter 21 MAC-based VLAN Commands

MAC VLAN (Virtual Local Area Network) is the way to classify the VLANs based on MAC Address. A MAC address is relative to a single VLAN ID. The untagged packets and the priority-tagged packets coming from the MAC address will be tagged with this VLAN ID.

21.1 mac-vlan mac-address

Description

The **mac-vlan mac-address** command is used to create a MAC-based VLAN entry. To delete a MAC-based VLAN entry, please use the **no mac-vlan mac-address** command.

Syntax

```
mac-vlan mac-address mac-addr vlan vlan-id [description descript]  
no mac-vlan mac-address mac-addr
```

Parameter

mac-addr—— MAC address, in the format of XX:XX:XX:XX:XX:XX.

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

descript—— Give a description to the MAC address for identification, which contains 8 characters at most.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VLAN 2 with the MAC address 00:11:11:01:01:12 and the name "TP":

```
Switch(config)#mac-vlan mac-address 00:11:11:01:01:12 vlan 2  
description TP
```

21.2 mac-vlan

Description

The **mac-vlan** command is used to enable a port for the MAC-based VLAN feature. Only the port is enabled can the configured MAC-based VLAN take effect. To disable the MAC-based VLAN function, please use **no mac-vlan** command. All the ports are disabled by default.

Syntax

mac-vlan

no mac-vlan

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Gigabit Ethernet port 1/0/3 for the MAC-based VLAN feature:

```
Switch(config)#interface gigabitEthernet 1/0/3
```

```
Switch(config-if)#mac-vlan
```

21.3 show mac-vlan

Description

The **show mac-vlan** command is used to display the information of the MAC-based VLAN entry. MAC address and VLAN ID can be used to filter the displayed information.

Syntax

show mac-vlan { **all** | **mac-address** *mac-addr* | **vlan** *vlan-id* }

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Parameter

mac-addr—— MAC address, in the format of XX:XX:XX:XX:XX:XX.

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

Example

Display the information of all the MAC-based VLAN entry:

```
Switch#show mac-vlan all
```

21.4 show mac-vlan interface

Description

The **show mac-vlan interface** command is used to display the port state of MAC-based VLAN.

Syntax

```
show mac-vlan interface
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the enable state of all the ports:

```
Switch#show mac-vlan interface
```

21.5 show dot1x mac-vlan

Description

The **show dot1x mac-vlan** command is used to display MAC entries that have been added to guest VLANs or assignment VLANs under MAC-based authentication.

Syntax

show dot1x mac-vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MAC entries that have been added to guest VLANs or assignment VLANs under MAC-based authentication:

```
Switch# show dot1x mac-vlan
```

21.6 show dot1x vlan

Description

The **show dot1x vlan** command is used to display the VLAN information that has been modified by the authentication function.

Syntax

show dot1x vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the VLAN information that has been modified by the authentication function:

```
Switch# show dot1x vlan
```

21.7 show dot1x interface switchport

Description

The **show dot1x interface switchport** command is used to display the interface switchport information that has been modified by the authentication function.

Syntax

```
show dot1x interface switchport
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the interface switchport information that has been modified by the authentication function:

```
Switch# show dot1x interface switchport
```

21.8 show dot1x acl

Description

The **show dot1x acl** command is used to display the ACL information bound to 802.1X authentication.

Syntax

```
show dot1x acl
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ACL information bound to 802.1X authentication:

```
Switch# show dot1x acl
```

21.9 show dot1x redirect-message

Description

The **show dot1x redirect-message** command is used to display 802.1X redirect-related information.

Syntax

```
show dot1x redirect-message
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display 802.1X redirect-related information:

```
Switch# show dot1x redirect-message
```

Chapter 22 Protocol-based VLAN Commands

Protocol VLAN (Virtual Local Area Network) is the way to classify VLANs based on Protocols. A Protocol is relative to a single VLAN ID. The untagged packets and the priority-tagged packets matching the protocol template will be tagged with this VLAN ID.

22.1 protocol-vlan template

Description

The **protocol-vlan template** command is used to create Protocol-based VLAN template. To delete Protocol-based VLAN template, please use **no protocol-vlan template** command.

Syntax

For L2/L2+ switches:

protocol-vlan template name *protocol-name* **frame** { **ether_2** **ether-type** *type* | **snap** **ether-type** *type* | **llc** **dsap** *dsap_type* **ssap** *ssap_type* }

no protocol-vlan template *template-idx*

For L3 switches:

protocol-vlan template name *protocol-name* **frame** { **ether_2** **ether-type** *type* | **snap** **ether-type** *type* | **llc** **dsap** *dsap_type* **ssap** *ssap_type* }

no protocol-vlan template *template-name*

Parameter

protocol-name — Give a name for the Protocol-based VLAN Template , which contains 8 characters at most.

ether_2 ether-type type — Specify the Ethernet type.

snap ether-type type — Specify the Ethernet type.

llc dsap dsap_type ssap ssap_type — Specify the DSAP type and the SSAP type.

template-idx — The number of the Protocol-based VLAN Template. You can get the template corresponding to the number by the [show protocol-vlan template](#) command.

template-name — The name of the Protocol-base VLAN Template. You can get the template corresponding to the number by the [show protocol-vlan template](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a Protocol-based VLAN template named "TP" whose Ethernet protocol type is 0x2024:

```
Switch(config)#protocol-vlan template name TP frame ether_2 ether-type
2024
```

22.2 protocol-vlan vlan

Description

The **protocol-vlan vlan** command is used to create a Protocol-based VLAN entry. To delete a Protocol-based VLAN entry, please use **no protocol-vlan vlan** command.

Syntax

For L2/L2+ switches:

protocol-vlan vlan *vlan-id* **priority** *priority* **template** *template-idx*
no protocol-vlan vlan *group-idx*

For L3 switches:

protocol-vlan vlan *vlan-id* **priority** *priority* **template** *template-name*
no protocol-vlan vlan *group-name*

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1-4094.

priority—— Specify the 802.1p priority for the packets that belong to the protocol VLAN, ranging from 0–7. The switch will determine the forwarding sequence according to this value. The packets with larger value of 802.1p priority have the higher priority.

template-idx——The number of the Protocol-based VLAN Template. You can get the template corresponding to the number by the [show protocol-vlan template](#) command.

group-idx——The number of the Protocol-based VLAN entry. You can get the Protocol-based VLAN entry corresponding to the number by the [show protocol-vlan vlan](#) command.

template-name——The name of the Protocol-based VLAN Template. You can get the template corresponding to the number by the [show protocol-vlan template](#) command.

group-name——The name of the Protocol-based VLAN entry. You can get the Protocol-based VLAN entry corresponding to the number by the [show protocol-vlan vlan](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create Protocol-based VLAN 2 and bind it with Protocol-based VLAN Template 3:

```
Switch(config)#protocol-vlan vlan 2 template 3
```

22.3 protocol-vlan group

Description

The **protocol-vlan** command is used to add the port to a specified protocol group. To remove the port from this protocol group, please use **no protocol-vlan group** command.

Syntax

For L2/L2+_ switches:

protocol-vlan group *index*

no protocol-vlan group *index*

For L3_ switches:

protocol-vlan group *name*

no protocol-vlan group *name*

Parameter

index—— Specify the protocol group ID.

name—— Specify the protocol group name.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add Gigabit Ethernet port 20 to protocol group 1:

```
Switch(config)#interface gigabitEthernet 1/0/20
Switch(config-if)#protocol-vlan group 1
```

22.4 show protocol-vlan template

Description

The **show protocol-vlan template** command is used to display the information of the Protocol-based VLAN templates.

Syntax

show protocol-vlan template

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the Protocol-based VLAN templates:

```
Switch(config)#show protocol-vlan template
```


22.5 show protocol-vlan vlan

Description

The **show protocol-vlan vlan** command is used to display the information about Protocol-based VLAN entry.

Syntax

show protocol-vlan vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display information of the Protocol-based VLAN entry:

```
Switch(config)#show protocol-vlan vlan
```

Chapter 23 Private VLAN Commands (Only for Certain Devices)



Note: Private VLAN commands are only available on certain devices.

Private VLANs are configured specially for saving VLAN resource of uplink devices and decreasing broadcast.

23.1 private-vlan primary

Description

The **private-vlan primary** command is used to configure the designated VLAN as the primary VLAN of the Private VLAN. To remove the primary VLAN property of the current VLAN, please use **no private-vlan primary** command.

Syntax

private-vlan primary

no private-vlan primary

Command Mode

VLAN Configuration Mode (VLAN)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the VLAN 3 as the primary VLAN of the private VLAN:

```
Switch(config)#vlan 3
```

```
Switch(config-vlan)#private-vlan primary
```

23.2 private-vlan community

Description

The **private-vlan community** command is used to configure the designated VLAN as the community VLAN of the Private VLAN. To remove the

community VLAN property of the current VLAN, please use **no private-vlan community** command.

Syntax

private-vlan community
no private-vlan community

Command Mode

VLAN Configuration Mode (VLAN)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the VLAN 4 as the community VLAN of the private VLAN:

```
Switch(config)#vlan 4
Switch(config-vlan)#private-vlan community
```

23.3 private-vlan isolated

Description

The **private-vlan isolated** command is used to configure the designated VLAN as the isolated VLAN of the Private VLAN. To remove the isolated VLAN property of the current VLAN, please use **no private-vlan isolated** command.

Syntax

private-vlan isolated
no private-vlan isolated

Command Mode

VLAN Configuration Mode (VLAN)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the VLAN 3 as the isolated VLAN of the private VLAN:

```
Switch(config)#vlan 3
```

```
Switch(config-vlan)#private-vlan isolated
```

23.4 private-vlan association

Description

The **private-vlan association** command is used to associate primary VLAN with secondary VLAN. To exterminate the currently association, please use **no private-vlan association** command.

Syntax

```
private-vlan association vlan_list
```

```
no private-vlan association vlan_list
```

Parameter

vlan_list — Secondary VLAN ID, ranging from 2 to 4094.

Command Mode

VLAN Configuration Mode (VLAN)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Associate primary VLAN 3 with community VLAN 4 as a private VLAN:

```
Switch(config)#vlan 3
```

```
Switch(config-vlan)#private-vlan association 4
```

23.5 switchport private-vlan

Description

The **switchport private-vlan** command is used to configure the private VLAN mode for the switchport. To invalid the configuration, please use **no switchport private-vlan** command.

Syntax

```
switchport private-vlan { promiscuous | host }
```

```
no switchport private-vlan
```

Parameter

promiscuous | host — Configure the private VLAN mode for the switchport.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure Gigabit Ethernet port 3 as "host":

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#switchport private-vlan host
```

23.6 switchport private-vlan host-association

Description

The **switchport private-vlan host-association** command is used to add host type port to private VLAN. To remove the port from Private VLAN, please use **no switchport private-vlan host-association** command.

Syntax

```
switchport private-vlan host-association primary_vlan_id  
secondary_vlan_id vlantype  
no switchport private-vlan host-association
```

Parameter

primary-vlan-id — Primary VLAN ID, ranging from 2 to 4094.

secondary-vlan-id — Secondary VLAN ID, ranging from 2 to 4094.

vlantype — Specify the type of the secondary VLAN, either *community* or *isolated*.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure host type Gigabit Ethernet port 1/0/3 as a member of primary VLAN 3 and secondary VLAN 4, with the type of VLAN 4 as community:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#switchport private-vlan host-association 3 4 community
```

23.7 switchport private-vlan mapping

Description

The **switchport private-vlan mapping** command is used to add promiscuous type port to private VLAN. To remove the port from Private VLAN, please use **no switchport private-vlan mapping** command.

Syntax

```
switchport private-vlan mapping primary_vlan_id secondary_vlan_id
no switchport private-vlan mapping
```

Parameter

primary-vlan-id—— Primary VLAN ID, ranging from 2 to 4094.

secondary-vlan-id—— Secondary VLAN ID, ranging from 2 to 4094.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure promiscuous type Gigabit Ethernet port 1/0/3 as a member of primary VLAN 3 and secondary VLAN 4:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#switchport private-vlan mapping 3 4
```

23.8 show vlan private-vlan

Description

The **show vlan private-vlan** command is used to display the Private VLAN configuration information of the switch.

Syntax

show vlan private-vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the configuration information of all Private VLAN:

```
Switch(config)#show vlan private-vlan
```

23.9 show vlan private-vlan interface

Description

The **show vlan private-vlan interface** command is used to display the Private VLAN configuration information of the specified port(s).

Syntax

show vlan private-vlan interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the configuration information of all the Ethernet ports:

```
Switch(config)#show vlan private-vlan interface
```


Chapter 24 VLAN-VPN Commands (Only for Certain Devices)



Note: VLAN-VPN commands are only available on certain devices.

VLAN-VPN (Virtual Private Network) function, the implement of a simple and flexible Layer 2 VPN technology, allows the packets with VLAN tags of private networks to be encapsulated with VLAN tags of public networks at the network access terminal of the Internet Service Provider. And these packets will be transmitted with double-tag across the public networks.

24.1 dot1q-tunnel

Description

The **dot1q-tunnel** command is used to enable the VLAN-VPN function globally. To disable the VLAN-VPN function, please use the **no dot1q-tunnel** command.

Syntax

dot1q-tunnel
no dot1q-tunnel

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the VLAN-VPN function globally:

```
Switch(config)#dot1q-tunnel
```

24.2 switchport dot1q-tunnel tpid

Description

The **switchport dot1q-tunnel tpid** command is used to configure Global TPID for the ports. To restore to the default value, please use the **no switchport dot1q-tunnel tpid** command.

Syntax

```
switchport dot1q-tunnel tpid tpid  
no switchport dot1q-tunnel tpid
```

Parameter

tpid—— The value of Global TPID. It must be 4 Hex integers. By default, it is 8100.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure TPID of port 1/0/2 as 0x9100:

```
Switch(config)#interface gigabitEthernet 1/0/2  
Switch(config-if)#switchport dot1q-tunnel tpid 9100
```

24.3 dot1q-tunnel mapping

Description

The **dot1q-tunnel mapping** command is used to enable the VLAN Mapping feature globally. To disable this function, please use the **no dot1q-tunnel mapping** command. By default, the VLAN Mapping feature is disabled.

Syntax

dot1q-tunnel mapping
no dot1q-tunnel mapping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the VLAN mapping feature globally:

```
Switch(config)#dot1q-tunnel mapping
```

24.4 switchport dot1q-tunnel mode

Description

The **switchport dot1q-tunnel mode** command is used to configure the VPN port's mode. To close this VPN port, please use the **no switchport dot1q-tunnel mode** command. By default, no port has been configured as the VPN port. The VPN port mode uni and nni cannot switch to each other directly, so please close the VPN port and switch to the other mode if needed.

Syntax

switchport dot1q-tunnel mode { uni | nni }
no switchport dot1q-tunnel mode

Parameter

uni——The port connected to the clients.
nni——The port connected to the ISP.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Gigabit Ethernet port 1/0/3 as the VPN UNI ports:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#switchport dot1q-tunnel mode uni
```

24.5 switchport dot1q-tunnel missdrop (only for certain devices)



Note:

For some devices, Missdrop can only be enabled on UNI ports.
For other devices, Missdrop can only be enabled on NNI ports.

Description

The **switchport dot1q-tunnel missdrop** command is used to enable the VLAN-VPN missdrop function for a specific port. To disable the VLAN-VPN missdrop function, please use the **no switchport dot1q-tunnel missdrop** command.

Syntax

```
switchport dot1q-tunnel missdrop
no switchport dot1q-tunnel missdrop
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the VLAN-VPN missdrop function for Gigabit Ethernet port 1/0/3:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#switchport dot1q-tunnel missdrop
```

24.6 switchport dot1q-tunnel use_inner_priority

Description

The **switchport dot1q-tunnel use_inner_priority** command is used to use the inner 802.1p priority. To disable this function, please use the **no switchport dot1q-tunnel use_inner_priority** command.

Syntax

```
switchport dot1q-tunnel use_inner_priority
no switchport dot1q-tunnel use_inner_priority
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the use inner priority function for Gigabit Ethernet port 1/0/3:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#switchport dot1q-tunnel use_inner_priority
```

24.7 switchport dot1q-tunnel mapping



Note:

For some devices, choose a UNI port to enable VLAN mapping.
For other devices, choose a NNI port to enable VLAN mapping.

Description

The **switchport dot1q-tunnel mapping** command is used to add the VLAN Mapping entry on a specified port. To delete the VLAN Mapping entry on this port, please use the **no switchport dot1q-tunnel mapping** command.

Syntax

```
switchport dot1q-tunnel mapping c-vlan sp-vlan [descript]  
no switchport dot1q-tunnel mapping [c-vlan]
```

Parameter

c-vlan—— Customer VLAN ID, ranging from 1 to 4094.
sp-vlan—— Service Provider VLAN ID, ranging from 1 to 4094.
descript—— Give a Description to the VLAN Mapping entry, which contains 16 characters at most.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a VLAN Mapping entry on the Gigabit Ethernet port 1/0/3 with the Customer VLAN as VLAN 2 and the Service Provider VLAN as VLAN 3:

```
Switch(config)#interface gigabitEthernet 1/0/3  
Switch(config-if)#switchport dot1q-tunnel mapping 2 3
```

24.8 switchport dot1q-tunnel replace

Description

The **switchport dot1q-tunnel replace** command is used to replace the customer VLAN ID with a VLAN ID of service provider on a specified port, rather than adds an outer tag. To delete the VLAN Replace entry on this port, please use the **no switchport dot1q-tunnel replace** command.

Syntax

switchport dot1q-tunnel replace *c-vlan sp-vlan* [*descript*]
no switchport dot1q-tunnel replace *c-vlan sp-vlan* [*descript*]

Parameters

c-vlan—— Customer VLAN ID, ranging from 1 to 4094.
sp-vlan—— Service Provider VLAN ID, ranging from 1 to 4094.
descript—— Give a Description to the VLAN Mapping entry, which contains 16 characters at most.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Before configuring VLAN Replace, enable VLAN Mapping globally.

Example

Add a VLAN Replace entry on the Gigabit Ethernet port 1/0/3 to replace the Customer VLAN (VLAN 2) with the Service Provider VLAN (VLAN 3):

```
Switch(config)# switchport dot1q-tunnel replace 2 3
```

24.9 switchport dot1q-tunnel replace-out

Description

The **switchport dot1q-tunnel replace-out** command is used to replace the VLAN ID of service provider with a customer VLAN ID on a specified port. To delete the VLAN Replace entry on this port, please use the **no switchport dot1q-tunnel replace-out** command.

Syntax

switchport dot1q-tunnel replace-out *sp-vlan c-vlan* [*descript*]
no switchport dot1q-tunnel replace-out *sp-vlan c-vlan* [*descript*]

Parameters

sp-vlan—— Service Provider VLAN ID, ranging from 1 to 4094.

c-vlan—— Customer VLAN ID, ranging from 1 to 4094.

descript—— Give a Description to the VLAN Mapping entry, which contains 16 characters at most.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Before configuring VLAN Replace-Out, enable VLAN Mapping globally.

Example

Add a VLAN Replace entry on the Gigabit Ethernet port 1/0/3 to replace the Service Provider VLAN (VLAN 2) with the Customer VLAN (VLAN 3):

```
Switch(config)# switchport dot1q-tunnel replace-out 2 3
```

24.10 show dot1q-tunnel

Description

The **show dot1q-tunnel** command is used to display the global configuration information of the VLAN VPN.

Syntax

```
show dot1q-tunnel
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration information of the VLAN VPN:


```
Switch(config)#show dot1q-tunnel
```

24.11 show dot1q-tunnel mapping

Description

The **show dot1q-tunnel mapping** command is used to display the information of VLAN Mapping entry.

Syntax

```
show dot1q-tunnel mapping
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of VLAN Mapping entry:

```
Switch(config)#show dot1q-tunnel mapping
```

24.12 show dot1q-tunnel interface

Description

The **show dot1q-tunnel mapping interface** command is used to display the VLAN VPN port type.

Syntax

```
show dot1q-tunnel interface
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port type of all VLAN VPN ports:

```
Switch(config)#show dot1q-tunnel interface
```

Chapter 25 ERPS Commands

ERPS (Ethernet Ring Protection Switching) is an Ethernet ring link layer technology with high reliability and stability. It can prevent broadcast storms caused by the data loop if the Ethernet ring is complete. With a high convergence speed, it can quickly restore the communication paths among the nodes in the ring network when a link failure happens.

25.1 erps ring

Description

The **erps ring** command is used to enable the ERPS ring function globally and create an ERPS ring. To disable the ERPS ring function, please use **no erps ring** command.

Syntax

erps ring *ring-id*
no erps ring *ring-id*

Parameter

ring-id—— The ID of the ERPS ring, ranging from 1 to 255.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ERPS ring function globally:

```
Switch(config)#erps ring 1
```

25.2 control-vlan

Description

The **control-vlan** command is used to configure a control VLAN for an ERPS ring to forward RAPS PDUs .

Syntax

control-vlan *vlan-id*

Parameter

vlan-id—Specify the ID of a control VLAN for ERPS ring, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure control VLAN 2 in ERPS ring 1:

```
Switch(config)#erps ring 1
Switch(ring-config)#control-vlan 2
```

25.3 description

Description

The **description** command is used to add description information of an ERPS ring. To restore the default description, please use the **no description** command.

Syntax

description *description*
no erps ring *ringid* **description**

Parameter

description—The description for the ERPS ring. It is the ring ID by default.
ringid—ERPS ring ID, e.g., 1, 5, 8

Command Mode

Global Configuration Mode
ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add description information "ring 1":

```
Switch(ring-config)#description "ring 1"
```

Restore ring 1's description to the default:

```
Switch(config)#no erps ring 1 description
```

25.4 guard-timer

Description

The **guard-timer** command is used to configure the Guard timer in an ERPS ring. By default, the Guard timer is 200 centiseconds in an ERPS ring. To disable the guard-timer function, please use **no guard-timer** command.

Syntax

guard-timer *time*

no guard-timer

Parameter

time — The time setting for guard-timer, ranging from 1 to 200, in centiseconds.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time for guard-timer as 100:

```
Switch(ring-config)#guard-timer 100
```

25.5 wtr-timer

Description

The **wtr-timer** command is used to configure the Wait to Restore (WTR) timer in an ERPS ring. By default, the WTR timer is 5 minutes in an ERPS ring. To disable the wtr-timer function, please use **no wtr-timer** command.

Syntax

wtr-timer *time*

no wtr-timer

Parameter

time — The time setting for wtr-timer, ranging from 1 to 12.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time for wtr-timer as 1:

```
Switch(ring-config)#wtr-timer 1
```

25.6 holdoff-timer

Description

The **holdoff-timer** command is used to configure the Holdoff timer in an ERPS ring. By default, the Holdoff timer is 0 deciseconds in an ERPS ring. When a fault occurs, the fault is not immediately reported to ERPS. Instead, the Holdoff timer starts. If the fault persists after the timer expires, the fault will be reported to ERPS. To disable the holdoff-timer function, please use **no holdoff-timer** command.

Syntax

holdoff-timer *time*

no holdoff-timer

Parameter

time — The time setting for holdoff-timer, ranging from 1 to 100.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time for holdoff-timer as 10:

```
Switch(ring-config)#holdoff-timer 10
```

25.7 protected-instance

Description

The **protected-instance** command is used to configure the Ethernet ring protection (ERP) instances in an ERPS ring. To disable the protected-instance function, please use **no protected-instance** command. By default, no ERP instance is configured in an ERPS ring.

Syntax

protected-instance *instance*

no protected-instance *instance*

Parameter

instance—— Protected instance for the ERPS ring. Valid values depend on the maximum number of spanning-tree instances supported/configured on the device.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the protected instance as 1, and map VLAN10-20 to instance 1:

```
Switch(ring)#spanning-tree mode mstp
Switch(ring)#spanning-tree mst configuration
Switch(ring)#instance 1 vlan 10-20
Switch(ring-config)#protected-instance 1
```

25.8 raps-mel

Description

The **raps-mel** command is used to configure the value of the MEL field in Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs) of the ERPS ring. To restore the default value of 7, please use the **no raps-mel** command.

Syntax

raps-mel *mel*
no erps ring *ringid* **raps-mel**

Parameter

mel—— MEL value of the ERPS ring, ranging from 0 to 7. The default value is 7.

ringid—— ERPS ring ID, e.g., 1, 5, 8

Command Mode

Global Configuration Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MEL value as 1:

```
Switch(ring-config)#raps-mel 1
```

Restore ring 1's RAPS-MEL to the default value:

```
Switch(config)#no erps ring 1 raps-mel
```

25.9 revertive

Description

The **revertive** command is used to configure the revertive switching or non-revertive switching of the ERPS ring. To disable this function, please use the **revertive disable** command. By default, ERPS rings use revertive switching.

Syntax

revertive enable

revertive disable

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the revertive function:

```
Switch(ring-config)#revertive enable
```

25.10 sub-ring

Description

The **sub-ring** command is used to configure the ERPS ring as an sub-ring. To disable this function, please use the **no sub-ring** command.

Syntax

sub-ring

no sub-ring

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the sub-ring function:

```
Switch(ring-config)#sub-ring
```

25.11 tc-notify erps

Description

The **tc-notify erps** command is used to enable the network topology change notification function. To disable this function, please use the **no tc-notify erps** command. By default, this function is disabled.

Syntax

tc-notify erps ring *ring-id*

no tc-notify erps ring *ring-id*

Parameter

ring-id—— the ring ID of the notification, ranging from 1 to 8.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the network topology change notification function of ring 1:

```
Switch(ring-config)#tc-notify erps ring 1
```

25.12 tc-protection interval

Description

The **tc-protection interval** command is used to configure the network topology change protection interval for sending topology change notification messages. To disable this function, please use the **no tc-protection interval** command.

Syntax

tc-protection interval *interval*

no tc-protection interval *interval*

Parameter

interval—— the time interval for tc-protection, ranging from 1 to 600.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the tc-protection interval of the ERPS ring as 1:

```
Switch(ring-config)#tc-protection interval 1
```

25.13 tc-protection threshold

Description

The **tc-protection threshold** command is used to configure the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval. To disable this function, please use the **no tc-protection threshold** command.

Syntax

tc-protection threshold *threshold*
no tc-protection threshold

Parameter

threshold—— the threshold for tc-protection, ranging from 1 to 255.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the tc-protection threshold of the ERPS ring as 1:

```
Switch(ring-config)#tc-protection threshold 1
```

25.14 version

Description

The **version** command is used to configure the ERPS version. To restore the ERPS ring's version to the default value of 1, please use the **no version** command,

Syntax

version *version*
no erps ring *ringid* **version**

Parameter

version—— the version of the ERPS function, ranging from 1 to 2. The default value is 1.

ringid—— ERPS ring ID, e.g., 1, 5, 8

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ERPS version as 2:

```
Switch(ring-config)#version 2
```

Restore the ERPS ring 1's version to the default value of 1:

```
Switch(config)# no erps ring 1 version
```

25.15 virtual-channel

Description

The **virtual-channel** command is used to configure the virtual channel (VC) mode for RAPS PDU transmission in a sub-ring. To disable this function, please use the **no virtual-channel** command.

Syntax

virtual-channel

no virtual-channel

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the virtual-channel function:

```
Switch(ring-config)#virtual-channel
```

25.16 erps ring rpl

Description

The **erps ring rpl** command is used to add a port to the ERPS ring and specify the role of the port. To remove the role of the port, please use the **no erps ring rpl** command.

Syntax

erps ring *ring id* [**rpl** *owner* | *neighbour*]

Parameter

ring id—— the ID of the ring that the port joins.

owner—— configure the role of the port as owner.

neighbour—— configure the role of the port as neighbour.

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the role of port 1/0/2 in ring 1 as owner:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)#erps ring 1 rpl owner
```

25.17 erps ring protect-switch

Description

The **erps ring protect-switch** command is used to configure a port blocking mode for the ERPS port.

Syntax

erps ring *ring id* [**protect-switch** *force* | *manual*]

Parameter

ring id—— the ID of the ERPS ring, ranging from 1-255.

force——block a port forcibly.

manual—— indicate the MS mode for blocking an ERPS port.

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the switch mode of port 1/0/2 in ring 1 as force:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)#erps ring 1 protect-switch force
```

25.18 show erps ring

Description

The **show erps ring** command is used to display the ERPS ring information.

Syntax

show erps ring {*ring-id* | *all*}

Parameter

ring id—— show the information of a specified ring, ranging from 1 to 8.

all—— show the information of all rings.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Show the information of all rings:

```
Switch(config)#show erps ring all
```

25.19 show erps statistics (only for certain devices)

Description

The **show erps statistics** command is used to display the ERPS packet statistics.

Syntax

show erps statistics

show erps statistics ring *ringld*

Parameter

ringld—— ERPS ring ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display packet statistics for all ERPS rings:

```
Switch(config)# show erps statistics
```

Display packet statistics for ERPS ring 1:

```
Switch(config)# show erps statistics ring 1
```

Chapter 26 GVRP Commands

GVRP (GARP VLAN registration protocol) is an implementation of GARP (generic attribute registration protocol). GVRP allows the switch to automatically add or remove the VLANs via the dynamic VLAN registration information and propagate the local VLAN registration information to other switches, without having to individually configure each VLAN.

26.1 gvrp

Description

The **gvrp** command is used to enable the GVRP function globally. To disable the GVRP function, please use **no gvrp** command.

Syntax

gvrp
no gvrp

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the GVRP function globally:

```
Switch(config)#gvrp
```

26.2 gvrp (interface)

Description

The **gvrp** command is used to enable the GVRP function for the desired port. To disable it, please use **no gvrp** command. The GVRP feature can only be enabled for the trunk-type ports.

Syntax

gvrp

no gvrp

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the GVRP function for Gigabit Ethernet ports 1/0/2-6:

```
Switch(config)#interface range gigabitEthernet 1/0/2-6
Switch(config-if-range)#gvrp
```

26.3 gvrp registration

Description

The **gvrp registration** command is used to configure the GVRP registration type for the desired port. To restore to the default value, please use **no gvrp registration** command.

Syntax

gvrp registration { normal | fixed | forbidden }
no gvrp registration

Parameter

normal | fixed | forbidden — Registration mode. By default, the registration mode is "normal".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the GVRP registration mode as "fixed" for Gigabit Ethernet ports 1/0/2-6:

```
Switch(config)#interface range gigabitEthernet 1/0/2-6
Switch(config-if-range)#gvrp registration fixed
```

26.4 gvrp timer

Description

The **gvrp timer** command is used to set a GVRP timer for the desired port. To restore to the default setting of a GARP timer, please use **no gvrp timer** command.

Syntax

gvrp timer { leaveall | join | leave } *value*

no gvrp timer [leaveall | join | leave]

Parameter

leaveall | join | leave — They are the three timers: leave All, join and leave. Once the LeaveAll Timer is set, the port with GVRP enabled can send a LeaveAll message after the timer times out, so that other GARP ports can re-register all the attribute information. After that, the LeaveAll timer will start to begin a new cycle. To guarantee the transmission of the Join messages, a GARP port sends each Join message two times. The Join Timer is used to define the interval between the two sending operations of each Join message. Once the Leave Timer is set, the GARP port receiving a Leave message will start its Leave timer, and deregister the attribute information if it does not receive a Join message again before the timer times out.

value — The value of the timer. The LeaveAll Timer ranges from 1000 to 30000 centiseconds and the default value is 1000 centiseconds. The Join Timer ranges from 20 to 1000 centiseconds and the default value is 20 centiseconds. The Leave Timer ranges from 60 to 3000 centiseconds and the default value is 60 centiseconds.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the GARP leaveall timer of Gigabit Ethernet port 1/0/6 as 2000 centiseconds and restore the join timer of it to the default value:

```
Switch(config)#interface gigabitEthernet 1/0/6
```

```
Switch(config-if)#gvrp timer leaveall 2000
```

```
Switch(config-if)#no gvrp timer join
```

26.5 show gvrp interface

Description

The **show gvrp interface** command is used to display the GVRP configuration information of a specified Ethernet port or of all Ethernet ports.

Syntax

```
show gvrp interface [fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port | port-channel port-channel-id]
```

Parameter

port — The port number.

port-channel-id — The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the GVRP configuration information of Gigabit Ethernet port 1:

```
Switch(config)#show gvrp interface gigabitEthernet 1/0/1
```

Display the GVRP configuration information of all Ethernet ports:

```
Switch(config)#show gvrp interface
```

26.6 show gvrp global

Description

The **show gvrp global** command is used to display the global GVRP status.

Syntax

show gvrp global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global GVRP status:

```
Switch(config)#show gvrp global
```

Chapter 27 IGMP Snooping Commands

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on Layer 2 switch. It can effectively prevent multicast groups being broadcasted in the network.

27.1 ip igmp snooping (global)

Description

The **ip igmp snooping** command is used to configure IGMP Snooping globally. To disable the IGMP Snooping function, please use **no ip igmp snooping** command.

Syntax

ip igmp snooping
no ip igmp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP Snooping function:

```
Switch(config)# ip igmp snooping
```

27.2 ip igmp snooping version

Description

The **ip igmp snooping version** command is used to configure IGMP version globally. To return to the default configuration, please use **no ip igmp snooping version** command.

Syntax

ip igmp snooping version {v1 | v2 | v3 }
no ip igmp snooping version

Parameter

v1 | v2 | v3—— Specify the IGMP version. By default, it is IGMP v3.

v1: The switch works as an IGMPv1 Snooping switch. It can only process IGMPv1 messages from the host. Report messages of other versions are ignored.

v2: The switch works as an IGMPv2 Snooping switch. It can process both IGMPv1 and IGMPv2 messages from the host. IGMPv3 messages are ignored.

v3: The switch works as an IGMPv3 Snooping switch. It can process IGMPv1, IGMPv2 and IGMPv3 messages from the host.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the IGMP version as v2:

```
Switch (config)# ip igmp snooping version v2
```

27.3 ip igmp snooping drop-unknown

Description

The **ip igmp snooping drop-unknown** command is used to configure the way how the switch processes multicast streams that are sent to unknown multicast groups as Discard. By default, it is Forward. To return to the default configuration, please use **no ip igmp snooping drop-unknown** command.

Syntax

ip igmp snooping drop-unknown

no ip igmp snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the operation to process unknown multicast as discard:

```
Switch(config)# ip igmp snooping drop-unknown
```

27.4 ip igmp snooping header-validation

Description

The **ip igmp snooping header-validation** command is used to enable IGMP Header Validation globally. To disable the IGMP Header Validation function, please use **no ip igmp snooping header-validation** command.

Generally, for IGMP packets, the TTL value should be 1, ToS field should be 0xC0, and Router Alert option should be 0x94040000. The fields to be validated depend on the IGMP version being used. IGMPv1 only checks the TTL field. IGMPv2 checks the TTL field and the Router Alert option. IGMPv3 checks TTL field, ToS field and Router Alert option. Packets that fail the validation process will be dropped.

Syntax

ip igmp snooping header-validation

no ip igmp snooping header-validation

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP Header Validation:

```
Switch(config)# ip igmp snooping header-validation
```

27.5 ip igmp snooping vlan-config

Description

The **ip igmp snooping vlan-config** command is used to enable VLAN IGMP Snooping function or to modify IGMP Snooping parameters. To disable the

VLAN IGMP Snooping function, please use **no ip igmp snooping vlan-config** command. To restore the default values, please use **no ip igmp snooping vlan-config** with specified parameters.

Syntax

ip igmp snooping vlan-config *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **ltime** *leave-time*]

no ip igmp snooping vlan-config *vlan-id-list* [**rtime** | **mtime** | **ltime**]

Parameter

vlan-id-list—— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

router-time—— The Router Port Aging Time. Within this time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more. Valid values are from 60 to 600 in seconds, and the default value is 300 seconds.

member-time—— The Member Port Aging Time. Within this time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more. Valid values are from 60 to 600 in seconds, and the default value is 260 seconds.

leave-time—— The Leave Time. Valid values are from 1 to 30 in seconds, and the default value is 1 second. When the switch receives a leave message from a port to leave a multicast group, it will wait for a Leave Time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

- If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends.
- The Leave Time mechanism will not take effect when Fast Leave takes effect.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IGMP Snooping function and modify Router Port Aging Time as 300 seconds, Member Port Aging Time as 200 seconds for VLAN 1-3:

```
Switch(config)# ip igmp snooping vlan-config 1-3 rtime 300
```

```
Switch(config)# ip igmp snooping vlan-config 1-3 mtime 200
```

27.6 ip igmp snooping vlan-config (immediate-leave)

Description

This command is used to enable the Fast Leave feature for specific VLANs.

To disable Fast Leave on the VLANs, please use **no ip igmp snooping vlan-config *vlan-id-list* immediate-leave** command. This function is disabled by default.

Syntax

ip igmp snooping vlan-config *vlan-id-list* immediate-leave

no ip igmp snooping vlan-config *vlan-id-list* immediate-leave

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Fast Leave for VLAN 1-3:

```
Switch(config)# ip igmp snooping vlan-config 1-3 immediate-leave
```

27.7 ip igmp snooping vlan-config (report-suppression)

Description

This command is used to enable the IGMP Report Suppression function for specific VLANs. When enabled, the switch will only forward the first IGMP report message for each multicast group to the IGMP querier and suppress subsequent IGMP report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the IGMP querier. To disable the IGMP report suppression function and forward all the IGMP reports to the Layer 3 device in specific VLANs, please use **no ip igmp snooping vlan-config *vlan-id-list* report-suppression** command. This function is disabled by default.

Syntax

ip igmp snooping vlan-config *vlan-id-list* report-suppression

no ip igmp snooping vlan-config *vlan-id-list* report-suppression

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IGMP Report Suppression for VLAN 1-3:

```
Switch(config)# ip igmp snooping vlan-config 1-3 report-suppression
```

27.8 ip igmp snooping vlan-config (router-ports-forbidd)

Description

This command is used to forbid the specified ports as being router ports in the specified VLAN(s). To delete the forbidden router ports, please use **no ip igmp snooping vlan-config *vlan-id-list* router-ports-forbidd** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* router-ports-forbidd interface { gigabitEthernet *port-list* | port-channel *port-channel-list* }
no ip igmp snooping vlan-config *vlan-id-list* router-ports-forbidd interface [gigabitEthernet *port-list* | port-channel *port-channel-list*]

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list — Forbid the specified ports as being router ports. Packets sent from multicast routers to these ports will be discarded.

port-channel-list — Forbid the specified port-channels as being router ports. Packets sent from multicast routers to these port-channels will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Forbid the Ethernet ports 1/0/1-3 as being router ports in VLAN 1 :

```
Switch(config)# ip igmp snooping vlan-config 1 router-ports-forbidd  
interface gigabitEthernet 1/0/1-3
```

27.9 ip igmp snooping vlan-config (rport interface)

Description

This command is used to specify the static router ports for specific VLANs. To delete the static router ports, please use **no ip igmp snooping vlan-config *vlan-id-list* rport interface** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* rport interface { **gigabitEthernet *port-list* | **port-channel** *port-channel-list* }**
no ip igmp snooping vlan-config *vlan-id-list* rport interface { **gigabitEthernet *port-list* | **port-channel** *port-channel-list* }**

Parameter

vlan-id-list—— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list—— The list of Ethernet ports.

port-channel-list—— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the router port as 1/0/1 for VLAN 1-2:

```
Switch(config)# ip igmp snooping vlan-config 1-2 rport interface  
gigabitEthernet 1/0/1
```

27.10 ip igmp snooping vlan-config (static)

Description

This command is used to configure interfaces to statically join a multicast group. To remove interfaces from a static multicast group, please use **no ip igmp snooping vlan-config *vlan-id-list* static** command.

Syntax

```
ip igmp snooping vlan-config vlan-id-list static ip interface  
{ gigabitEthernet port-list | port-channel port-channel-list }  
no ip igmp snooping vlan-config vlan-id-list static ip interface  
{ gigabitEthernet port-list | port-channel port-channel-list }
```

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

ip — Specify the IP address of the multicast group that the hosts want to join.

port-list — The list of Ethernet ports.

port-channel-list — The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure port ports 1/0/1-3 in VLAN 2 to statically join multicast group 225.0.0.1:

```
Switch(config)# ip igmp snooping vlan-config 2 static 225.0.0.1 interface  
gigabitEthernet 1/0/1-3
```

27.11 ip igmp snooping vlan-config (querier)

Description

This command is used to enable the IGMP Snooping Querier feature for specific VLANs. To disable the IGMP Snooping Querier feature on the VLANs, please use **no ip igmp snooping vlan-config** *vlan-id-list* **querier** command without any parameters. To restore the default values, please use **no ip igmp snooping vlan-config** *vlan-id-list* **querier** command with specified parameters.

Syntax

```
ip igmp snooping vlan-config vlan-id-list querier [max-response-time  
response-time | query-interval interval] general-query source-ip ip-addr |  
last-member-query-count count | last-member-query-interval interval]  
no ip igmp snooping vlan-config vlan-id-list querier [max-response-time |  
query-interval | general-query source-ip | last-member-query-count ]
```

Parameter

vlan-id-list—— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

response-time—— The host's maximum response time to general query messages. Valid values are from 1 to 25 seconds, and the default value is 10 seconds.

query-interval *interval*—— The interval between general query messages sent by the switch. Valid values are from 10 to 300 seconds, and the default value is 60 seconds.

ip-addr—— The source IP address of the general query messages sent by the switch. It should be a unicast address. By default, it is 0.0.0.0.

count—— The number of group-specific queries to be sent. With IGMP Snooping Querier enabled, when the switch receives an IGMP leave message, it obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out group-specific queries to this multicast group through the port receiving the leave message. If specified count of group-specific queries are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table. Valid values are from 1 to 5, and the default value is 2.

last-member-query-interval *interval*—— The interval between group-specific queries.. Valid values are from 1 to 5 seconds, and the default value is 1 second.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IGMP Snooping Querier for VLAN 3, and configure the query interval as 100 seconds:

```
Switch(config)# ip igmp snooping vlan-config 3 querier
```

```
Switch(config)# ip igmp snooping vlan-config 3 querier query interval 100
```

27.12 ip igmp snooping vlan-config drop-unknown



Note: This command is only available on certain devices.

Description

The **ip igmp snooping vlan-config drop-unknown** command is used to enable the drop-unknown function for the specified VLAN. When enabled, unregistered IPv4 multicast traffic within this VLAN will be discarded. To disable this function, please use the **no ip igmp snooping vlan-config drop-unknown** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **drop-unknown**

no ip igmp snooping vlan-config *vlan-id-list* **drop-unknown**

Parameter

vlan-id-list — Single VLAN or VLAN range, maximum length 64 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable drop-unknown for VLAN 1:

```
Switch(config)# ip igmp snooping vlan-config 1 drop-unknown
```

27.13 ip igmp snooping vlan-config route-unknown



Note: This command is only available on certain devices.

Description

The **ip igmp snooping vlan-config route-unknown** command is used to enable the route-unknown function for the specified VLAN. When enabled, unregistered multicast traffic in this VLAN will be forwarded to IGMP snooping router ports. To disable this function, please use the **no ip igmp snooping vlan-config route-unknown** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* route-unknown

no ip igmp snooping vlan-config *vlan-id-list* route-unknown

Parameter

vlan-id-list — Single VLAN or VLAN range, maximum length 64 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable route-unknown for VLAN 1:

```
Switch(config)# ip igmp snooping vlan-config 1 route-unknown
```

27.14 ip igmp snooping vlan-config ssdp-flood

Description

The **ip igmp snooping vlan-config ssdp-flood** command is used to enable the unconditional SSDP flooding on the specified port. Since the cause of SSDP packet loss in user scenarios is the enabling of multicast and drop unknown, this function can only take effect normally when both the current VLAN multicast and global multicast are enabled.

After enabling, if IGMP snooping for the VLAN and globally is detected to be enabled, a dedicated multicast group is created and all ports within the VLAN are joined to this group. This created group cannot be manually modified or

adjusted by the user, but the member information can be adjusted by adding or removing ports from the VLAN.

Syntax

ip igmp snooping vlan-config *vlan list* ssdp-flood

Parameter

vlan list— The VLAN on which this function needs to be enabled.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

After enabling IGMP snooping globally and on VLAN 1, enable unconditional SSDP flooding on VLAN 1:

```
Switch(config)# ip igmp snooping vlan-config 1 ssdp-flood
```

27.15 ip igmp snooping vlan-config querier-election

Description

The **ip igmp snooping vlan-config querier-election** command is used to enable the querier-election function for the specified VLAN(s). To disable this function, please use **no ip igmp snooping vlan-config querier-election** command. The default value is 2. The default robustness value for a querier is 2. When the local device is not the elected querier, the robustness value is used to calculate the query interval of the current elected querier. The calculation formula is: Elected Querier Interval = (queryInterval * robustness) + maxResponseTime / 2.

Syntax

ip igmp snooping vlan-config *vlan-id-list* querier robustness *robustness*
no ip igmp snooping vlan-config *vlan-id-list* querier robustness

Parameter

vlan-id-list — A single VLAN ID or a VLAN ID range. Maximum length: 64 characters.

robustness — The robustness value of the querier. Value range: 1 to 255 (integer).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the querier robustness value for VLAN 1 to 5:

```
Switch(config)# ip igmp snooping vlan-config 1 querier robustness 5
```

27.16 ip igmp snooping querier robustness

Description

The **ip igmp snooping querier robustness** command is used to configure the robustness value for the querier. To disable this function, please use **no ip igmp snooping querier robustness** command without any parameters. By default, the querier-election function is disabled for VLANs.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **querier-election**

no ip igmp snooping vlan-config *vlan-id-list* **querier-election**

Parameter

vlan-id-list — A single VLAN ID or a VLAN ID range. Maximum length: 64 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the querier-election function for VLAN 1:

```
Switch(config)# ip igmp snooping vlan-config 1 querier-election
```

27.17 ip igmp snooping (interface)

Description

The **ip igmp snooping** command is used to enable the IGMP Snooping function for the desired port. To disable the IGMP Snooping function, please use **no ip igmp snooping** command.

Syntax

ip igmp snooping

no ip igmp snooping

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP Snooping function of port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
```

```
Switch(config-if)# ip igmp snooping
```

27.18 ip igmp snooping max-groups

Description

The **ip igmp snooping max-groups** command is used to configure the maximum number of groups that a port can join in. The **ip igmp snooping max-groups action** is used to configure the action that the port takes when it receives an IGMP report message and the maximum number of entries is in the forwarding table. To remove the maximum group limitation and return to

the default of no limitation on the specified port, please use the **no ip igmp snooping max-groups** command. To return to the default action of dropping the report, please use the **no ip igmp snooping max-groups action** command. These commands only apply to the dynamic multicast groups.

Syntax

```
ip igmp snooping max-groups maxgroup  
ip igmp snooping max-groups action { drop | replace }  
no ip igmp snooping max-groups  
no ip igmp snooping max-groups action
```

Parameter

maxgroup—— Specify the maximum numbers of groups that the port can join. It ranges from 0 to 1000 and the default value is 1000.

drop —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the port will not join any new multicast group.

replace —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the maximum numbers of groups that ports 1/0/2-5 can join as 10, and configure the throttling action as replace:

```
Switch(config)#interface range gigabitEthernet 1/0/2-5  
Switch(config-if-range)#ip igmp snooping max-groups 10  
Switch(config-if-range)#ip igmp snooping max-groups action replace
```

27.19 ip igmp snooping immediate-leave

Description

The **ip igmp snooping immediate-leave** command is used to configure the Fast Leave function for port. To disable the Fast Leave function, please use **no ip igmp snooping immediate-leave** command.

Syntax

ip igmp snooping immediate-leave
no ip igmp snooping immediate-leave

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Fast Leave function for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# ip igmp snooping immediate-leave
```

27.20 ip igmp snooping authentication



Note: This command is only available on certain devices.

Description

The **ip igmp snooping authenticaiton** command is used to authenticate the users who want to join the limited multicast source. To disable the multicast authentication, please use **no ip igmp snooping authentication** command.

Syntax

ip igmp snooping authentication
no ip igmp snooping authentication

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

The IGMP Authentication feature will take effect only when AAA function is enabled and the RADIUS server is configured. For how to enable AAA function and configure RADIUS server, please refer to [aaa enable](#) and [radius-server host](#).

Example

Enable IGMP authentication on port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# ip igmp snooping authentication
```

27.21 ip igmp snooping accounting



Note: This command is only available on certain devices.

Description

The **ip igmp snooping accounting** command is used to enable IGMP accounting globally. To disable the IGMP accounting, please use **no ip igmp snooping accounting** command.

Syntax

```
ip igmp snooping accounting
no ip igmp snooping accounting
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP accounting globally:

```
Switch(config)# ip igmp snooping accounting
```

27.22 ip igmp snooping tcn

Description

The **ip igmp snooping tcn** command is used to globally enable the TCN flood for IGMP function. When enabled, IGMP snooping will respond to Topology Change Notifications (TCN). To disable this function, please use the **no ip igmp snooping tcn** command.

Syntax

ip igmp snooping tcn
no ip igmp snooping tcn

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the TCN flood for IGMP function:

```
Switch(config)# ip igmp snooping tcn
```

27.23 ip igmp snooping tcn flood-query-count

Description

The **ip igmp snooping tcn flood-query-count** command is used to configure the number of General Query messages that need to be received before stopping multicast flooding in TCN receive mode. To restore the default value,

please use the **no ip igmp snooping tcn flood-query-count** command. The default value is 2.

Syntax

ip igmp snooping tcn flood-query-count *count*

no ip igmp snooping tcn flood-query-count

Parameter

count — The number of General Query messages that need to be received in TCN receive mode before stopping flooding. Value range: 1 to 10 (integer).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the number of General Query messages to be received before stopping flooding in TCN receive mode to 5:

```
Switch(config)# ip igmp snooping tcn flood-query-count 5
```

27.24 ip igmp snooping tcn query-solicit

Description

The **ip igmp snooping tcn query-solicit** command is used to configure the sending of General Leave messages (gaddr=0.0.0.0), also known as Query Solicitation messages, towards router ports in TCN receive mode. To disable the sending of General Leave messages in TCN receive mode, please use the **no ip igmp snooping tcn query-solicit** command. By default, General Leave messages are not sent to router ports upon entering TCN receive mode.

Syntax

ip igmp snooping tcn query-solicit

no ip igmp snooping tcn query-solicit

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the sending of General Leave messages towards router ports in TCN receive mode:

```
Switch(config)# ip igmp snooping tcn tcn query-solicit
```

27.25 ip igmp snooping vlan-config tcn-flood

Description

The **ip igmp snooping vlan-config tcn-flood** command is used to configure unknown multicast traffic flooding within a VLAN after the VLAN enters the TCN state. To restore the default configuration, please use the **no ip igmp snooping vlan-config tcn-flood** command. By default, whether unknown multicast traffic floods after a VLAN enters the TCN state is determined by the drop-unknown configuration.

Syntax

ip igmp snooping vlan-config *vlan-id-list* tcn-flood

no ip igmp snooping vlan-config *vlan-id-list* tcn-flood

Parameter

vlan-id-list — A single VLAN ID or a VLAN ID range. Maximum length: 64 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure unknown multicast traffic flooding within VLAN 1 after VLAN 1 enters the TCN state:

```
Switch(config)# ip igmp snooping vlan-config 1 tcn-flood
```

27.26 ip igmp snooping querier tcn-query-count

Description

The **ip igmp snooping querier tcn-query-count** command is used to configure the number of General Query messages that need to be sent before stopping multicast flooding in TCN transmit mode. To restore the default value, please use the **no ip igmp snooping querier tcn-query-count** command. The default value is 2.

Syntax

ip igmp snooping tcn flood-query-count *count*

no ip igmp snooping tcn flood-query-count

ip igmp snooping vlan-config *vlan-id-list* **querier tcn-query-count** *count*

no ip igmp snooping vlan-config *vlan-id-list* **querier tcn-query-count**

Parameter

vlan-id-list—— A single VLAN ID or a VLAN ID range. Maximum length: 64 characters.

count—— The number of General Query messages that need to be received in TCN receive mode before stopping flooding. Value range: 1 to 10 (integer).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the number of General Query messages to be sent before stopping flooding in TCN transmit mode for VLAN 1 to 5:

```
Switch(config)# ip igmp snooping vlan-config 1 querier tcn-query-count 5
```

27.27 ip igmp snooping querier tcn-query-interval

Description

The **ip igmp snooping querier tcn-query-interval** command is used to configure the time interval for sending General Query messages in TCN transmit mode. To restore the default value, please use the **no ip igmp snooping querier tcn-query-interval** command. The default value is 10.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **querier tcn-query-interval** *interval*

no ip igmp snooping vlan-config *vlan-id-list* **querier tcn-query-interval**

Parameter

vlan-id-list—— A single VLAN ID or a VLAN ID range. Maximum length: 64 characters.

interval—— The time interval for sending General Query messages in TCN transmit mode. Value range: 1 to 255 seconds (integer).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time interval for sending General Query messages in TCN transmit mode for VLAN 1 to 5 seconds:

```
Switch(config)# ip igmp snooping vlan-config 1 querier tcn-query-interval 5
```

27.28 ip igmp profile

Description

The **ip igmp profile** command is used to create the configuration profile. To delete the corresponding profile, please use **no ip igmp profile** command.

Syntax

ip igmp profile *id*

no ip igmp profile *id*

Parameter

id —— Specify the id of the configuration profile, ranging from 1 to 999.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the profile 1:

```
Switch(config)# ip igmp profile 1
```

27.29 deny

Description

The **deny** command is used to configure the filtering mode of profile as deny.

Syntax

deny

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the filtering mode of profile 1 as deny:

```
Switch(config)# ip igmp profile 1
Switch(config-igmp-profile)#deny
```

27.30 permit

Description

The **permit** command is used to configure the filtering mode of profile as permit.

Syntax

permit

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the filtering mode of profile 1 as permit:

```
Switch(config)# ip igmp profile 1
Switch(config-igmp-profile)#permit
```

27.31 range

Description

The **range** command is used to configure the range of the profile's filtering multicast address. To delete the corresponding filtering multicast address, please use **no range** command. A profile contains 16 filtering IP-range entries at most.

Syntax

range *start-ip end-ip*
no range *start-ip end-ip*

Parameter

start-ip—— The start filtering multicast IP address.

end-ip—— The end filtering multicast IP address.

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure one of the filter multicast address entry as range 225.1.1.1 to 226.3.2.1 in profile 1:

```
Switch(config)# ip igmp profile 1
Switch(config-igmp-profile)#range 225.1.1.1 226.3.2.1
```

27.32 ip igmp filter

Description

The **ip igmp filter** command is used to bind the specified profile to the interface. To delete the binding, please use **no ip igmp filter** command.

Syntax

ip igmp filter *profile-id*

no ip igmp filter

Parameter

profile-id—— Specify the profile ID, ranging from 1 to 999.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind profile 1 to interface gigabitEthernet 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# ip igmp filter 1
```

27.33 clear ip igmp snooping statistics

Description

The **clear ip igmp snooping statistics** command is used to clear the statistics of the IGMP packets.

Syntax

clear ip igmp snooping statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the statistics of the IGMP packets:

```
Switch(config)# clear ip igmp snooping statistics
```

27.34 show ip igmp snooping

Description

The **show ip igmp snooping** command is used to display the global configuration of IGMP snooping.

Syntax

show ip igmp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of IGMP:

```
Switch# show ip igmp snooping
```

27.35 show ip igmp snooping interface

Description

The **show ip igmp snooping interface** command is used to display the port configuration of IGMP snooping. If no interface is specified, it displays all interfaces' IGMP snooping configurations.

Syntax

```
show ip igmp snooping interface [ gigabitEthernet [port-list] |  
port-channel [ port-channel-list ] ] { authentication | basic-config |  
max-groups | packet-stat }
```

Parameter

port-list — The list of Ethernet ports.

Port-channel-list — The list of port channels.

authentication | **basic-config** | **max-groups** | **packet-stat** — The related configuration information selected to display.

Note: Authentication is only available on certain devices.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP basic configuration configuration of all ports and port channels:

```
Switch# show ip igmp snooping interface basic-config
```

Display the IGMP basic configuration of port 1/0/2:

```
Switch# show ip igmp snooping interface gigabitEthernet 1/0/2  
basic-config
```

Display the IGMP packet statistics of ports 1/0/1-4:

```
Switch# show ip igmp snooping interface gigabitEthernet 1/0/1-4  
packet-stat
```


27.36 show ip igmp snooping vlan

Description

The **show ip igmp snooping vlan** command is used to display the VLAN configuration of IGMP snooping.

Syntax

show ip igmp snooping vlan [*vlan-id*]

Parameter

vlan-id——The VLAN ID selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP snooping configuration information of VLAN 2:

```
Switch# show ip igmp snooping vlan 2
```

27.37 show ip igmp snooping groups

Description

The **show ip igmp snooping groups** command is used to display the information of all IGMP snooping groups. It can be extended to some other commands to display the dynamic and static multicast information of a selected VLAN.

Syntax

show ip igmp snooping groups [*vlan* *vlan-id*] [*multicast_addr* | count | dynamic | dynamic count | static | static count]

Parameter

vlan-id——The VLAN ID selected to display the information of all multicast items.

multicast_addr—— IP address of the multicast group.

count—— The numbers of all multicast groups.

dynamic—— Display dynamic multicast groups.

dynamic count—— The numbers of all dynamic multicast groups.

static—— Display static multicast groups.

static count—— The numbers of all static multicast groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all IGMP snooping groups:

```
Switch#show ip igmp snooping groups
```

Display all the multicast entries in VLAN 5:

```
Switch(config)#show ip igmp snooping groups vlan 5
```

Display the count of multicast entries in VLAN 5:

```
Switch(config)#show ip igmp snooping groups vlan 5 count
```

Display the dynamic multicast groups of VLAN 5

```
Switch(config)#show ip igmp snooping groups vlan 5 dynamic
```

Display the static multicast groups of VLAN 5

```
Switch(config)#show ip igmp snooping groups vlan 5 static
```

Display the count of dynamic multicast entries of VLAN 5

```
Switch(config)#show ip igmp snooping groups vlan 5 dynamic count
```

Display the count of static multicast entries of VLAN 5

```
Switch(config)#show ip igmp snooping groups vlan 5 static count
```

27.38 show ip igmp profile

Description

The **show ip igmp profile** command is used to display the configuration information of all the profiles or a specific profile.

Syntax

```
show ip igmp profile [ id ]
```

Parameter

id—— Specify the ID of the profile, ranging from 1 to 999.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of all profiles:

```
Switch(config)# show ip igmp profile
```

Chapter 28 Layer 3 IGMP Commands (Only for Certain Devices)

28.1 ip igmp (global)

Description

The **ip igmp** command is used to enable IGMP globally. To disable the IGMP function, please use **no ip igmp** command.

Syntax

ip igmp

no ip igmp

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP function globally:

```
Switch(config)# ip igmp
```

28.2 ip igmp (on specific ports)

Description

The **ip igmp** command is used to enable IGMP on specific ports. To disable the IGMP function, please use **no ip igmp** command.

Syntax

ip igmp

no ip igmp

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP function on VLAN 2:

```
Switch(config)#interface vlan 2
```

```
Switch(config-if)#ip igmp
```

28.3 ip igmp header-validation

Description

The **ip igmp header-validation** command is used to enable IGMP message header validation functions: TTL (Time To Live), ToS (Type of Service), and Router Alert options. For IGMPv1, only the TTL field is validated. For IGMPv2, the TTL and Router Alert fields are validated. For IGMPv3, the TTL, ToS and Router Alert fields are validated. To disable the IGMP function, please use **no ip igmp header-validation** command.



Note: For certain models, this command is used to configure the Router Alert options only. Actual running results may vary by model/versions/regions.

Syntax

```
ip igmp header-validation [ vrf vrfname ]
```

```
no ip igmp header-validation [ vrf vrfname ]
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP message header validation:

```
Switch(config)# ip igmp header-validation
```

28.4 ip igmp join-group

Description

This command is used to configure a static group join on an interface and join the group in the kernel.



Note: Do not use the ip igmp join-group command unless it is used in a test environment.

Syntax

ip igmp join-group *group_addr* [**source** *src_addr*]

no ip igmp join-group *group_addr* [**source** *src_addr*]

Parameter

group_addr — Multicast group address to join.

src_addr — Specified multicast source for the group join.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip igmp join-group 235.0.0.1 souce 192.168.0.1
```

28.5 ip igmp mroute-proxy

Description

Configure this command on the IGMP proxy downstream interface to specify the proxy upstream interface for this interface.

Syntax

ip igmp mroute-proxy *intf_type* *intf_id*

no ip igmp mroute-proxy

Parameter

intf_type — Interface type of the specified proxy upstream interface.

intf_id — Interface ID of the specified proxy upstream interface.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip igmp mroute-proxy vlan 1
```

28.6 ip igmp offlink

Description

This command is used to allow receiving IGMP Report messages with source IP addresses not from the local network segment.

Syntax

ip igmp offlink

no ip igmp offlink

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip igmp offlink
```

28.7 ip igmp proxy unsolicited-report-interval

Description

This command is used to configure the unsolicited report interval for the proxy upstream interface. Default is 1000 milliseconds.

Syntax

ip igmp proxy unsolicited-report-interval *value*

no ip igmp proxy unsolicited-report-interval

Parameter

value — Unsolicited report interval value, in milliseconds, range 1000 to 25500.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip igmp proxy unsolicited-report-interval 1500
```

28.8 ip igmp proxy-service

Description

Configure this interface as the proxy upstream interface.

Syntax

ip igmp proxy-service

no ip igmp proxy-service

Parameter

None,

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip igmp proxy-service
```

28.9 ip igmp querier-timeout

Description

This command is used to configure the timeout period for other queriers when this interface is not the querier. Default is $(\text{robustness (default: 2)} * \text{query-interval (default: 125)}) + (\text{query-max-response-time (default: 10)} / 2) = 255$ seconds.

Syntax

ip igmp querier-timeout *value*

no ip igmp querier-timeout

Parameter

value — Querier timeout value, in seconds, range 60 to 300,

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip igmp querier-timeout 100
```

28.10 ip igmp static-group

Description

This command is used to configure a static group join on the interface.

Syntax

ip igmp static-group *group_addr* [**source** *src_addr*]

no ip igmp static-group *group_addr* [**source** *src_addr*]

Parameter

group_addr — Multicast group address to join.

src_addr — Specified multicast source for the group join.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip igmp static-group 235.0.0.1 souce 192.168.0.1
```

28.11 ip igmp version

Description

The **ip igmp version** command is used to configure IGMP version globally. To return to the default configuration IGMPv3, please use **no ip igmp version** command.

Syntax

ip igmp version {v1 | v2 | v3 }

no ip igmp version

Parameter

v1 | v2 | v3—— Specify the IGMP version. By default, it is IGMP v3.

v1: The switch works as an IGMPv1 switch. It can only process IGMPv1 messages from the host. Report messages of other versions are ignored.

v2: The switch works as an IGMPv2 switch. It can process both IGMPv1 and IGMPv2 messages from the host. IGMPv3 messages are ignored.

v3: The switch works as an IGMPv3 switch. It can process IGMPv1, IGMPv2 and IGMPv3 messages from the host.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the IGMP version as v2:

```
Switch (config-if)#ip igmp version v2
```

28.12 ip igmp

last-member-query-count

Description

The **ip igmp last-member-query-count** command is used to configure the number of times special group query messages sent on the specified interface. To restore the default value, please use **no ip igmp last-member-query-count** command.

Syntax

ip igmp last-member-query-count *count*

no ip igmp last-member-query-count

Parameter

count: The number of times IGMP group-specific query messages are sent, ranging from 1-20. The default value is 2.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the number of times special group query messages sent on VLAN 2 as 3:

```
Switch (config)#interface vlan 2
```

```
Switch (config-if)#ip igmp last-member-query-count 3
```

28.13 ip igmp

last-member-query-interval

Description

The **ip igmp last-member-query-interval** command is used to configure the time interval for sending special group query messages on the specified interface. To restore the default value, please use **no ip igmp last-member-query-interval** command.

Syntax

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval

Parameter

interval: The interval for sending IGMP group-specific query messages. The value range is 10-255 (1/10 second). The default value is 10 (1/10 second).

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time interval for sending special group query messages sent on VLAN 2 to 2 seconds:

```
Switch (config)#interface vlan 2
Switch (config-if)#ip igmp last-member-query-interval 20
```

28.14 ip igmp query-interval

Description

The **ip igmp query-interval** command is used to configure the IGMP general query interval on a specified interface. To restore the default value, please use **no ip igmp query-interval** command.

Syntax

ip igmp query-interval *interval*

no ip igmp query-interval

Parameter

interval: The time interval for sending IGMP general query messages on the specified interface. The value range is 1-3600 seconds. The default value is 125 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the interval for sending IGMP general query messages on VLAN 2 to 50 seconds:

```
Switch (config)#interface vlan 2
Switch (config-if)#ip igmp query-interval 50
```

28.15 ip igmp

query-max-response-time

Description

The **ip igmp query-max-response-time** command is used to configure the maximum response time to IGMP general query messages on the specified interface. To restore the default value, please use **no ip igmp query-max-response-time** command.

Syntax

ip igmp query-max-response-time *time*
no ip igmp query-max-response-time

Parameter

time: The maximum response time for general group query messages on the specified interface, the value range is 10-255 (1/10 seconds), the default value is 100 (1/10 seconds).

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum response time for general group query messages on VLAN 2 to 5 seconds:

```
Switch (config)#interface vlan 2
Switch (config-if)#ip igmp query-max-response-time 50
```

28.16 ip igmp robustness

Description

The **ip igmp robustness** command is used to configure the robustness coefficient on the specified interface. To restore the default value, please use **no ip igmp robustness** command.

Syntax

ip igmp robustness *robustness*

no ip igmp robustness

Parameter

robustness: Specify the IGMP robustness coefficient, the value range is 1-255, and the default value is 2.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the robustness coefficient on VLAN 2 to 3:

```
Switch (config)#interface vlan 2
Switch (config-if)#ip igmp robustness 3
```

28.17 ip igmp startup-query-interval

Description

The **ip igmp startup-query-interval** command is used to configure the time interval for sending initial query packets on the specified interface. To restore the default value, please use **no ip igmp startup-query-interval** command.

Syntax

ip igmp startup-query-interval *interval*
no ip igmp startup-query-interval

Parameter

interval: The interval for sending IGMP initial query messages. The value range is 1-300 seconds. The default value is 31 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time interval for sending initial query packets on VLAN 2 to 10 seconds:

```
Switch (config)#interface vlan 2
Switch (config-if)#ip igmp query-interval 10
```

28.18 show ip igmp

Description

The **show ip igmp** command is used to display basic IGMP information.

Syntax

```
show ip igmp [ vrf vrfname ]
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

vrfname — Virtual Routing and Forwarding instance name.

Example

Display basic IGMP information:

```
Switch(config)#show ip igmp
```

28.19 show ip igmp groups

Description

The **show ip igmp groups** command is used to display the information of all dynamic multicast groups or specified multicast groups.

Syntax

```
show ip igmp groups [ interface intf_type intf_id ] [ group_addr ] [ detail ]
show ip igmp [ vrf vrfname ] groups [ group_addr ] [ detail ]
```

Parameter

intf_type — Specified interface type to display.

intf_id — Specified interface ID to display.

group_addr — Specified multicast group member to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of dynamic multicast 224.0.2.40:

```
Switch(config)#show ip igmp groups 224.0.2.40 detail
```

28.20 show ip igmp proxy groups

Description

The **show ip igmp proxy groups** command is used to display the IGMP proxy upstream interface member group information.

Syntax

```
show ip igmp proxy groups [ interface intf_type intf_id ] [ group_addr ]  
[ detail ]
```

```
show ip igmp [ vrf vrfname ] proxy groups [ group_addr ] [ detail ]
```

Parameter

intf_type — Specified interface type to display.

intf_id — Specified interface ID to display.

group_addr — Specified multicast group member to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP proxy upstream interface member group information.

```
Switch(config)# show ip igmp proxy groups detail
```


28.21 show ip igmp interface

Description

The **show ip igmp interface** command is used to display IGMP interface status/packet statistics.

Syntax

show ip igmp interface *intf_type intf_id* [**statistic**]

Parameter

intf_type — Specified interface type to display.

intf_id — Specified interface ID to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the IGMP status/packet statistics on port 1/0/1:

```
Switch# show ip igmp interface vlan 1
```

Chapter 29 PIM Commands (Only for Certain Devices)

Protocol Independent Multicast, abbreviated as PIM, uses unicast routing information to provide multicast forwarding functions in a layer 3 network.

29.1 ip multicast-routing

Description

The **ip multicast-routing** command is used to enable the IP multicast-routing function globally. To disable this function, please use the **no ip multicast-routing** command.

Syntax

ip multicast-routing [**vrf** *vrfname*]

no ip multicast-routing [**vrf** *vrfname*]

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IP multicast-routing function globally:

```
Switch(config)#ip multicast-routing
```

29.2 ip pim (globally)

Description

The **ip pim** command is used to enable IP PIM globally. To disable the IP PIM function, please use **no ip pim** command.



Note: This command applies to L2+ switches only.

Syntax

ip pim {dense-mode | sparse-mode }
no ip pim {dense-mode | sparse-mode }

Parameter

dense-mode: Enable PIM DM globally.

sparse-mode: Enable PIM SM globally

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable PIM DM globally:

```
Switch (config)#ip pim dense-mode
```

29.3 ip pim (on specific ports)

Description

The **ip pim** command is used to configure IP PIM on a specified port. To disable the IP PIM function, please use **no ip pim** command.

Syntax

ip pim
no ip pim

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable PIM on port 2:

```
Switch (config)#interface vlan 2
```

```
Switch (config-if)#ip pim
```

29.4 ip pim dense-mode

Description

This command is used to configure the PIM DM (Dense Mode).



Note: This command applies to L3 switches only.

Syntax

```
ip pim dense-mode [vrf vrfname]
```

```
no ip pim dense-mode [vrf vrfname]
```

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config)# ip pim dense-mode vrf test
```

29.5 ip pim sparse-mode

Description

This command is used to configure PIM Sparse Mode (SM).



Note: This command applies to L3 switches only.

Syntax

```
ip pim sparse-mode [vrf vrfname]
```

```
no ip pim sparse-mode [vrf vrfname]
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim sparse-mode vrf test
```

29.6 ip pim anycast-rp

Description

Anycast RP is an extension mechanism of the PIM-SM protocol. By configuring the same anycast address for multiple physical RPs, it enables multicast sources to register nearby and receivers to join nearby, addressing issues in the traditional single-RP model such as traffic concentration, slow fault convergence, and non-optimal paths. During configuration, both the anycast-rp address and member rp addresses are recommended to be configured as loopback addresses. Each anycast-rp member device needs to be configured with all member rp addresses. When removing the configuration, you can delete the entire anycast-rp configuration or only a specific member rp configuration.

Syntax

```
ip pim anycast-rp anycast_rp_addr member_addr [vrf vrfname]  
no ip pim anycast-rp anycast_rp_addr [member_addr] [vrf vrfname]
```

Parameter

anycast_rp_addr: The anycast-rp address, representing a set of RPs.

member_addr: A member rp address within the RP set.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Assume Switch A and Switch B are building an anycast-rp. The anycast-rp address for both Switch A and Switch B is 1.1.1.1. Switch A's member-rp is 2.2.2.2, and Switch B's member-rp is 3.3.3.3. Using Switch A configuration as an example, it needs to configure all local and remote member rps:

```
Switch (config)# ip pim anycast-rp 1.1.1.1 2.2.2.2
```

```
Switch (config)# ip pim anycast-rp 1.1.1.1 3.3.3.3
```

29.7 ip pim ignore-rp-set-priority

Description

This command configures to ignore the priority field of the RP-set during RP election, which is disabled by default.

Syntax

```
ip pim ignore-rp-set-priority [vrf vrfname]
```

```
no ip pim ignore-rp-set-priority [vrf vrfname]
```

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Ignore the priority field of the RP-set during RP election:

```
Switch (config)# ip pim ignore-rp-set-priority
```

29.8 ip pim register-rate-limit

Description

This command configures the number of register messages the Designated Router (DR) can send per second. Register messages exceeding this limit will be dropped. Default is 0, meaning unlimited.

Syntax

```
ip pim register-rate-limit value [vrf vrfname]
```

```
no ip pim register-rate-limit [vrf vrfname]
```

Parameter

Value: Range for the number of register messages sent per second, ranging from 1 - 65535.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Ignore the priority field of the RP-set during RP election:

```
Switch (config)# ip pim ignore-rp-set-priority
```

29.9 ip pim register-rp-reachability

Description

This command configures the checking the RP reachability for register messages. Default is enabled. By default, it is not displayed in show running-config. It will appear after being disabled with the no command.

Syntax

```
ip pim register-rp-reachability [ vrf vrfname]
```

```
no ip pim register-rp-reachability [ vrf vrfname]
```

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config)# ip pim register-rp-reachability
```

29.10 ip pim register-source

Description

This command configures the IP header source address for register messages sent by the Designated Router (DR), which can be configured as an IP address or an interface (using the interface's IP address). The configured source address should be unicast reachable to the RP to ensure proper PIM-SM registration/register-stop flow. By default, the source address is the RPF interface address towards the multicast source.

Syntax

```
ip pim register-source {ip_addr | interface intf_type intf_id} [vrf vrfname]  
no ip pim register-source [vrf vrfname]
```

Parameter

ip_addr: IP address to be used as the source address for register messages.

intf_type: Interface type to be used for the register message source address.

intf_id: Interface ID to be used for the register message source address.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim register-source 192.168.10.1  
Switch(config)# ip pim register-source interface loopback 1  
Switch(config)# no ip pim register-source
```

29.11 ip pim register-suppression

Description

This command configures the time (in seconds) for which the Designated Router (DR) stops sending data-encapsulated registers to the RP after receiving a register-stop message. Default is 60 seconds.

Syntax

```
ip pim register-suppression value [vrf vrfname]
```


no ip pim register-suppression [vrf *vrfname*]

Parameter

value: Registration suppression time, in seconds, range 1 - 65535.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim register-suppression 100
```

29.12 ip pim router-id

Description

This command configures the PIM router-id, which uniquely identifies a PIM device.

Syntax

ip pim router-id *router-id* [vrf *vrfname*]

no ip pim router-id [vrf *vrfname*]

Parameter

router-id: Dotted-decimal parameter.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim router-id 1.2.3.4
```

29.13 ip pim bsr-candidate

Description

This command is used to configure a candidate BSR on the interface.

Syntax

```
ip pim bsr-candidate interface intf_type intf_id [hash-mask-length]  
[priority] [interval] [vrf vrfname]  
no ip pim bsr-candidate [vrf vrfname]
```

Parameter

intf_type: Interface type used for C-BSR.

intf_id: Interface ID used for C-BSR.

hash-mask-length: Hash mask length used to map multicast group addresses to RPs. Default is 30, range 0 - 32.

priority: C-BSR election priority, where a higher value wins. Default is 0, range 0-255.

interval: Interval for sending PIM BSR messages, in seconds. Default is 60 seconds, range 1 - 16383.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim bsr-candidate int loopback 1 vrf test  
Switch(config)# no ip pim bsr-candidate vrf test
```

29.14 ip pim rp-candidate

Description

This command is used to configure a candidate RP.

Syntax

```
ip pim rp-candidate interface intf_type intf_id group_addr group_mask  
[interval] [priority] [vrf vrfname]
```

no ip pim rp-candidate interface *intf_type intf_id group_addr group_mask*
[**vrf** *vrfname*]

Parameter

intf_type —— Interface type used for C-RP.
intf_id —— Interface ID used for C-RP.
group_addr —— Multicast group address.
group_mask —— Multicast group mask.
interval —— C-RP advertisement message sending interval. Default is 60 seconds, range 1 - 16383.
priority —— C-RP election priority, where a lower value wins. Default is 192, range 0-255.
vrfname —— Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim rp-candidate interface loopback 1 235.0.0.1  
255.0.0.0 vrf test
```

29.15 ip pim rp-register-kat

Description

This command is used to configure the KeepAlive Timer (KAT) time used by the RP to monitor register messages and multicast routing state. Default value is $3 * \text{registerSuppression}(\text{default:60}) + \text{reg\_probe}(\text{default:5}) = 185$ seconds.

Syntax

ip pim rp-register-kat *value* [**vrf** *vrfname*]
no ip pim rp-register-kat [**vrf** *vrfname*]

Parameter

value —— KAT time, in seconds, range 1 - 65535.
vrfname —— Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim rp-register-kat 100
```

29.16 ip pim spt-threshold

Description

This command is used to configure the device to automatically switch to the SPT forwarding tree. Default is enabled. By default, it is not displayed in show running-config. It will appear after being disabled with the no command.

Syntax

```
ip pim spt-threshold [ vrf vrfname]
```

```
no ip pim spt-threshold [ vrf vrfname]
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim spt-threshold
```

29.17 ip pim rp-address

Description

This command is used to configure a static RP.

Syntax

```
ip pim rp-address rp_addr group_addr group_mask [ override ] [ vrf  
vrfname ]
```

no ip pim rp-address *rp_addr group_addr group_mask* [**vrf** *vrfname*]

Parameter

rp_addr: IP address of the RP.

group_addr: Multicast group address.

group_mask: Multicast group mask.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim rp-address 1.1.1.1 235.0.0.1 255.255.255.0 vrf test
```

29.18 ip pim ssm

Description

This command is used to configure the PIM-SSM

Syntax

ip pim ssm { *group_addr group_mask* | **default** } [**vrf** *vrfname*]

no ip pim ssm { *group_addr group_mask* | **default** } [**vrf** *vrfname*]

Parameter

group_addr — Multicast group address.

group_mask — Multicast group mask.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim ssm 235.0.0.0 255.0.0.0 vrf test
```

29.19 ip pim bsr-border

Description

This command is used to configure the management border of the BSR domain.

Syntax

ip pim bsr-border
no ip pim bsr-border

Parameter

None

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the BSR management border on VLAN interface 2:

```
Switch(config)# ip pim bsr-border
```

29.20 ip pim exclude-genid

Description

This command is used to configure the interface to send PIM hello messages without the Generation ID field. Default is disabled.

Syntax

ip pim exclude-genid
no ip pim exclude-genid

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip pim exclude-genid
```

29.21 ip pim dr-priority

Description

This command is used to configure the priority of the designated router (DR).

Syntax

ip pim dr-priority *pri*

no ip pim dr-priority

Parameter

pri: DR priority, ranging from 0 to 4294967295. Its default value is 1.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DR priority on VLAN interface 2 to 100:

```
Switch(config)#interface vlan 2
```

```
Switch(config-if)# ip pim dr-priority 100
```

29.22 ip pim hello-holdtime

Description

This command is used to configure the aging time for PIM neighbors on the interface. Default is $3.5 * \text{hello-interval}(\text{default:30}) = 105$ seconds.

Syntax

ip pim hello-holdtime *value*

no ip pim hello-holdtime

Parameter

value: hello-holdtime value, in seconds, range 1 - 65535.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ip pim hello-holdtime 100
```

29.23 ip pim hello-interval

Description

The **ip pim hello-interval** command is used to configure the time interval for sending Hello messages on the interface. To restore the default value, please use **no ip pim hello-interval** command.

Syntax

ip pim hello-interval *interval*

no ip pim hello-interval

Parameter

interval: The time interval for sending Hello messages, ranging from 1 to 18725 seconds. The default value is 30 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the interval for VLAN interface 2 to send Hello messages to 100 seconds:

```
Switch (config)#interface vlan 2
```

```
Switch (config-if)# ip pim hello-interval 100
```

29.24 ip pim passive

Description

The **ip pim hello-interval** command is used to configure the interface to enter passive mode, where it stops actively sending PIM messages. Default is disabled.

Syntax

ip pim passive

no ip pim passive

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ip pim passive
```

29.25 ip pim propagation-delay

Description

This command is used to configure the propagation-delay field in the LAN Prune Delay option of PIM hello messages sent on the interface. Default is 500 milliseconds.

Syntax

ip pim propagation-delay *value*

no ip pim propagation-delay

Parameter

value: propagation-delay value, in milliseconds, range 1 - 32767.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ip pim propagation-delay 1000
```

29.26 ip pim state-refresh

Description

This command is used to configure the interval at which State-Refresh messages are sent on the interface in PIM Dense Mode. Default is 60 seconds.

Syntax

ip pim state-refresh origination-interval *value*

no ip pim state-refresh origination-interval

Parameter

value — State-Refresh message sending interval, in seconds, range 1 - 100.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ip pim state-refresh origination-interval 100
```

29.27 ip pim unicast-bsm

Description

This command is used to configure the interface to reply with a unicast PIM bootstrap message upon receiving a PIM hello message from a new neighbor. Default is disabled.

Syntax

ip pim unicast-bsm

no ip pim unicast-bsm

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ip pim unicast-bsm
```

29.28 ip pim join-prune-interval

Description

This command is used to configure the interval for sending join/prune messages on the interface. To restore the default configuration, please use the **no ip pim join-prune-interval** command.

Syntax

ip pim join-prune-interval *interval*

no ip pim join-prune-interval

Parameter

interval: The interval for sending join/prune messages, ranging from 1 to 18724 seconds. The default value is 60 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the interval for sending join/prune messages to 100 seconds.

```
Switch (config)#interface vlan 2
```

```
Switch (config-if)# ip pim join-prune-interval 100
```

29.29 show ip multicast

Description

The **show ip multicast** command is used to display the global configuration information of IP multicast.

Syntax

show ip multicast [**vrf** *vrfname*]

Parameter

vrfname: Virtual Routing and Forwarding instance name

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration information of IP multicast:

```
Switch(config)#show ip multicast
```

29.30 show ip mroute

Description

The **show ip mroute** command is used to display the multicast routing table.

Syntax

show ip mroute [**vrf** *vrfname*] [[**group** *ip-addr*] | [**source** *ip-addr*] | **detail** | **static** [**source** *source-ip*]] [**summary**]]

Parameter

vrfname: Virtual Routing and Forwarding instance name

group ip-addr: Multicast group IP address

source ip-addr: Multicast source IP address

detail: Displays detailed multicast routing table

static [**source** *source-ip*]: Displays all static multicast routing entries or static multicast routing entries with a specified source IP address

summary: Displays summary information of multicast routing entries

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all multicast routing entries:

```
Switch(config)#show ip mroute
```

29.31 show ip pim

Description

The **show ip pim** command is used to display the IP PIM global configuration related information.

Syntax

```
show ip pim [ vrf vrfname ]
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP PIM global configuration related information:

```
Switch(config)# show ip pim
```

29.32 show ip pim interface

Description

The **show ip pim interface** command is used to display brief/detailed PIM interface information of specified interfaces or all interfaces.

Syntax

```
show ip pim interface { intf_type intf_id | all } [ detail ]
```

```
show ip pim vrf vrfname interface all [ detail ]
```

Parameter

intf_type — Specifies the interface type to display.

intf_id — Specifies the interface ID to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim vrf test interface all detail
```

29.33 show ip pim local-MemberShip

Description

The **show ip pim interface** command is used to display PIM group membership information.

Syntax

show ip pim local-MemberShip [**interface** *intf_type intf_id*]

show ip pim vrf *vrfname* **local-MemberShip**

Parameter

intf_type — Specifies the interface type to display.

intf_id — Specifies the interface ID to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim local-MemberShip interface vlan 1
```

29.34 show ip pim mroute

Description

This command is used to PIM multicast route related information.

Syntax

```
show ip pim [ vrf vrfname ] mroute [ group group_addr ] [ source src_addr ]  
detail
```

Parameter

group_addr ——— Specifies the multicast group to query.
src_addr ——— Specifies the multicast source to query.
vrfname ——— Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim vrf test mroute group 235.0.0.1 source  
192.168.101.1 detail
```

29.35 show ip pim neighbor

Description

The **show ip pim neighbor** command is used to display the IP PIM neighbor information.

Syntax

```
show ip pim neighbor [ interface intf_type intf_id ] [ detail ]  
show ip pim vrf vrfname neighbor [ detail ]
```

Parameter

intf_type ——— Specifies the interface type to display.
intf_id ——— Specifies the interface ID to display.
vrfname ——— Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim neighbor interfave vlan 1
```

29.36 show ip pim nexthop

Description

This command is used to PIM next-hop related information.

Syntax

```
show ip pim [ vrf vrfname ] nexthop
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim nexthop
```

29.37 show ip pim statistic

Description

The **show ip pim statistic** command is used to display the IP PIM statistic information.

Syntax

```
show ip pim statistic [ interface intf_type intf_id ]
```

```
show ip pim [ vrf vrfname ] statistic
```


Parameter

intf_type — Specifies the interface type to display.
intf_id — Specifies the interface ID to display.
vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display packet count information of all PIM interfaces:

```
Switch(config)#show ip pim vrf test statistic
```

29.38 show ip pim bsr-router

Description

This command is used to view the information of candidate BSRs and candidate RPs.

Syntax

```
show ip pim [ vrf vrfname ] bsr-router
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim vrf test bsr-router
```

29.39 show ip pim rp mapping

Description

This command is used to view the multicast group information mapped to RPs.

Syntax

```
show ip pim [ vrf vrfname ] rp mapping [ rp_addr | candidate | static ]
```

Parameter

rp_addr ——— Specifies the RP address to query.
vrfname ——— Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim rp mapping
```

29.40 show ip pim rp-hash

Description

This command is used to view the the hash result of the specified multicast group.

Syntax

```
show ip pim [ vrf vrfname ] rp hash group_addr
```

Parameter

group_addr ——— Specifies the multicast group to query.
vrfname ——— Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ip pim vrf test rp hash 235.0.0.1
```

29.41 show ip pim ssm

Description

This command is used to display PIM SSM configuration information.

Syntax

```
show ip pim [ vrf vrfname ] ssm
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Privileged EXEC Mode and Any Configuration Mode

Example

```
Switch(config)# show ip pim vrf test ssm
```

Chapter 30 PIM6 Commands (Only for Certain Devices)

30.1 ipv6 multicast-routing

Description

The **ipv6 multicast-routing** command is used to enable the IPv6 multicast-routing function globally. To disable this function, please use the **no ipv6 multicast-routing** command.

Syntax

ipv6 multicast-routing [**vrf** *vrfname*]

no ipv6 multicast-routing [**vrf** *vrfname*]

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IPv6 multicast-routing function globally:

```
Switch(config)#ipv6 multicast-routing
```

30.2 ipv6 pim anycast-rp

Description

Anycast RP is an extension mechanism of the PIM-SM protocol. By configuring the same anycast address for multiple physical RPs, it enables multicast sources to register with the nearest RP and receivers to join the nearest RP, addressing issues in the traditional single-RP model such as traffic concentration, slow fault convergence, and suboptimal paths.

During configuration, it is recommended to configure the anycast-rp and member RP addresses as loopback addresses. Each anycast-rp member device must be configured with all member RPs.

During deconfiguration, you can delete the entire anycast-rp configuration or remove only a specific member RP configuration.

Syntax

```
ipv6 pim anycast-rp anycast_rp_addr member_addr [vrf vrfname]  
no ipv6 pim anycast-rp anycast_rp_addr [member_addr] [vrf vrfname]
```

Parameter

anycast_rp_addr: The anycast-rp address, representing a set of RPs.

member_addr: A member rp address within the RP set.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Assume Switch A and Switch B form an anycast-RP. The anycast-RP address for both Switch A and Switch B is 1:1::1:1. Switch A's member-RP is 2:2::2:2, and Switch B's member-RP is 3:3::3:3.

Taking Switch A configuration as an example, both local and remote member RPs must be configured:

```
Switch(config)# ipv6 pim anycast-rp 1:1::1:1 2:2::2:2  
Switch(config)# ipv6 pim anycast-rp 1:1::1:1 3:3::3:3
```

30.3 ipv6 pim bsr-candidate

Description

This command is used to configure a candidate BSR on the interface.

Syntax

```
ipv6 pim bsr-candidate interface intf_type intf_id [hash-mask-length]  
[priority] [interval] [vrf vrfname]  
no ipv6 pim bsr-candidate [vrf vrfname]
```

Parameter

intf_type: Interface type used for C-BSR.

intf_id: Interface ID used for C-BSR.

hash-mask-length: Hash mask length used to map multicast group addresses to RPs. Default is 30, range 0 - 32.

priority: C-BSR election priority, where a higher value wins. Default is 0, range 0-255.

interval: Interval for sending PIM BSR messages, in seconds. Default is 60 seconds, range 1 - 16383.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim bsr-candidate int loopback 1 vrf test
Switch(config)# no ipv6 pim bsr-candidate vrf test
```

30.4 ipv6 pim dense-mode

Description

This command is used to configure the PIM DM.

Syntax

```
ipv6 pim dense-mode [ vrf vrfname ]
no ipv6 pim dense-mode [ vrf vrfname ]
```

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config)# ipv6 pim dense-mode vrf test
```

30.5 ipv6 pim

ignore-rp-set-priority

Description

This command configures to ignore the priority field of the RP-set during RP election, which is disabled by default.

Syntax

ipv6 pim ignore-rp-set-priority [vrf *vrfname*]

no ipv6 pim ignore-rp-set-priority [vrf *vrfname*]

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Ignore the priority field of the RP-set during RP election:

```
Switch (config)# ipv6 pim ignore-rp-set-priority
```

30.6 ipv6 pim register-rate-limit

Description

This command configures the number of register messages the Designated Router (DR) can send per second. Register messages exceeding this limit will be dropped. Default is 0, meaning unlimited.

Syntax

ipv6 pim register-rate-limit *value* [vrf *vrfname*]

no ipv6 pim register-rate-limit [vrf *vrfname*]

Parameter

Value: Range for the number of register messages sent per second, ranging from 1 - 65535.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Ignore the priority field of the RP-set during RP election:

```
Switch (config)# ipv6 pim ignore-rp-set-priority
```

30.7 ipv6 pim register-rp-reachability

Description

This command configures the checking the RP reachability for register messages. Default is enabled. By default, it is not displayed in show running-config. It will appear after being disabled with the no command.

Syntax

ipv6 pim register-rp-reachability [vrf *vrfname*]

no ipv6 pim register-rp-reachability [vrf *vrfname*]

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config)# ipv6 pim register-rp-reachability
```

30.8 ipv6 pim register-source

Description

This command configures the IP header source address of register packets sent by the Designated Router (DR). You can configure an IP address or an

interface, using the interface's IP address. The configured source address should be unicast-reachable to the RP to ensure proper PIM-SM registration and registration-stop processes. By default, the source address is the RPF interface address pointing to the multicast source.

Syntax

```
ipv6 pim register-source {ip_addr | interface intf_type intf_id} [vrf vrfname]  
no ipv6 pim register-source [vrf vrfname]
```

Parameter

ip_addr: IP address to be used as the source address for register messages.

intf_type: Interface type to be used for the register message source address.

intf_id: Interface ID to be used for the register message source address.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim register-source 2001:1::101  
Switch(config)# ipv6 pim register-source interface loopback 1  
Switch(config)# no ipv6 pim register-source
```

30.9 ipv6 pim register-suppression

Description

This command configures the time (in seconds) for which the Designated Router (DR) stops sending data-encapsulated registers to the RP after receiving a register-stop message. Default is 60 seconds.

Syntax

```
ipv6 pim register-suppression value [vrf vrfname]  
no ipv6 pim register-suppression [vrf vrfname]
```

Parameter

value: Registration suppression time, in seconds, range 1 - 65535.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim register-suppression 100
```

30.10 ipv6 pim router-id

Description

This command configures the PIM router-id, which uniquely identifies a PIM device.

Syntax

ipv6 pim router-id *router-id* [**vrf** *vrfname*]

no ipv6 pim router-id [**vrf** *vrfname*]

Parameter

router-id: Dotted-decimal parameter.

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim router-id 1.2.3.4
```

30.11 ipv6 pim rp embedded

Description

This command is used to configure embedding the RP address into IPv6 multicast addresses.

Syntax

ipv6 pim rp embedded enable [**vrf** *vrfname*]

no ipv6 pim rp embedded enable [**vrf** *vrfname*]

Parameter

vrfname: Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim rp embedded enable
```

30.12 ipv6 pim rp-address

Description

This command is used to configure a static RP.

Syntax

ipv6 pim rp-address *rp_addr group_prefix* [**override**] [**vrf** *vrfname*]

no ipv6 pim rp-address *rp_addr group_prefix* [**vrf** *vrfname*]

Parameter

rp_addr — IP address of the RP.

group_prefix — Multicast group prefix.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim rp-address 2001:1::101 ff1e::1/64
```

30.13 ipv6 pim rp-candidate

Description

This command is used to configure a candidate RP.

Syntax

ipv6 pim rp-candidate interface *intf_type intf_id group_prefix* [**interval** *interval*] [**priority** *priority*] [**vrf** *vrfname*]

no ipv6 pim rp-candidate interface *intf_type intf_id group_prefix* [**vrf** *vrfname*]

Parameter

intf_type — Interface type used for C-RP.

intf_id — Interface ID used for C-RP.

group_prefix — Multicast group prefix.

interval — C-RP advertisement packet transmission interval. Default is 60 seconds, ranging from 1 - 16383.

priority — C-RP election priority. Lower priority values take precedence. Default is 192, ranging from 0-255.

vrfname — Virtual routing and forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim rp-candidate interface loopback 1 ff1e::1/64
```

30.14 ipv6 pim rp-register-kat

Description

This command is used to configure the KeepAlive Timer (KAT) time used by the RP to monitor register messages and multicast routing state. Default value is $3 * \text{registerSuppression}(\text{default:60}) + \text{reg\_probe}(\text{default:5}) = 185$ seconds.

Syntax

ipv6 pim rp-register-kat *value* [**vrf** *vrfname*]

no ipv6 pim rp-register-kat [vrf *vrfname*]

Parameter

value — KAT time, in seconds, range 1 - 65535.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim rp-register-kat 100
```

30.15 ipv6 pim sparse-mode

Description

This command is used to configure PIM Sparse Mode (SM).

Syntax

ipv6 pim sparse-mode [vrf *vrfname*]

no ipv6 pim sparse-mode [vrf *vrfname*]

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim sparse-mode vrf test
```

30.16 ipv6 pim spt-threshold

Description

This command is used to configure the device to automatically switch to the SPT forwarding tree. Default is enabled. By default, it is not displayed in show running-config. It will appear after being disabled with the no command.

Syntax

ipv6 pim spt-threshold [**vrf** *vrfname*]

no ipv6 pim spt-threshold [**vrf** *vrfname*]

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ipv6 pim spt-threshold
```

30.17 ipv6 pim ssm

Description

This command is used to configure the PIM-SSM

Syntax

ipv6 pim ssm { *group_prefix* | **default** } [**vrf** *vrfname*]

no ipv6 pim ssm { *group_prefix* | **default** } [**vrf** *vrfname*]

Parameter

group_prefix — Multicast group prefix.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip pim ssm ff1e::1/64 vrf test
```

30.18 ipv6 pim (on specific ports)

Description

The **ipv6 pim** command is used to configure IP PIM on a specified port. To disable the IP PIM function, please use **no ipv6 pim** command.

Syntax

ipv6 pim

no ipv6 pim

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable PIM6 on port 2:

```
Switch (config)#interface vlan 2
```

```
Switch (config-if)#ipv6 pim
```

30.19 ipv6 pim bsr-border

Description

This command is used to configure to prevent the interface from sending or receiving BSR messages, used to isolate PIM domains. Disabled by default.

Syntax

ipv6 pim bsr-border

no ipv6 pim bsr-border

Parameter

None

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the BSR management border on VLAN interface 2:

```
Switch(config-if) # ipv6 pim bsr-border
```

30.20 ipv6 pim dr-priority

Description

This command is used to configure the priority of the designated router (DR).

Syntax

ipv6 pim dr-priority *pri*

no ipv6 pim dr-priority

Parameter

pri: DR priority, ranging from 0 to 4294967295. Its default value is 1.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DR priority on VLAN interface 2 to 100:

```
Switch(config)#interface vlan 2
```

```
Switch(config-if)# ipv6 pim dr-priority 100
```

30.21 ipv6 pim exclude-genid

Description

This command is used to configure the interface to send PIM hello messages without the Generation ID field. Default is disabled.

Syntax

ipv6 pim exclude-genid
no ipv6 pim exclude-genid

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 pim exclude-genid
```

30.22 ipv6 pim hello-holdtime

Description

This command is used to configure the aging time for PIM neighbors on the interface. Default is $3.5 * \text{hello-interval}(\text{default:30}) = 105$ seconds.

Syntax

ipv6 pim hello-holdtime *value*
no ipv6 pim hello-holdtime

Parameter

value:hello-holdtime value, in seconds, range 1 - 65535.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 pim hello-holdtime 100
```

30.23 ipv6 pim hello-interval

Description

The **ipv6 pim hello-interval** command is used to configure the time interval for sending Hello messages on the interface. To restore the default value, please use **no ipv6 pim hello-interval** command.

Syntax

ipv6 pim hello-interval *interval*

no ipv6 pim hello-interval

Parameter

interval: The time interval for sending Hello messages, ranging from 1 to 18725 seconds. The default value is 30 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the interval for VLAN interface 2 to send Hello messages to 100 seconds:

```
Switch (config)#interface vlan 2
Switch (config-if)# ipv6 pim hello-interval 100
```

30.24 ipv6 pim join-prune-interval

Description

This command is used to configure the interval for sending join/prune messages on the interface. To restore the default configuration, please use the **no ipv6 pim join-prune-interval** command.

Syntax

ipv6 pim join-prune-interval *value*

no ipv6 pim join-prune-interval

Parameter

value: The interval for sending join/prune messages, ranging from 1 to 18000 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the interval for sending join/prune messages to 100 seconds.

```
Switch (config)#interface vlan 2
```

```
Switch (config-if)# ipv6 pim join-prune-interval 100
```

30.25 ipv6 pim passive

Description

The **ipv6 pim hello-interval** command is used to configure the interface to enter passive mode, where it stops actively sending PIM messages. Default is disabled.

Syntax

ipv6 pim passive

no ipv6 pim passive

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ipv6 pim passive
```

30.26 ipv6 pim propagation-delay

Description

This command is used to configure the propagation-delay field in the LAN Prune Delay option of PIM hello messages sent on the interface. Default is 500 milliseconds.

Syntax

ipv6 pim propagation-delay *value*

no ipv6 pim propagation-delay

Parameter

value: propagation-delay value, in milliseconds, range 1 - 32767.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ipv6 pim propagation-delay 1000
```

30.27 ipv6 pim state-refresh

Description

This command is used to configure the interval at which State-Refresh messages are sent on the interface in PIM Dense Mode. Default is 60 seconds.

Syntax

ipv6 pim state-refresh origination-interval *value*

no ipv6 pim state-refresh origination-interval

Parameter

value — State-Refresh message sending interval, in seconds, range 1 - 100.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ipv6 pim state-refresh origination-interval 100
```

30.28 ipv6 pim unicast-bsm

Description

This command is used to configure the interface to reply with a unicast PIM bootstrap message upon receiving a PIM hello message from a new neighbor. Default is disabled.

Syntax

```
ilpv6 pim unicast-bsm  
no ipv6 pim unicast-bsm
```

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch (config-if)# ipv6 pim unicast-bsm
```

30.29 show ipv6 multicast

Description

The **show ipv6 multicast** command is used to display the global configuration information of IPv6 multicast.

Syntax

```
show ipv6 multicast [ vrf vrfname ]
```

Parameter

vrfname: Virtual Routing and Forwarding instance name

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration information of IPv6 multicast:

```
Switch(config)#show ipv6 multicast
```

30.30 show ipv6 pim

Description

The **show ipv6 pim** command is used to display the IPv6 PIM global configuration related information.

Syntax

```
show ipv6 pim [ vrf vrfname ]
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP PIM global configuration related information:

```
Switch(config)# show ipv6 pim
```

30.31 show ipv6 pim bsr-router

Description

This command is used to view the information of candidate BSRs and candidate RPs.

Syntax

show ipv6 pim [vrf *vrfname*] bsr-router

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim vrf test bsr-router
```

30.32 show ipv6 pim interface

Description

The **show ipv6 pim interface** command is used to display brief/detailed PIM interface information of specified interfaces or all interfaces.

Syntax

show ipv6 pim interface { *intf_type intf_id* | all } [detail]

show ipv6 pim vrf *vrfname* interface all [detail]

Parameter

intf_type — Specifies the interface type to display.

intf_id — Specifies the interface ID to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim vrf test interface all detail
```

30.33 show ipv6 pim

local-MemberShip

Description

The **show ipv6 pim interface** command is used to display PIM group membership information.

Syntax

show ipv6 pim local-MemberShip [**interface** *intf_type intf_id*]

show ipv6 pim vrf *vrfname* **local-MemberShip**

Parameter

intf_type — Specifies the interface type to display.

intf_id — Specifies the interface ID to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim local-MemberShip interface vlan 1
```

30.34 show ipv6 pim mroute

Description

This command is used to PIM multicast route related information.

Syntax

show ipv6 pim [**vrf** *vrfname*] **mroute** [**group** *group_addr*] [**source** *src_addr*]
detail

Parameter

group_addr — Specifies the multicast group to query.

src_addr — Specifies the multicast source to query.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim vrf test mroute group 235.0.0.1 source  
192.168.101.1 detail
```

30.35 show ipv6 pim neighbor

Description

The **show ipv6 pim neighbor** command is used to display the IP PIM neighbor information.

Syntax

show ipv6 pim neighbor [**interface** intf_type intf_id] [**detail**]

show ipv6 pim vrf *vrfname* **neighbor** [**detail**]

Parameter

intf_type — Specifies the interface type to display.

intf_id — Specifies the interface ID to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim neighbor interfave vlan 1
```

30.36 show ipv6 pim nexthop

Description

This command is used to PIM next-hop related information.

Syntax

show ipv6 pim [vrf *vrfname*] nexthop

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim nexthop
```

30.37 show ipv6 pim rp-hash

Description

This command is used to view the the hash result of the specified multicast group.

Syntax

show ipv6 pim [vrf *vrfname*] rp hash *group_addr*

Parameter

group_addr — Specifies the multicast group to query.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim vrf test rp hash ff1e::1
```

30.38 show ipv6 pim rp mapping

Description

This command is used to view the multicast group information mapped to RPs.

Syntax

```
show ipv6 pim [ vrf vrfname ] rp mapping [ rp_addr | candidate | static ]
```

Parameter

rp_addr — Specifies the RP address to query.
vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)# show ipv6 pim rp mapping
```

30.39 show ipv6 pim ssm

Description

This command is used to display PIM SSM configuration information.

Syntax

```
show ipv6 pim [ vrf vrfname ] ssm
```

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Privileged EXEC Mode and Any Configuration Mode

Example

```
Switch(config)# show ipv6 pim vrf test ssm
```

30.40 show ipv6 pim statistic

Description

The **show ipv6 pim statistic** command is used to display the IP PIM statistic information.

Syntax

show ipv6 pim statistic [**interface** *intf_type intf_id*]

show ipv6 pim [**vrf** *vrfname*] **statistic**

Parameter

intf_type — Specifies the interface type to display.

intf_id — Specifies the interface ID to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

```
Switch(config)#show ipv6 pim vrf test statistic
```

Chapter 31 Static Multicast Routing Commands (Only for Certain Devices)

Multicast routing creates multicast routing table entries based on existing unicast routing information or multicast static routing. When creating multicast routing table entries, multicast routing protocols use the RPF (Reverse Path Forward) checking mechanism to ensure that multicast data can be forwarded along the correct path. Multicast static route entries are one of the important basis for RPF inspection and are mainly used to change or connect RPF routes.

31.1 ip mroute

Description

The **ip mroute** command is used to add/modify static multicast routing entries globally. To delete the specified static multicast routing entry, please use the **no ip mroute** command.

Syntax

ip mroute { *source-address* } { *mask* } { *rpf-address* } [*distance*]

no ip mroute { *source-address* } { *mask* }

Parameter

source-address: IP address of the multicast source, in the format 192.168.0.1

mask: Subnet mask for the multicast source IP address

rpf-address: Specify the ingress interface of the RPF entry

distance: Management parameters of static multicast routing entries, ranging from 0 to 255. The smaller the value, the higher the priority. If the value of the static multicast route is smaller than the value of other RPF entries, the static multicast route takes effect. The default value is 1.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a static multicast routing entry with the source address 192.168.0.1, the subnet mask 255.255.255.255, the incoming interface of the RPF entry 192/168.1.1, and the management parameter 1:

```
Switch(config)#ip mroute 192.168.0.1 255.255.255.255 192.168.1.1 1
```

31.2 show ip mroute static

Description

The **show ip mroute static** command is used to display the IP mroute static information.

Syntax

```
show ip mroute static { source source-ip }
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display all static multicast routing entries:

```
Switch(config)#show ip mroute static
```

Chapter 32 VRF Commands (Only for Certain Devices)

Virtual Routing and Forwarding (VRF) allows multiple instances of routing tables to coexist on the same gateway (switch).

Each VRF can be considered a virtual router, which includes the following elements:

- 1) An independent routing table (including an independent address space);
- 2) A set of interfaces belonging to this VRF;
- 3) Routing protocols dedicated to this VRF;
- 4) Each device can maintain one or more VRFs alongside a public routing table (global routing table). Multiple VRF instances are isolated and independent.

Purpose:

VRF enhances functionality by enabling the division of network paths without requiring multiple devices, effectively transforming one physical router into multiple virtual routers.

Benefits:

Because routing instances are independent, identical or overlapping IP addresses can be used without conflict. VRF improves network security through automatic traffic isolation and can eliminate the need for encryption or authentication. VRF is commonly used by ISPs to create separate VPNs for customers, hence it is often called VPN Routing and Forwarding.

32.1 vrf

Description

The **vrf** command is used to create a VRF instance and enters its configuration view. To delete the instance, please use the **no vrf** command.

Syntax

vrf *vrf-name*

no vrf *vrf-name*

Parameter

vrf-name: VRF instance name (1-15 characters).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a VRF instance named vrf1:

```
Switch(config)#vrf vrf1
```

32.2 address-family

Description

The **address-family** command is used to enable the specified address family (IPv4/IPv6) for the VRF and enter its configuration view. To disable the address family, please use the **no address-family** command.

Syntax

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

```
no address-family {ipv4 | ipv6}
```

Parameter

None

Command Mode

VRF Instance View

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IPv4 for the vrf1 instance:

```
Switch(config)#vrf vrf1
```

```
Switch (config-vrf)#address-family ipv4
```

32.3 exit-address-family

Description

The **exit-address-family** command is used to exit the VRF address family view and returns to the VRF configuration view.

Syntax

```
exit-address-family
```


Parameter

None

Command Mode

VRF Address Family View

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Exit the IPv4 view of vrf1:

```
Switch(config)#vrf vrf1
Switch (config-vrf)#address-family ipv4
Switch (config-vrf-af)#exit-address-family
```

32.4 vrf forwarding

Description

The **vrf forwarding** command is used to assign a L3 interface to a VRF instance. To remove the interface from the VRF and returns it to the global routing table, please use the **no vrf forwarding** command. Note: Switching VRFs deletes all existing interface configurations.

Syntax

```
vrf forwarding vrf-name
no vrf forwarding vrf-name
```

Parameter

vrf-name: VRF instance name (1-15 characters).

Command Mode

L3 Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Assign interface VLAN 1 to the vrf1 instance:

```
Switch(config) # interface vlan 1
Switch(config-if)# vrf forwarding vrf1
```

32.5 show vrf

Description

The **show vrf** command is used to view the configured VRF instance information.

Syntax

show vrf {brief | interface | name *vrf-name* }

Parameter

vrf-name: VRF instance name

Command Mode

Privileged EXEC Mode or Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

View the configured VRF instance information:

```
Switch (config)# show vrf brief
```

```
Switch (config)# show vrf interface
```

```
Switch (config)# show vrf name vrf1
```

Chapter 33 MLD Snooping Commands

MLD Snooping (Multicast Listener Discovery Snooping) is a multicast control mechanism running on Layer 2 switch. It can effectively prevent multicast groups being broadcasted in the IPv6 network.

33.1 ipv6 mld snooping (global)

Description

The **ipv6 mld snooping** command is used to enable MLD Snooping function globally. If this function is disabled, all related MLD Snooping function would not work. To disable this function, please use **no ipv6 mld snooping** command.

Syntax

ipv6 mld snooping
no ipv6 mld snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable MLD Snooping:

```
Switch(config)# ipv6 mld snooping
```

33.2 ipv6 mld snooping drop-unknown

Description

The **ipv6 mld snooping drop-unknown** command is used to enable the unknown multicast packets filter function. To disable this function, please use **no ipv6 mld snooping drop-unknown** command. By default, it is disabled.

Syntax

ipv6 mld snooping drop-unknown
no ipv6 mld snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable unknown multicast filter function:

```
Switch(config)# ipv6 mld snooping drop-unknown
```

33.3 ipv6 mld snooping vlan-config

Description

The **ipv6 mld snooping vlan-config** command is used to enable VLAN MLD Snooping function or to modify MLD Snooping parameters. To disable the VLAN MLD Snooping function, please use **no ipv6 mld snooping vlan-config** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **ltime** *leave-time*]

no ipv6 mld snooping vlan-config *vlan-id-list* [**rtime** | **mtime** | **ltime**]

Parameter

vlan-id-list—— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

router-time—— The Router Port Aging Time. Within this time, if the switch does not receive any MLD query messages from the router port, it will consider this port is not a router port any more. Valid values are from 60 to 600 in seconds, and the default value is 300 seconds.

member-time—— The Member Port Aging Time. Within this time, if the switch does not receive any MLD report messages from the member port, it will consider this port is not a member port any more. Valid values are from 60 to 600 in seconds, and the default value is 260 seconds.

leave-time—— The Leave Time. Valid values are from 1 to 30 in seconds, and the default value is 1 second. When the switch receives a done message from a port to leave a multicast group, it will wait for a Leave Time before removing the port from the multicast group. During the period, if the switch receives

any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

- If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends.
- The Leave Time mechanism will not take effect when Fast Leave takes effect.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the MLD Snooping function and modify Router Port Time as 300 seconds, Member Port Time as 200 seconds for VLAN 1-3:

```
Switch(config)# ipv6 mld snooping vlan-config 1-3 rtime 300
Switch(config)# ipv6 mld snooping vlan-config 1-3 mtime 200
```

33.4 ipv6 mld snooping vlan-config (immediate-leave)

Description

This command is used to enable the Fast Leave feature for specific VLANs.

To disable Fast Leave on the VLANs, please use **no ipv6 mld snooping vlan-config *vlan-id-list* immediate-leave** command. This function is disabled by default.

Syntax

```
ipv6 mld snooping vlan-config vlan-id-list immediate-leave
no ipv6 mld snooping vlan-config vlan-id-list immediate-leave
```

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Fast Leave for VLAN 1-3:

```
Switch(config)# ipv6 mld snooping vlan-config 1-3 immediate-leave
```

33.5 ipv6 mld snooping vlan-config (report-suppression)

Description

This command is used to enable the MLD Report Suppression function for specific VLANs. When enabled, the switch will only forward the first MLD report message for each multicast group to the MLD querier and suppress subsequent MLD report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the MLD querier. To disable the MLD report suppression function and forward all the MLD reports to the Layer 3 device in specific VLANs, please use **no ipv6 mld snooping vlan-config *vlan-id-list* report-suppression** command. This function is disabled by default.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* report-suppression

no ipv6 mld snooping vlan-config *vlan-id-list* report-suppression

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MLD Report Suppression for VLAN 1-3:

```
Switch(config)# ipv6 mld snooping vlan-config 1-3 report-suppression
```

33.6 ipv6 mld snooping vlan-config (router-ports-forbidd)

Description

This command is used to forbid the specified ports as being router ports in the specified VLAN(s). To delete the forbidden router ports, please use **no ipv6 mld snooping vlan-config *vlan-id-list* router-ports-forbidd** command.

Syntax

```
ipv6 mld snooping vlan-config vlan-id-list router-ports-forbidd interface  
{ gigabitEthernet port-list | port-channel port-channel-list }  
no ipv6 mld snooping vlan-config vlan-id-list router-ports-forbidd  
interface [ gigabitEthernet port-list | port-channel port-channel-list ]
```

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list — Forbid the specified ports as being router ports. Packets sent from multicast routers to these ports will be discarded.

port-channel-list — Forbid the specified port-channels as being router ports. Packets sent from multicast routers to these port-channels will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Forbid the Ethernet ports 1/0/1-3 as being router ports in VLAN 1:

```
Switch(config)# ipv6 mld snooping vlan-config 1 router-ports-forbidd  
interface gigabitEthernet 1/0/1-3
```

33.7 ipv6 mld snooping vlan-config (rport interface)

Description

This command is used to specify the static router ports for specific VLANs.
To delete the static router ports, please use **no ipv6 mld snooping
vlan-config *vlan-id-list* rport interface** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* rport interface { **gigabitEthernet
port-list | **port-channel** *port-channel-list* }**
no ipv6 mld snooping vlan-config *vlan-id-list* rport interface
{ **gigabitEthernet *port-list* | **port-channel** *port-channel-list* }**

Parameter

vlan-id-list—— The ID list of the VLAN desired to modify configuration,
ranging from 1 to 4094, in the format of 1-3, 5.
port-list—— The list of Ethernet ports.
port-channel-list—— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these
commands.

Example

Set the router port as 1/0/1 for VLAN 1-2:

```
Switch(config)# ipv6 mld snooping vlan-config 1-2 rport interface  
gigabitEthernet 1/0/1
```

33.8 ipv6 mld snooping vlan-config (static)

Description

This command is used to configure interfaces to statically join a multicast
group. To remove interfaces from a static multicast group, please use **no
ipv6 mld snooping vlan-config *vlan-id-list* static** command.

Syntax

```
ipv6 mld snooping vlan-config vlan-id-list static ip interface  
{ gigabitEthernet port-list | port-channel port-channel-list }  
no ipv6 mld snooping vlan-config vlan-id-list static ip interface  
{ gigabitEthernet port-list | port-channel port-channel-list}
```

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

ip — Specify the IP address of the multicast group that the hosts want to join.

port-list — The list of Ethernet ports.

port-channel-list — The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure port ports 1/0/1-3 in VLAN 2 to statically join multicast group ff80::1234:1:

```
Switch(config)# ipv6 mld snooping vlan-config 2 static ff80::1234:1  
interface gigabitEthernet 1/0/1-3
```

33.9 ipv6 mld snooping vlan-config (querier)

Description

This command is used to enable the MLD Snooping Querier feature for specific VLANs. To disable the MLD Snooping Querier feature on the VLANs, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **querier** command without any parameters. To restore the default values, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **querier** command with specified parameters.

Syntax

```
ipv6 mld snooping vlan-config vlan-id-list querier [ max-response-time  
response-time | query-interval interval | general-query source-ip ip-addr |  
last-listener-query-count count | last-listener-query-interval interval ]  
  
no ipv6 mld snooping vlan-config vlan-id-list querier [ max-response-time |  
query-interval | general-query source-ip | last-listener-query-count |  
last-listener-query-interval ]
```

Parameter

vlan-id-list—— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

response-time—— The host's maximum response time to general query messages. Valid values are from 1 to 25 seconds, and the default value is 10 seconds.

query-interval *interval*—— The interval between general query messages sent by the switch. Valid values are from 10 to 300 seconds, and the default value is 60 seconds.

ip-addr—— The source IP address of the general query messages sent by the switch. It should be a unicast address. By default, it is fe80::2ff:ffff:fe00:1.

count—— The number of group-specific queries to be sent. With MLD Snooping Querier enabled, when the switch receives an MLD done message, it obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out group-specific queries to this multicast group through the port receiving the done message. If specified count of group-specific queries are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table. Valid values are from 1 to 5, and the default value is 2.

last-member-query-interval *interval*—— The interval between group-specific queries. Valid values are from 1 to 5 seconds, and the default value is 1 second.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MLD Snooping Querier for VLAN 3, and configure the query interval as 100 seconds:

```
Switch(config)# ipv6 mld snooping vlan-config 3 querier
Switch(config)# ipv6 mld snooping vlan-config 3 querier query interval
100
```

33.10 ipv6 mld snooping vlan-config drop-unknown



Note: This command is only available on certain devices.

Description

The **ipv6 mld snooping vlan-config drop-unknown** command is used to enable the drop-unknown function for the specified VLAN. When enabled, unregistered IPv6 multicast traffic within this VLAN will be discarded. To disable this function, please use the **no ipv6 mld snooping vlan-config drop-unknown** command.

Syntax

```
ipv6 mld snooping vlan-config vlan-id-list drop-unknown
no ipv6 mld snooping vlan-config vlan-id-list drop-unknown
```

Parameter

vlan-id-list — Single VLAN or VLAN range, maximum length 64 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable drop-unknown for VLAN 1:

```
Switch(config)# ipv6 mld snooping vlan-config 1 drop-unknown
```

33.11 ipv6 mld snooping

vlan-config route-unknown



Note: This command is only available on certain devices.

Description

The **ipv6 mld snooping vlan-config route-unknown** command is used to enable the route-unknown function for the specified VLAN. When enabled, unregistered multicast traffic in this VLAN will be forwarded to MLD snooping router ports. To disable this function, please use the **no ipv6 mld snooping vlan-config route-unknown** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **route-unknown**

no ipv6 mld snooping vlan-config *vlan-id-list* **route-unknown**

Parameter

vlan-id-list — Single VLAN or VLAN range, maximum length 64 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable route-unknown for VLAN 1:

```
Switch(config)# ipv6 mld snooping vlan-config 1 route-unknown
```

33.12 ipv6 mld snooping

(interface)

Description

The **ipv6 mld snooping** command is used to enable MLD Snooping function on the desired port. To disable this function, please use **no ipv6 mld snooping** command.

Syntax

ipv6 mld snooping
no ipv6 mld snooping

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable MLD Snooping on port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# ipv6 mld snooping
```

33.13 ipv6 mld snooping max-groups

Description

The **ipv6 mld snooping max-groups** command is used to configure the maximum number of groups that a port can join in. The **ipv6 mld snooping max-groups action** is used to configure the action that the port takes when it receives an MLD report message and the maximum number of entries is in the forwarding table. To remove the maximum group limitation and return to the default of no limitation on the specified port, please use the **no ipv6 mld snooping max-groups** command. To return to the default action of dropping the report, please use the **no ipv6 mld snooping max-groups action** command. These commands only apply to the dynamic multicast groups.

Syntax

ipv6 mld snooping max-groups *maxgroup*
ipv6 mld snooping max-groups action { drop | replace }
no ipv6 mld snooping max-groups
no ipv6 mld snooping max-groups action

Parameter

maxgroup—— Specify the maximum numbers of groups that the port can join. It ranges from 0 to 1000 and the default value is 1000.

drop — When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the port will not join any new multicast group.

replace — When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the maximum numbers of groups that ports 1/0/2-5 can join as 10, and configure the throttling action as replace:

```
Switch(config)#interface range gigabitEthernet 1/0/2-5
Switch(config-if-range)#ipv6 mld snooping max-groups 10
Switch(config-if-range)#ipv6 mld snooping max-groups action replace
```

33.14 ipv6 mld snooping immediate-leave

Description

The **ipv6 mld snooping immediate-leave** command is used to configure the Fast Leave function for port. To disable the Fast Leave function, please use **no ipv6 mld snooping immediate-leave** command.

Syntax

ipv6 mld snooping immediate-leave
no ipv6 mld snooping immediate-leave

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the Fast Leave function for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# ipv6 mld snooping immediate-leave
```

33.15 ipv6 mld profile

Description

The **ipv6 mld profile** command is used to create the configuration profile. To delete the corresponding profile, please use **no ipv6 mld profile** command.

Syntax

```
ipv6 mld profile id
no ipv6 mld profile id
```

Parameter

id—— Specify the id of the configuration profile, ranging from 1 to 999.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Create the profile 1:

```
Switch(config)# ipv6 mld profile 1
```

33.16 deny

Description

The **deny** command is used to configure the filtering mode of profile as deny.

Syntax

```
deny
```

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the filtering mode of profile 1 as deny:

```
Switch(config)# ipv6 mld profile 1
Switch(config-MLD-profile)#deny
```

33.17 permit

Description

The **permit** command is used to configure the filtering mode of profile as permit.

Syntax

permit

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the filtering mode of profile 1 as permit:

```
Switch(config)# ipv6 mld profile 1
Switch(config-igmp-profile)#permit
```

33.18 range

Description

The **range** command is used to configure the range of the profile's filtering multicast address. To delete the corresponding filtering multicast address, please use **no range** command. A profile contains 16 filtering IP-range entries at most.

Syntax

range *start-ip end-ip*
no range *start-ip end-ip*

Parameter

start-ip—— Start IPv6 multicast address of the filter entry..

end-ip—— End IPv6 multicast address of the filter entry.

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure one of the filter multicast address entry as range ff80::1234 to ff80::1235 in profile 1:

```
Switch(config)# ipv6 mld profile 1
Switch(config-igmp-profile)#range ff80::1234 ff80::1235
```

33.19 ipv6 mld filter

Description

The **ipv6 mld filter** command is used to bind the specified profile to the interface. To delete the binding, please use **no ipv6 mld filter** command.

Syntax

ipv6 mld filter *profile-id*
no ipv6 mld filter

Parameter

profile-id—— Specify the profile ID, ranging from 1 to 999.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Bind profile 1 to interface gigabitEthernet 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# ipv6 mld filter 1
```

33.20 clear ipv6 mld snooping statistics

Description

The **clear ipv6 mld snooping statistics** command is used to clear the statistics of the MLD packets.

Syntax

clear ipv6 mld snooping statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the statistics of the MLD packets:

```
Switch(config)# clear ipv6 mld snooping statistics
```

33.21 show ipv6 mld snooping

Description

The **show ipv6 mld snooping** command is used to display the global configuration of MLD Snooping.

Syntax

show ipv6 mld snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of MLD Snooping:

```
Switch(config)# show ipv6 mld snooping
```

33.22 show ipv6 mld snooping interface

Description

The **show ipv6 mld snooping interface** command is used to display the port configuration of MLD snooping.

Syntax

```
show ipv6 mld snooping interface [ gigabitEthernet [ port | port-list ] ]  
{ basic-config | max-groups | packet-stat }
```

```
show ipv6 mld snooping interface [ port-channel [ port-channel-list ] ]  
{ basic-config | max-groups }
```

Parameter

port — The Ethernet port number.

port-list — The list of Ethernet ports.

basic-config | max-groups | packet-stat — The related configuration information selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MLD basic configuration configuration of all ports and port channels:

```
Switch# show ipv6 mld snooping interface basic-config
```

Display the MLD basic configuration of port 1/0/2:

```
Switch# show ipv6 mld snooping interface gigabitEthernet 1/0/2  
basic-config
```

Display the MLD packet statistics of ports 1/0/1-4:

```
Switch# show ipv6 mld snooping interface gigabitEthernet 1/0/1-4  
packet-stat
```

33.23 show ipv6 mld snooping vlan

Description

The **show ipv6 mld snooping vlan** command is used to display VLAN information of MLD Snooping.

Syntax

show ipv6 mld snooping vlan [*vlan-id*]

Parameter

vlan-id—— The VLAN ID selected to display, ranging from 1 to 4094.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the VLAN information:

```
Switch(config)# show ipv6 mld snooping vlan
```

33.24 show ipv6 mld snooping groups

Description

The **show ipv6 mld snooping groups** command is used to display multicast groups.

Syntax

show ipv6 mld snooping groups [**vlan** { *vlan-id* }] [*ipv6_multicast_addr* |
count | dynamic | dynamic count | static | static count]

Parameter

vlan-id——The VLAN ID selected to display the information of all multicast items.

ipv6_multicast_addr—— IPv6 address of the multicast group.

count—— The numbers of all multicast groups.

dynamic—— Display dynamic multicast groups.

dynamic count—— The numbers of all dynamic multicast groups.

static—— Display static multicast groups.

static count—— The numbers of all static multicast groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the multicast groups:

```
Switch(config)# show ipv6 mld snooping groups
```

33.25 show ipv6 mld profile

Description

The **show ipv6 mld profile** command is used to display the configuration information of all the profiles or a specific profile.

Syntax

```
show ipv6 mld profile [ id ]
```

Parameter

id—— Specify the ID of the profile, ranging from 1 to 999.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of all profiles:

```
Switch(config)# show ipv6 mld profile
```

Chapter 34 IPv6 MLD Commands (Only for Certain Devices)

MLD (Multicast Listener Discovery) is a multicast member management protocol for IPv6 environments. Its function is similar to IGMP in IPv4, used for endpoints to report multicast group listening states to routers and control the forwarding scope of IPv6 multicast traffic.

34.1 ipv6 mld

Description

This command is used to configure the global hardware switch for MLD, allowing MLD packets to be sent to the CPU. Disabled by default.

Syntax

ipv6 mld

no ipv6 mld

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# (config)# ipv6 mld
```

34.2 ipv6 mld

last-member-query-count

Description

This command is used to configure the Last Member Query Count on an interface. Default is 2.

Syntax

ipv6 mld last-member-query-count *value*

no ipv6 mld last-member-query-count

Parameter

value — Last Member Query Count, ranging from 1 to 20.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld last-member-query-count 3
```

34.3 ipv6 mld last-member-query-interval

Description

This command is used to configure the Last Member Query Interval on an interface. Default is 1000 milliseconds.

Syntax

ipv6 mld last-member-query-interval *value*

no ipv6 mld last-member-query-interval

Parameter

value — Last Member Query Interval, in milliseconds, ranging from 1000 to 25500.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld last-member-query-interval 2000
```

34.4 ipv6 mld mroute-proxy

Description

Configure this command on the MLD proxy downstream interface to specify the proxy upstream interface for this interface.

Syntax

ipv6 mld mroute-proxy *intf_type* *intf_id*

no ipv6 mld mroute-proxy

Parameter

intf_type — Interface type of the specified proxy upstream interface.

intf_id — Interface ID of the specified proxy upstream interface.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld mroute-proxy vlan 1
```

34.5 ipv6 mld proxy-service

Description

Configure an interface as the MLD proxy upstream interface.

Syntax

ipv6 mld proxy-service

no ipv6 mld proxy-service

Parameter

None,

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld proxy-service
```

34.6 ipv6 mld querier-timeout

Description

This command is used to configure the timeout period for other queriers when this interface is not the querier. Default is $(\text{robustness (default: 2)} * \text{query-interval (default: 125)}) + (\text{query-max-response-time (default: 10)} / 2) = 255$ seconds.

Syntax

ipv6 mld querier-timeout *value*

no ipv6 mld querier-timeout

Parameter

value — Querier timeout value, in seconds, ranging from 60 to 300.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld querier-timeout 100
```

34.7 ipv6 mld query-interval

Description

This command is used to configure the interval at which the querier sends query messages. Default is 125 seconds.

Syntax

ipv6 mld query-interval *value*

no ipv6 mld query-interval

Parameter

value — Query interval value, in seconds, range 1 to 18000.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld query-interval 100
```

34.8 ipv6 mld query-max-response-time

Description

This command is used to configure the maximum query response time. Default is 10 seconds.

Syntax

ipv6 mld query-max-response-time *value*

no ipv6 mld query-max-response-time

Parameter

value — Maximum query response time value, in seconds, range 1 to 240.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld query-max-response-time 5
```

34.9 ipv6 mld robustness

Description

This command is used to configure the robustness value. Default is 2.

Syntax

ipv6 mld robustness *value*

no ipv6 mld robustness

Parameter

value — Robustness value, range 2 to 7.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld robustness 3
```

34.10 ipv6 mld startup-query-count

Description

This command is used to configure the initial query count for the querier.
Default is 2.

Syntax

ipv6 mld startup-query-count *value*

no ipv6 mld startup-query-count

Parameter

value — Startup query count value, range 1 to 20.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld startup-query-count 3
```

34.11 ipv6 mld startup-query-interval

Description

This command is used to configure the initial query interval for the querier.
Default is 31 seconds.

Syntax

ipv6 mld startup-query-interval *value*

no ipv6 mld startup-query-interval

Parameter

value — Startup query interval value, in seconds, range 1 to 18000.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld startup-query-interval 100
```

34.12 ipv6 mld static-group

Description

This command is used to configure a static group join on the interface.

Syntax

ipv6 igmp static-group *group_addr* [**source** *src_addr*]

no ipv6 mld static-group *group_addr* [**source** *src_addr*]

Parameter

group_addr — Multicast group address to join.

src_addr — Specified multicast source for the group join.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld static-group ff1e::1 souce 2001:1::101
```

34.13 ipv6 mld version

Description

This command is used to configure the MLD version. Default is MLDv2.

Syntax

ipv6 mld version *value*

no ipv6 mld version

Parameter

value — Version value, range 1 to 2.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config-if)# ipv6 mld version 1
```

34.14 show ipv6 mld groups

Description

This command is used to display the MLD member group information.

Syntax

show ipv6 mld groups [**interface** *intf_type intf_id*] [*group_addr*] [**detail**]

show ipv6 mld [**vrf** *vrfname*] **groups** [*group_addr*] [**detail**]

Parameter

intf_type — Specified interface type to display.

intf_id — Specified interface ID to display.

group_addr — Specified multicast group member to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch#show ipv6 mld groups detail
```

34.15 show ipv6 mld proxy groups

Description

This command is used to display MLD proxy upstream interface member group information.

Syntax

```
show ipv6 mld proxy groups [ interface intf_type intf_id] [ group_addr]  
[ detail ]
```

```
show ipv6 mld [ vrf vrfname] proxy groups [ group_addr] [ detail ]
```

Parameter

intf_type — Specified interface type to display.

intf_id — Specified interface ID to display.

group_addr — Specified multicast group member to display.

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch# show ipv6 mld proxy groups detail
```

34.16 show ipv6 mld interface

Description

This command is used to display MLD interface status/packet statistics.

Syntax

show ipv6 mld interface *intf_type intf_id* [**statistic**]

Parameter

intf_type — Specified interface type to display.

intf_id — Specified interface ID to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch# show ipv6 mld interface vlan 1
```

34.17 show ipv6 mld

Description

This command is used to display MLD global configuration and interface status under a VRF.

Syntax

show ipv6 mld [**vrf** *vrfname*]

Parameter

vrfname — Virtual Routing and Forwarding instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch# show ipv6 mld vrf test
```

Chapter 35 CPP Commands

CPP (CPU Protect Policy) is a feature designed to prevent a large volume of service packets or malicious attack packets from overwhelming CPU resources, thereby avoiding a sharp increase in CPU utilization that could degrade device performance and ensuring the normal operation of device functions. This feature employs a three-level rate limiting mechanism at the protocol, queue, and CPU port levels to strictly control the number of packets sent to the CPU within a unit of time, guaranteeing efficient CPU processing of normal service traffic.

35.1 cpp-policy

Description

This command enters the CPP policy configuration view. If the specified policy does not exist, it will be created first. A maximum of 12 policies can be created. Its no command deletes a previously created policy. If the policy being deleted is the currently applied one, the default policy will be automatically applied upon deletion. When creating a new policy, its parameters are initially the same as the default policy.

Syntax

cpp-policy *policyName*

no cpp-policy *policyName*

Parameter

policyName — Policy name. Only numbers, letters, and the following symbols are allowed: _@:/.+#. Length is limited to 1–31 characters, and the policy name cannot start with "default".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a policy named "policy_1" and enter its configuration view:

```
Switch(config)#cpp-policy policy_1
```

Delete the policy named "policy_1":

```
Switch(config)#no cpp-policy policy_1
```


35.2 rate-limit protocol

Description

This command sets the rate limit value for a specified protocol within the currently configured policy, or prohibits packets of that protocol from being sent to the CPU. Its no command restores the rate limit setting to the default value. If the configured policy is the currently applied one, the new rate limit value takes effect immediately without needing to re-apply the policy.

Syntax

```
rate-limit protocol { 8021x | arp-bc | arp-uc | bfd | bgp | bgpv6 | dns |  
dhcp-client | dhcp-server | dhcpv6-client | dhcpv6-server | dldp | efm | erps |  
ftp | tftp | gvrp | http | https | isis | lacp | lldp | mld-gmq |  
mld-gmrpt | mld-gmdone | mld-mlr | mpls-uc | mpls-bc | nd-rs | nd-ra | nd-ns |  
nd-na | nd-redirect | ospf | ospfv3 | pim | pimv6 | pppoe | ntp | ptp | rpvst |  
radius | rip | ripng | stp | snmp | ssh | tacplus | telnet | vrrp | vrrpv6 | icmp |  
icmpv6 | igmp | tcp-other | udp-other | other }  
{ deny | cir cirValue [cbs cbsValue] | status { disabled | enabled }}
```

```
no rate-limit protocol { 8021x | arp-bc | arp-uc | bfd | bgp | bgpv6 | dns |  
dhcp-client | dhcp-server | dhcpv6-client | dhcpv6-server | dldp | efm | erps |  
ftp | tftp | gvrp | http | https | isis | lacp | lldp | mld-gmq |  
mld-gmrpt | mld-gmdone | mld-mlr | mpls-uc | mpls-bc | nd-rs | nd-ra | nd-ns |  
nd-na | nd-redirect | ospf | ospfv3 | pim | pimv6 | pppoe | ntp | ptp | rpvst |  
radius | rip | ripng | stp | snmp | ssh | tacplus | telnet | vrrp | vrrpv6 | icmp |  
icmpv6 | igmp | tcp-other | udp-other | other }  
{ deny | cir cirValue [cbs cbsValue] | status { disabled | enabled }}
```

Parameter

cirValue — Committed Information Rate (kbit/s), indicating the long-term average data transfer rate committed by the device.

cbsValue — Committed Burst Size (byte), indicating the maximum burst data volume allowed in a short period, used to handle traffic peaks. If not set, the system automatically sets it to 125 times the *cirValue*.

status — The status configuration for the corresponding protocol.

Command Mode

CPP Policy Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Disable Telnet rate limiting:

```
Switch(config)# cpp-policy policy_1
Switch(config-cpp-policy)# rate-limit protocol telnet status disable
```

35.3 rate-limit queue-rate (only for certain devices)

Description

This command sets the rate limit value for a specified queue within the currently configured policy. Its no command restores the rate limit setting to the default value. If the configured policy is the currently applied one, the new rate limit value takes effect immediately without needing to re-apply the policy.

Syntax

rate-limit queue-rate *queueId* **cir** *cirValue* **cbs** *cbsValue*

no rate-limit queue-rate *queueId*

Parameter

queueId — Queue ID. 0–7 correspond to Queue 0 to Queue 7.

cirValue — Committed Information Rate (kbit/s), indicating the long-term average data transfer rate committed by the device.

cbsValue — Committed Burst Size (byte), indicating the maximum burst data volume allowed in a short period, used to handle traffic peaks. If not set, the system automatically sets it to 125 times the *cirValue*.

Command Mode

CPP Policy Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a policy named "policy_1", enter its view, and set the CIR for Queue 0 to 10,000 kbps and CBS to 100 * 4KB within this policy:

```
Switch(config)# cpp-policy policy_1
Switch(config-cpp-policy)# rate-limit queue-rate 0 cir 10000 cbs 100
```

Restore the rate limit setting for Queue 1 in this policy to its default value:

```
Switch(config-cpp-policy)# no rate-limit queue-rate 1
```

35.4 rate-limit cpu-rate (only for certain devices)

Description

This command sets the rate limit value for the CPU port within the currently configured policy. Its no command restores the rate limit setting to the default value. If the configured policy is the currently applied one, the new rate limit value takes effect immediately without needing to re-apply the policy.

Syntax

rate-limit cpu-rate *cirValue* **cbs** *cbsValue*

no rate-limit cpu-rate

Parameter

cirValue — Committed Information Rate (kbit/s), indicating the long-term average data transfer rate committed by the device.

cbsValue — Committed Burst Size (byte), indicating the maximum burst data volume allowed in a short period, used to handle traffic peaks. If not set, the system automatically sets it to 125 times the *cirValue*.

Command Mode

CPP Policy Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a policy named "policy_1", enter its view, and set the CIR for the CPU port to 10,000 kbps and CBS to 100 * 4KB within this policy:

```
Switch(config)# cpp-policy policy_1
```

```
Switch(config-cpp-policy)# rate-limit cpu-rate cir 10000 cbs 100
```

Restore the rate limit setting for the CPU port in this policy to its default value:

```
Switch(config-cpp-policy)# no rate-limit cpu-rate
```

35.5 cpp-policy-apply default-policy

Description

This command applies the default policy, making its three-level rate limiting take effect on the switch chip.

Syntax

cpp-policy-apply default-policy

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Apply the default policy:

```
Switch(config)# cpp-policy-apply default-policy
```

35.6 cpp-policy-apply policy

Description

This command applies a specified policy, making its three-level rate limiting take effect on the switch chip. Its no command deactivates the specified policy and re-applies the default policy.

Syntax

cpp-policy-apply policy *policyName*

no cpp-policy-apply policy *policyName*

Parameter

policyName — Policy name. Only numbers, letters, and the following symbols are allowed: _@:/.+#. Length is limited to 1–31 characters, and the policy name cannot start with "default". A user-defined policy must be created using `cpp-policy policyName` before it can be applied.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Apply the policy named "policy_1":

```
Switch(config)# cpp-policy-apply policy policy_1
```

Deactivate the policy named "policy_1" and re-apply the default policy:

```
Switch(config)# no cpp-policy-apply policy policy_1
```

35.7 show cpp all

Description

This command is used to display all CPP policy-related information, including the remaining number of configurable policies, the name of the currently running policy, and the configured parameter values for the three-level rate limiting of existing policies.

Syntax

```
show cpp all
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display all information related to the CPP policy:

```
Switch# show cpp all
```

35.8 show cpp default-policy

Description

This command is used to display information about the CPP default policy, including the policy status (whether it is applied) and the parameter values for its three-level rate limiting.

Syntax

show cpp default-policy

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display information about the CPP default policy:

```
Switch# show cpp default-policy
```

35.9 show cpp policy

Description

This command is used to display information about a specified CPP policy, including the policy status (whether it is applied) and the parameter values for its three-level rate limiting.

Syntax

show cpp policy *policyName*

Parameter

policyName — Policy name. Only numbers, letters, and the following symbols are allowed: _@:/.+#. Length is limited to 1–31 characters, and the policy name cannot start with "default".

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display information about the CPP policy named "policy_1":

```
Switch# show cpp policy policy_1
```

35.10 show cpp statistics all (only for certain devices)

Description

This command is used to display statistics for packets sent to the CPU for all protocols supported by the CPP rate limiting policy. The statistics include passed packet count, dropped packet count, passed byte count, dropped byte count, real-time rate, and packet loss rate. Statistics are refreshed every 5 seconds. The rate is a real-time value, while the other statistical items are cumulative historical values.

Syntax

show cpp statistics all

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display packet statistics for all protocols sent to the CPU supported by CPP rate limiting policies:

```
Switch# show cpp statistics all
```

35.11 show cpp statistics protocol (only for certain devices)

Description

This command is used to display statistics for packets of a specified protocol sent to the CPU. The statistics include passed packet count, dropped packet count, passed byte count, dropped byte count, real-time rate, and packet loss rate. Statistics are refreshed every 5 seconds. The rate is a real-time value, while the other statistical items are cumulative historical values.

Syntax

```
show cpp statistics protocol { 8021x | arp-bc | arp-uc | bfd | bgp | bgpv6 | dns  
| dhcp-client | dhcp-server | dhcpv6-client | dhcpv6-server | dldp | efm | erps |  
ftp | tftp | gvrp | http | https | isis | lacp | lbd | ldp | lldp | mdns | mld-gmq |  
mld-gmrpt | mld-gmdone | mld-mlr | mpls-uc | mpls-bc | nd-rs | nd-ra | nd-ns |  
nd-na | nd-redirect | ospf | ospfv3 | pim | pimv6 | pppoe | ntp | ptp | rpvst |  
radius | rip | ripng | stp | snmp | ssh | tacplus | telnet | vrrp | vrrpv6 | icmp |  
icmpv6 | igmp | tcp-other | udp-other | }
```

Parameter

protocol — Protocol type, used to select the protocol for which statistics are to be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display statistics for BPG packets sent to the CPU:

```
Switch# show cpp statistics protocol bgp
```

35.12 show cpp statistics cpu-rate

Description

This command is used to display packet statistics received by the CPU over a 5-second interval, including the passed packet count, passed byte count, and real-time rate for each queue and the CPU port.

Syntax

```
show cpp statistics cpu-rate
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display packet statistics received by the CPU over a 5-second interval:

```
Switch# show cpp statistics cpu-rate
```

35.13 clear cpp statistics all (only for certain devices)

Description

This command is used to clear the statistics for packets sent to the CPU for all protocols supported by the CPP rate limiting policy.

Syntax

```
clear cpp statistics all
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Clear packet statistics for all protocols sent to the CPU supported by CPP rate limiting policies:

```
Switch# clear cpp statistics all
```

35.14 clear cpp statistics protocol (only for certain devices)

Description

This command is used to clear the statistics for packets of a specified protocol sent to the CPU.

Syntax

```
clear cpp statistics protocol { 8021x | arp-bc | arp-uc | bfd | bgp | bgpv6 | dns  
| dhcp-client | dhcp-server | dhcpv6-client | dhcpv6-server | dldp | efm | erps |
```

ftp | tftp | gvrp | http | https | isis | lacp | lldp | mld-gmq |
mld-gmrpt | mld-gmdone | mld-mlr | mpls-uc | mpls-bc | nd-rs | nd-ra | nd-ns |
nd-na | nd-redirect | ospf | ospfv3 | pim | pimv6 | pppoe | ntp | ptp | rpvst |
radius | rip | ripng | stp | snmp | ssh | tacplus | telnet | vrrp | vrrpv6 | icmp |
icmpv6 | igmp | tcp-other | udp-other }

Parameter

protocol — Protocol type, used to select the protocol for which statistics are to be cleared.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Clear statistics for BGP packets sent to the CPU:

```
Switch# clear cpp statistics protocol bgp
```

Chapter 36 MVR Commands

MVR (Multicast VLAN Registration) allows a single multicast VLAN to be shared for multicast member ports in different VLANs in IPv4 network. In IGMP Snooping, if member ports are in different VLANs, a copy of the multicast streams is sent to each VLAN that has member ports. While MVR provides a dedicated multicast VLAN to forward multicast traffic over the Layer 2 network, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs.

36.1 mvr (global)

Description

The **mvr** command is used to enable MVR globally. To disable MVR, please use **no mvr** command.

Syntax

mvr

no mvr

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MVR globally:

```
Switch(config)# mvr
```

36.2 mvr group

Description

The **mvr group** command is used to add multicast groups to MVR. To delete multicast groups from MVR, please use **no mvr group** command. You can configure up to 511 multicast groups.

Syntax

mvr group *ip-addr* [*count*]

no mvr group *ip-addr* [*count*]

Parameter

ip-addr — The start IP address of the contiguous series of multicast groups.

count — The number of the multicast groups to be added to the MVR. Valid values are from 1 to 256, and the default value is 1.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add multicast groups 225.1.2.3 -239.1.2.5 to MVR:

```
Switch (config)# mvr group 225.1.2.3 3
```

36.3 mvr mode

Description

The **mvr mode** command is used to configure the MVR mode as compatible or dynamic. By default, it is compatible. To return to the default configuration, please use **no mvr mode** command.

Syntax

mvr mode { compatible | dynamic }

no mvr mode

Parameter

compatible — In this mode, the switch does not forward report or leave messages from the hosts to the IGMP querier. So the IGMP querier cannot learn the multicast groups membership information from the switch. You have to statically configure the IGMP querier to transmit all the required multicast streams to the switch via the multicast VLAN.

dynamic — In this mode, after receiving report or leave messages from the hosts, the switch will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). So the IGMP querier can learn the multicast groups membership information through the report and leave messages, and transmit the multicast streams to the switch via the multicast VLAN according to the multicast forwarding table.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MVR mode as dynamic:

```
Switch(config)# mvr mode dynamic
```

36.4 mvr querytime

Description

The **mvr querytime** command is used to configure the maximum time to wait for IGMP report on a receiver port before removing the port from multicast group membership. To return to the default configuration, please use **no mvr querytime** command.

Syntax

mvr querytime *time*

no mvr querytime

Parameter

time — The query response time. Valid values are from 1 to 100 tenths of a second, and the default value is 5 tenths of a second.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the query response time of MVR as 1 second, that is 10 tenths of a second:

```
Switch(config)# mvr querytime 10
```

36.5 mvr vlan

Description

The **mvr vlan** command is used to specify the multicast VLAN. By default, it is VLAN 1. To return to the default configuration, please use **no mvr vlan** command.

Syntax

mvr vlan *vlan-id*

no mvr vlan

Parameter

vlan-id—— The ID of the multicast VLAN. Valid values are from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the multicast VLAN as VLAN 10:

```
Switch(config)# mvr vlan 10
```

36.6 mvr (interface)

Description

This command is used to enable MVR for specific interfaces. To disable MVR for the interfaces, please use **no mvr** command. By default, it is disabled.

Syntax

mvr

no mvr

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MVR for port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)#mvr
```

36.7 mvr type

Description

The **mvr type** command is used to configure the MVR port type as receiver or source. By default, the port is a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation fails. To return to the default configuration, please use **no mvr type** command.

Syntax

mvr type { source | receiver }

no mvr type

Parameter

source — Configure the uplink ports that receive and send multicast data on the multicast VLAN as source ports. Source ports should belong to the multicast VLAN.

receiver — Configure the ports that are connecting to the hosts as receiver ports. A receiver port can only belong to one VLAN, and cannot belong to the multicast VLAN.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the port 1/0/3 as a receiver port:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)#mvr type receiver
```

36.8 mvr immediate

Description

The **mvr immediate** command is used to enable the Fast Leave feature of MVR for specified port. To disable the Fast Leave feature of MVR for specific ports, please use **no mvr immediate** command.

Syntax

mvr immediate

no mvr immediate

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Only receiver ports support Fast Leave. Before enabling Fast Leave for a port, make sure there is only a single receiver device connecting to the port.

Example

Enable the Fast Leave feature of MVR for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)#mvr immediate
```

36.9 mvr vlan (group)

Description

This command is used to statically add ports to an MVR group. Then the ports can receive multicast traffic sent to the IP multicast address via the multicast VLAN.

Syntax

mvr vlan *vlan-id* group *ip-addr*

Parameter

vlan-id—— The ID of the multicast VLAN. Valid values are from 1 to 4094.

ip-addr—— The IP address of the multicast group.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

This command applies to only receiver ports. The switch adds or removes the receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts. You can also statically add a receiver port to an MVR group.

Example

Add port 1/0/3 to MVR group 225.1.2.3 statically. The multicast VLAN is VLAN 10:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)#mvr vlan 10 group 225.1.2.3
```

36.10 mvr mode dynamic auto-enable

Description

The **mvr mode dynamic auto-enable** command is used to enable automatic addition of source ports to all multicast groups. To disable this function, please use **no mvr mode dynamic auto-enable** command.

Syntax

mvr mode dynamic auto-enable
no mvr mode dynamic auto-enable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable automatic addition of source ports to all multicast groups:

```
Switch(config)#mvr mode dynamic auto-enable
```

36.11 show mvr

Description

The **show mvr** command is used to display the global configuration of MVR.

Syntax

```
show mvr
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of mvr:

```
Switch# show mvr
```

36.12 show mvr interface

Description

The **show mvr interface** command is used to display the MVR configurations of specific interfaces.

Syntax

```
show mvr interface gigabitEthernet [port | port-list]
```

Parameter

port——The Ethernet port number.

port-list—— The list of Ethernet ports.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MVR configuration of port 1/0/3:

```
Switch# show mvr interface gigabitEthernet 1/0/3
```

36.13 show mvr members

Description

The **show mvr members** command is used to display the membership information of all MVR groups or the specified MVR group.

Syntax

show mvr members [*ip-addr*] [**status** active | inactive]

Parameter

ip-addr——The multicast IP address of the MVR group.

active—— Display all active MVR groups.

inactive——Display all inactive MVR groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the membership information of all MVR groups:

```
Switch# show mvr members
```

Chapter 37 MSTP Commands

MSTP (Multiple Spanning Tree Protocol), compatible with both STP and RSTP and subject to IEEE 802.1s, can disbranch a ring network. STP is to block redundant links and backup links as well as optimize paths.

37.1 debug spanning-tree

Description

The **debug spanning-tree** command is used to enable debugging of spanning-tree activities. To disable the debugging function, please use **no debug spanning-tree** command.

Syntax

debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

no debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

Parameters

all — Display all the spanning-tree debug messages.

bpdu receive — Display the debug messages of the received spanning-tree bridge protocol data unit (BPDU).

bpdu transmit — Display the debug messages of the sent spanning-tree BPDU.

cmpmsg — Display the message priority debug messages.

errors — Display the MSTP error debug messages.

flush — Display the address table flushing debug messages.

init — Display the data structure initialization debug messages.

migration — Display the version migration debug messages.

proposals — Display the MSTP handshake debug messages.

roles — Display the MSTP interface role switchling debug messages.

state — Display the MSTP interface state change debug messages.

tc — Display the MSTP topology event debug messages.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display all the spanning-tree debug messages:

```
Switch# debug spanning-tree all
```

37.2 debug spanning-tree port-state

Description

The **debug spanning-tree port-state** command is used to enable debugging of spanning-tree port-state activities. To disable the debugging function, please use the **no debug spanning-tree port-state** command.

Syntax

debug spanning-tree port-state { asic-db | cache | hardware | self-healing }

no debug spanning-tree port-state { asic-db | cache | hardware | self-healing }

Parameters

asic-db — Display the spanning-tree port-state debug messages for the ASIC database.

cache — Display the spanning-tree port-state debug messages for the cache.

hardware — Display the spanning-tree port-state debug messages for hardware programming.

self-healing — Display the spanning-tree port-state debug messages for self-healing.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the spanning-tree port-state debug messages for hardware:

```
Switch# debug spanning-tree port-state hardware
```

37.3 spanning-tree (global)

Description

The **spanning-tree** command is used to enable STP function globally. To disable the STP function, please use **no spanning-tree** command.

Syntax

spanning-tree

no spanning-tree

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the STP function:

```
Switch(config)# spanning-tree
```

37.4 spanning-tree (interface)

Description

The **spanning-tree** command is used to enable STP function for a port. To disable the STP function, please use **no spanning-tree** command.

Syntax

spanning-tree

no spanning-tree

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the STP function for port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# spanning-tree
```

37.5 spanning-tree priority

Description

The **spanning-tree priority** command is used to configure the bridge priority. To return to the default value of bridge priority, please use **no spanning-tree priority** command.

Syntax

```
spanning-tree priority pri
no spanning-tree priority
```

Parameter

pri—— The bridge priority value, which must be a multiple of 4096. It ranges from 0 to 61440, and the default value is 32768. A lower value indicates a higher priority, with 0 being the highest priority.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the bridge priority as 4096:

```
Switch(config)# spanning-tree priority 4096
```

37.6 spanning-tree common-config

Description

The **spanning-tree common-config** command is used to configure the parameters of the ports for comparison in the CIST and the common parameters of all instances. To return to the default configuration, please use

no spanning-tree common-config command. CIST (Common and Internal Spanning Tree) is the spanning tree in a switched network, connecting all devices in the network.

Syntax

```
spanning-tree common-config [ port-priority pri] [ ext-cost ext-cost]
[ int-cost int-cost] [ portfast { enable | disable }] [ point-to-point { auto | open
| close }]
```

```
no spanning-tree common-config
```

Parameter

pri—— Port Priority, which must be multiple of 16 ranging from 0 to 240. By default, the port priority is 128. Port Priority is an important criterion on determining if the port connected to this port will be chosen as the root port. In the same condition, the port with the highest priority will be chosen as the root port. The lower value has the higher priority.

ext-cost—— External Path Cost, which is used to choose the path and calculate the path costs of ports in different MST regions. It is an important criterion on determining the root port. The lower value has the higher priority. It ranges from 0 to 2000000. By default, it is 0 which is mean auto.

int-cost—— Internal Path Cost, which is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on determining the root port. The lower value has the higher priority. By default, it is automatic. It ranges from 0 to 2000000. By default, it is 0 which is mean auto.

portfast —— Enable/ Disable Edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding rapidly without waiting for forward delay.

point-to-point —— The P2P link status, with auto, open and close options. By default, the option is auto. If the two ports in the P2P link are root port or designated port, they can transit their states to forwarding rapidly to reduce the unnecessary forward delay.

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet |
two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet |
hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the STP function of port 1, and configure the Port Priority as 64, ExtPath Cost as 100, IntPath Cost as 100, and then enable Edge Port:

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# spanning-tree common-config port-priority 64 ext-cost
100 int-cost 100 portfast enable point-to-point open
```

37.7 spanning-tree mode

Description

The **spanning-tree mode** command is used to configure the STP mode of the switch. To return to the default configurations, please use **no spanning-tree mode** command.

Syntax

```
spanning-tree mode { stp | rstp | mstp }
no spanning-tree mode
```

Parameter

stp ——Spanning Tree Protocol, the default value.
rstp ——Rapid Spanning Tree Protocol
mstp ——Multiple Spanning Tree Protocol

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the spanning-tree mode as rpvst:

```
Switch(config)# spanning-tree mode rpvst
```

37.8 spanning-tree mst configuration

Description

The **spanning-tree mst configuration** command is used to access MST Configuration Mode from Global Configuration Mode, as to configure the VLAN-Instance mapping, region name and revision level. To return to the default configuration of the corresponding Instance, please use **no spanning-tree mst configuration** command.

Syntax

spanning-tree mst configuration

no spanning-tree mst configuration

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enter into the MST configuration mode:

```
Switch(config)# spanning-tree mst configuration
```

```
Switch(Config-mst)#
```

37.9 instance

Description

The **instance** command is used to configure the VLAN-Instance mapping. To remove the VLAN-instance mapping or disable the corresponding instance, please use **no instance** command. When an instance is disabled, the related mapping VLANs will be removed.

Syntax

instance *instance-id* **vlan** *vlan-id*

no instance *instance-id* [**vlan** *vlan-id*]

Parameters

instance-id—— Instance ID.

vlan-id—— The VLAN ID selected to mapping with the corresponding instance.

Command Mode

MST Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Map the VLANs 1-100 to Instance 1:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 1-100
```

Disable Instance 1, namely remove all the mapping VLANs 1-100:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# no instance 1
```

Remove VLANs 1-50 in mapping VLANs 1-100 for Instance 1:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# no instance 1 vlan 1-50
```

37.10 name

Description

The **name** command is used to configure the region name of MST instance.

Syntax

name *name*

Parameters

name—— The region name, used to identify MST region. It ranges from 1 to 32 characters.

Command Mode

MST Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the region name of MST as "region1":

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name region1
```

37.11 revision

Description

The **revision** command is used to configure the revision level of MST instance.

Syntax

revision *revision*

Parameters

revision — The revision level for MST region identification, ranging from 0 to 65535.

Command Mode

MST Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the revision level of MST as 100:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 100
```

37.12 spanning-tree mst instance

Description

The **spanning-tree mst instance** command is used to configure the priority of MST instance. To return to the default value of MST instance priority, please use **no spanning-tree mst instance** command.

Syntax

spanning-tree mst instance *instance-id* **priority** *pri*
no spanning-tree mst instance *instance-id* **priority**

Parameter

instance-id—— Instance ID.

pri—— MSTI Priority, which must be multiple of 4096 ranging from 0 to 61440. By default, it is 32768. MSTI priority is an important criterion on determining if the switch will be chosen as the root bridge in the specific instance.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MST Instance 1 and configure its priority as 4096:

```
Switch(config)# spanning-tree mst instance 1 priority 4096
```

37.13 spanning-tree mst

Description

The **spanning-tree mst** command is used to configure MST Instance Port. To return to the default configuration of the corresponding Instance Port, please use **no spanning-tree mst** command. A port can play different roles in different spanning tree instance. You can use this command to configure the parameters of the ports in different instance IDs as well as view status of the ports in the specified instance.

Syntax

spanning-tree mst instance *instance-id*[[**port-priority** *pri*] | [**cost** *cost*]]

no spanning-tree mst instance *instance-id*

Parameter

instance-id—— Instance ID.

pri—— Port Priority, which must be multiple of 16 ranging from 0 to 240. By default, it is 128. Port Priority is an important criterion on determining if the port will be chosen as the root port by the device connected to this port.

cost—— Path Cost, ranging from 0 to 200000. The lower value has the higher priority. Its default value is 0 meaning "auto".

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the priority of port 1 in MST Instance 1 as 64, and path cost as 2000:

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# spanning-tree mst instance 1 port-priority 64 cost 2000
```

37.14 spanning-tree timer

Description

The **spanning-tree timer** command is used to configure forward-time, hello-time and max-age of Spanning Tree. To return to the default configurations, please use **no spanning-tree timer** command.

Syntax

```
spanning-tree timer [{ forward-time forward-time ] [ hello-time hello-time ]
[ max-age max-age ]
no spanning-tree timer
```

Parameter

forward-time — Forward Delay, which is the time for the port to transit its state after the network topology is changed. Forward Delay ranges from 4 to 30 in seconds and it is 15 by default. Otherwise, $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$.

hello-time — Hello Time, which is the interval to send BPDU packets, and used to test the links. Hello Time ranges from 1 to 10 in seconds and it is 2 by default. Otherwise, $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$.

max-age — The maximum time the switch can wait without receiving a BPDU before attempting to reconfigure, ranging from 6 to 40 in seconds. By default, it is 20.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure forward-time, hello-time and max-age for Spanning Tree as 16 seconds, 3 seconds and 22 seconds respectively:

```
Switch(config)# spanning-tree timer forward-time 16 hello-time 3  
max-age 22
```

37.15 spanning-tree hold-count

Description

The **spanning-tree hold-count** command is used to configure the maximum number of BPDU packets transmitted per Hello Time interval. To return to the default configurations, please use **no spanning-tree hold-count** command.

Syntax

spanning-tree hold-count *value*

no spanning-tree hold-count

Parameter

value—— The maximum number of BPDU packets transmitted per Hello Time interval, ranging from 1 to 20 in pps. By default, it is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the hold-count of STP as 8pps:

```
Switch(config)# spanning-tree hold-count 8
```

37.16 spanning-tree max-hops

Description

The **spanning-tree max-hops** command is used to configure the maximum number of hops that occur in a specific region before the BPDU is discarded. To return to the default configurations, please use **no spanning-tree max-hops** command.

Syntax

spanning-tree max-hops *value*

no spanning-tree max-hops

Parameter

value—— The maximum number of hops that occur in a specific region before the BPDU is discarded, ranging from 1 to 40 in hop. By default, it is 20.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the max-hops of STP as 30:

```
Switch(config)# spanning-tree max-hops 30
```

37.17 spanning-tree bpdudfilter

Description

The **spanning-tree bpdudfilter** command is used to enable the BPDU filter function for a port. With the BPDU Filter function enabled, the port does not forward BPDUs from the other switches. To disable the BPDU filter function, please use **no spanning-tree bpdudfilter** command.

Syntax

spanning-tree bpdudfilter

no spanning-tree bpdudfilter

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BPDU filter function for port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# spanning-tree bpdudfilter
```

37.18 spanning-tree bpdudflood

Description

The **spanning-tree bpdudflood** command is used to enable the BPDU forward function for a port. With the function enabled, the port still can forward spanning tree BPDUs when the spanning tree function is disabled on this port. To disable the BPDU filter function, please use **no spanning-tree bpdudflood** command.

Syntax

spanning-tree bpdudflood
no spanning-tree bpdudflood

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BPDU forward function for port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# spanning-tree bpdudflood
```

37.19 spanning-tree bpduguard

Description

The **spanning-tree bpduguard** command is used to enable the BPDU Guard for edge ports. When enabled, if an edge port receives a BPDU packet, the port will automatically be set to an ERROR-PORT, disabling its forwarding functionality. Note that this feature only takes effect on edge ports and does not apply to other port types, such as root ports. In this mode, to restore the port status, manual intervention is required; otherwise, the port will remain in the ERROR-PORT state. There are two methods for manual recovery:

- Restart the spanning tree feature: no spanning-tree, spanning-tree.
- Disable BPDU Guard: no spanning-tree bpduguard.

Syntax

spanning-tree bpduguard

no spanning-tree bpduguard

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BPDU protect function for port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# spanning-tree bpduguard
```

37.20 spanning-tree guard loop

Description

The **spanning-tree guard loop** command is used to enable the Loop Protect function for a port. Loop Protect is to prevent the loops in the network brought by recalculating STP because of link failures and network congestions. To disable the Loop Protect function, please use **no spanning-tree guard loop** command.

Syntax

spanning-tree guard loop

no spanning-tree guard loop

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet |
two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet |
hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Loop Protect function for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# spanning-tree guard loop
```

37.21 spanning-tree guard root

Description

The **spanning-tree guard root** command is used to enable the Root Protect function for a port. With the Root Protect function enabled, the root bridge will set itself automatically as ERROR-PORT when receiving BPDU packets with higher priority, in order to maintain the role of root ridge. To disable the Root Protect function, please use **no spanning-tree guard root** command.

Syntax

spanning-tree guard root

no spanning-tree guard root

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet |
two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet |
hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Root Protect function for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# spanning-tree guard root
```

37.22 spanning-tree guard tc

Description

The **spanning-tree guard tc** command is used to enable the TC Protect of Spanning Tree function for a port. To disable the TC Protect of Spanning Tree function, please use **no spanning-tree guard tc** command. A switch removes MAC address entries upon receiving TC-BPDUs. If a malicious user continuously sends TC-BPDUs to a switch, the switch will be busy with removing MAC address entries, which may decrease the performance and stability of the network. With the Protect of Spanning Tree function enabled, you can configure the number of TC-BPDUs in a required time, so as to avoid the process of removing MAC addresses frequently.

Syntax

```
spanning-tree guard tc
no spanning-tree guard tc
```

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the TC Protect of Spanning Tree for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# spanning-tree guard tc
```

37.23 spanning-tree mcheck

Description

The **spanning-tree mcheck** command is used to enable mcheck.

Syntax

spanning-tree mcheck

Command Mode

Interface Configuration Mode ({ fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | hundred-gigabitEthernet | port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable mcheck for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# spanning-tree mcheck
```

37.24 show spanning-tree active

Description

The **show spanning-tree active** command is used to display the active information of spanning-tree.

Syntax

show spanning-tree active

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the active information of spanning-tree:

```
Switch(config)# show spanning-tree active
```

37.25 show spanning-tree bridge

Description

The **show spanning-tree bridge** command is used to display the bridge parameters.

Syntax

show spanning-tree bridge [forward-time | hello-time | hold-count | max-age
| max-hops | mode | priority | state]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bridge parameters:

```
Switch(config)# show spanning-tree bridge
```

37.26 show spanning-tree interface

Description

The **show spanning-tree interface** command is used to display the spanning-tree information of all ports or a specified port.

Syntax

show spanning-tree interface [**gigabitEthernet** *port* | **port-channel**
port-channel-id] [edge | ext-cost | int-cost | mode | p2p | priority | role | state |
status]

Parameter

port — The Ethernet port number.

port-channel-id — The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the spanning-tree information of all ports:

```
Switch(config)# show spanning-tree interface
```

Display the spanning-tree information of port 1/0/2:

```
Switch(config)# show spanning-tree interface gigabitEthernet 1/0/2
```

Display the spanning-tree mode information of port 1/0/2:

```
Switch(config)# show spanning-tree interface gigabitEthernet 1/0/2 mode
```

37.27 show spanning-tree vlan

Description

The **show Spanning-tree vlan** command is used to display the RPVST spanning tree calculation status for the specified VLAN.

Syntax

Show Spanning-tree vlan <vlanId>

Parameter

vlanId—— The VLAN ID.

Command Mode

Global Configuration Mode

Privilege Requirement

None.

Example

Display the RPVST spanning tree calculation status for VLAN 1:

```
Switch(config)# show spanning-tree vlan 1
```

37.28 show spanning-tree interface-security

Description

The **show spanning-tree interface-security** command is used to display the protect information of all ports or a specified port.

Syntax

show spanning-tree interface-security [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] [**bpdufilter** | **bpduflood** | **bpduguard** | **loop** | **root** | **tc**]

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the protect information of all ports:

```
Switch(config)# show spanning-tree interface-security
```

Display the protect information of port 1:

```
Switch(config)# show spanning-tree interface-security gigabitEthernet  
1/0/1
```

Display the interface security bpdudfilter information:

```
Switch(config)# show spanning-tree interface-security bpdudfilter
```

37.29 show spanning-tree mst

Description

The **show spanning-tree mst** command is used to display the related information of MST Instance.

Syntax

```
show spanning-tree mst { configuration [ digest ] | instance instance-id  
[ interface [ gigabitEthernet port | port-channel port-channel-id ] ] }
```

Parameter

instance-id—— Instance ID desired to show.

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the region information and mapping information of VLAN and MST Instance:

```
Switch(config)#show spanning-tree mst configuration
```


Display the related information of MST Instance 1:

```
Switch(config)#show spanning-tree mst instance 1
```

Display all the ports information of MST Instance 1:

```
Switch(config)#show spanning-tree mst instance 1 interface
```

37.30 show spanning-tree instance

Description

The **show spanning-tree instance** command is used to display Spanning Tree information for all configured instances.

Syntax

```
show spanning-tree instance
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display Spanning Tree information for all configured instances:

```
Switch(config)# show spanning-tree instance
```

Chapter 38 Debug Commands

38.1 debug feppacket packet-dump cpu-traffic position

Description

The **debug feppacket packet-dump cpu-traffic position** command is used to specify packets capture position.

Syntax

debug feppacket packet-dump cpu-traffic position { all | sdk-rx | module-rx | kernel-rx | sdk-tx | module-tx | kernel-tx | rule-own }

Parameter

sdk-rx: Captures raw packets obtained from the SDK, which can be used to debug whether packets enter the CPU. Additional information: tppacket structure descriptor.

module-rx: Captures packets that have been processed by tppacket rules and are forwarded to the corresponding module. It can be used to debug whether the module matches the packets. Additional information: tppacket structure descriptor, rule node information.

kernel-rx: Captures packets sent to the kernel. Additional information: tppacket structure descriptor.

sdk-tx: Captures all packets sent through the SDK, which can be used to verify whether packets are successfully delivered to the MAC.

module-tx: Captures packets sent by the module via the tpPacketSend function. Additional information: tppacket structure descriptor.

kernel-tx: Captures packets sent from the kernel. Additional information: tppacket structure descriptor.

rule-own: Captures packets processed by tppacket rules, forwarded to the corresponding module, and owned (own) by it. Additional information: tppacket structure descriptor, rule node information.

all: Captures packets at all the above locations (default).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

Enable packets capture at all positions:

```
Switch# debug feppacket packet-dump cpu-traffic position all
```

38.2 debug feppacket packet-dump cpu-traffic dst-mac

Description

The **debug feppacket packet-dump cpu-traffic dst-mac** command is used to set the destination MAC address filter.

Syntax

```
debug feppacket packet-dump cpu-traffic dst-mac mac address
```

Parameter

mac address: The destination MAC address, in the format of xx:xx:xx:xx:xx:xx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic dst-mac  
00:1a:2b:3c:4d:5e
```

38.3 debug feppacket packet-dump cpu-traffic src-mac

Description

The **debug feppacket packet-dump cpu-traffic src-mac** command is used to set the source MAC address filter.

Syntax

debug feppacket packet-dump cpu-traffic src-mac *mac address*

Parameter

mac address: The source MAC address, in the format of xx:xx:xx:xx:xx:xx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic src-mac  
00:1a:2b:3c:4d:5e
```

38.4 debug feppacket packet-dump cpu-traffic len-type

Description

The **debug feppacket packet-dump cpu-traffic len-type** command is used to set the length type filter.

Syntax

debug feppacket packet-dump cpu-traffic len-type *length type*

Parameter

length type: Specify the length, in decimal or hexadecimal format (range: 0 - 65535).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic len-type 1500
```

38.5 debug feppacket packet-dump cpu-traffic ip-protocol

Description

The **debug feppacket packet-dump cpu-traffic ip-protocol** command is used to set the IP protocol type filter.

Syntax

debug feppacket packet-dump cpu-traffic ip-protocol *ip protocol type*

Parameter

ip protocol type: Specify the IP protocol type, in decimal or hexadecimal format (range: 0 - 255).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic ip-protocol 6
```

38.6 debug feppacket packet-dump cpu-traffic dst-ipv4

Description

The **debug feppacket packet-dump cpu-traffic dst-ipv4** command is used to set the destination IPv4 address filter.

Syntax

```
debug feppacket packet-dump cpu-traffic dst-ipv4 address
```

Parameter

address: The IPv4 address, in the format of a.b.c.d.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic dst-ipv4 192.168.1.100
```

38.7 debug feppacket packet-dump cpu-traffic src-ipv4

Description

The **debug feppacket packet-dump cpu-traffic src-ipv4** command is used to set the source IPv4 address filter.

Syntax

debug feppacket packet-dump cpu-traffic src-ipv4 *address*

Parameter

address: The IPv4 address, in the format of a.b.c.d.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic src-ipv4 10.0.0.50
```

38.8 debug feppacket packet-dump cpu-traffic dst-ipv6

Description

The **debug feppacket packet-dump cpu-traffic dst-ipv6** command is used to set the destination IPv6 address filter.

Syntax

debug feppacket packet-dump cpu-traffic dst-ipv6 *address*

Parameter

address: The IPv6 address, in the format of
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic dst-ipv6  
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

38.9 debug feppacket packet-dump cpu-traffic src-ipv4

Description

The **debug feppacket packet-dump cpu-traffic src-ipv6** command is used to set the source IPv6 address filter.

Syntax

debug feppacket packet-dump cpu-traffic src-ipv6 *address*

Parameter

address: The IPv6 address, in the format of
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic src-ipv6  
fe80:0000:0000:0000:0202:b3ff:fe1e:8329
```


38.10 debug feppacket packet-dump cpu-traffic dst-port

Description

The **debug feppacket packet-dump cpu-traffic dst-port** command is used to set the transport layer destination port filter.

Syntax

debug feppacket packet-dump cpu-traffic dst-port *transport port*

Parameter

transport port: The destination port number, ranging from 0 to 65535.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic dst-port 443
```

38.11 debug feppacket packet-dump cpu-traffic src-port

Description

The **debug feppacket packet-dump cpu-traffic src-port** command is used to set the transport layer source port filter.

Syntax

debug feppacket packet-dump cpu-traffic src-port *transport port*

Parameter

transport port: The source port number, ranging from 0 to 65535.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic src-port 55000
```

38.12 debug feppacket packet-dump cpu-traffic tail

Description

The **debug feppacket packet-dump cpu-traffic tail** command is used to set the packet tail data filter. This configuration checks if the 5th, 6th, and 7th bytes from the end of the packet simultaneously equal the specified tail value (e.g., adding ten 0x88 bytes to the packet tail would allow capture using this filter). Packets not matching are not captured.

Syntax

```
debug feppacket packet-dump cpu-traffic tail value
```

Parameter

value: The tail value, in decimal or hexadecimal format (range: 0 - 255).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic tail 1
```

38.13 debug feppacket packet-dump cpu-traffic rx-port

Description

The **debug feppacket packet-dump cpu-traffic rx-port** command is used to set the switch receive port filter. This configuration checks if the rxPort field in the tppacket structure equals the specified rx-port. Packets not matching are not captured.

Syntax

```
debug feppacket packet-dump cpu-traffic rx-port value
```

Parameter

value: Received port.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic rx-port 1/0/1
```

38.14 debug feppacket packet-dump cpu-traffic tx-port

Description

The **debug feppacket packet-dump cpu-traffic tx-port** command is used to set the switch send port filter. This configuration checks if the uportList in the tppacket structure contains the specified tx-port. Packets not containing it are not captured.

Syntax

debug feppacket packet-dump cpu-traffic tx-port *value*

Parameter

value: Send port.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic tx-port
```

38.15 debug feppacket packet-dump cpu-traffic count limit

Description

The **debug feppacket packet-dump cpu-traffic count limit** command is used to set the maximum number of packets to dump.

Syntax

debug feppacket packet-dump cpu-traffic count limit *limit*

Parameter

limit: The count limit value, ranging from 0 to 2^32. The default value is 128.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic count limit 100
```

38.16 debug feppacket packet-dump cpu-traffic dump-to

Description

The **debug feppacket packet-dump cpu-traffic dump-to** command is used to specify the packet dump location.

Syntax

```
debug feppacket packet-dump cpu-traffic dump-to { stdout | txt-file |  
txt-ring-file | pcap-file | pcap-ring-file }
```

Parameter

tdout: (Default) Dumps packets to standard output (serial port), includes extra information (tppacket info, etc.).

txt-file: Dumps packets to a text file, includes extra information (tppacket info, etc.).

pcap-file: Dumps packets to a pcap file, contains no extra information, can be viewed with Wireshark.

txt-ring-file: Dumps packets to a ring (circular) text file. For example, if count-limit is set to 100, when the number of captured packets exceeds 100, the file is cleared and capturing starts anew.

pcap-ring-file: Dumps packets to a ring (circular) pcap file. For example, if count-limit is set to 100, when the number of captured packets exceeds 100, the file is cleared and capture restarts.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump cpu-traffic dump-to txt-file
```

38.17 debug feppacket packet-dump port-rx rx-port dst-mac

Description

The **debug feppacket packet-dump port-rx rx-port** command is used to capture all packets received on a specific port of a switch, regardless of whether the packet was originally intended to enter the CPU or was directly forwarded. The **debug feppacket packet-dump port-rx rx-port dst-mac** command is used to set the destination MAC address filter.

Syntax

```
debug feppacket packet-dump port-rx rx-port value dst-mac mac address
```

Parameter

value: Receive port number.

mac address: The destination MAC address, in the format of xx:xx:xx:xx:xx:xx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 dst-mac  
00:1a:2b:3c:4d:5e
```

38.18 debug feppacket packet-dump port-rx rx-port src-mac

Description

The **debug feppacket packet-dump port-rx rx-port src-mac** command is used to set the source MAC address filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* **src-mac** *mac address*

Parameter

value: Receive port number.

mac address: The source MAC address, in the format of xx:xx:xx:xx:xx:xx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 src-mac  
00:1a:2b:3c:4d:5e
```

38.19 debug feppacket packet-dump port-rx rx-port len-type

Description

The **debug feppacket packet-dump port-rx rx-port len-type** command is used to set the length type filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* **len-type** *length type*

Parameter

value: Receive port number.

length type: Specify the length, in decimal or hexadecimal format (range: 0 - 65535).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 len-type  
1500
```

38.20 debug feppacket packet-dump port-rx rx-port ip-protocol

Description

The **debug feppacket packet-dump port-rx rx-port ip-protocol** command is used to set the IP protocol type filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* ip-protocol *ip protocol type*

Parameter

value: Receive port number.

ip protocol type: Specify the IP protocol type, in decimal or hexadecimal format (range: 0 - 255).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 ip-protocol 6
```

38.21 debug feppacket packet-dump port-rx rx-port dst-ipv4

Description

The **debug feppacket packet-dump port-rx rx-port dst-ipv4** command is used to set the destination IPv4 address filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* dst-ipv4 *address*

Parameter

value: Receive port number.

address: The IPv4 address, in the format of a.b.c.d.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 dst-ipv4  
192.168.1.100
```

38.22 debug feppacket packet-dump port-rx rx-port src-ipv4

Description

The **debug feppacket packet-dump port-rx rx-port *value* src-ipv4** command is used to set the source IPv4 address filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* src-ipv4 *address*

Parameter

value: Receive port number.

address: The IPv4 address, in the format of a.b.c.d.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 src-ipv4  
10.0.0.50
```

38.23 debug feppacket packet-dump port-rx rx-port dst-ipv6

Description

The **debug feppacket packet-dump port-rx rx-port dst-ipv6** command is used to set the destination IPv6 address filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* **dst-ipv6** *address*

Parameter

value: Receive port number.

address: The IPv6 address, in the format of
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 dst-ipv6  
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

38.24 debug feppacket packet-dump port-rx rx-port src-ipv4

Description

The **debug feppacket packet-dump port-rx rx-port src-ipv6** command is used to set the source IPv6 address filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* **src-ipv6** *address*

Parameter

value: Receive port number.

address: The IPv6 address, in the format of
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 src-ipv6  
fe80:0000:0000:0000:0202:b3ff:fe1e:8329
```

38.25 debug feppacket packet-dump port-rx rx-port dst-port

Description

The **debug feppacket packet-dump port-rx rx-port dst-port** command is used to set the transport layer destination port filter.

Syntax

debug feppacket packet-dump port-rx rx-port *value* **dst-port** *transport port*

Parameter

value: Receive port number.

transport port: The destination port number, ranging from 0 to 65535.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 dst-port 443
```

38.26 debug feppacket packet-dump port-rx rx-port src-port

Description

The **debug feppacket packet-dump port-rx rx-port src-port** command is used to set the transport layer source port filter.

Syntax

```
debug feppacket packet-dump port-rx rx-port value src-port transport  
port
```

Parameter

value: Receive port number.

transport port: The source port number, ranging from 0 to 65535.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 src-port  
55000
```

38.27 debug feppacket packet-dump port-rx rx-port tail

Description

The **debug feppacket packet-dump port-rx rx-port tail** command is used to set the packet tail data filter. This configuration checks if the 5th, 6th, and 7th bytes from the end of the packet simultaneously equal the specified tail value (e.g., adding ten 0x88 bytes to the packet tail would allow capture using this filter). Packets not matching are not captured.

Syntax

debug feppacket packet-dump port-rx rx-port *value* **tail** *value*

Parameter

value: Receive port number.

value: The tail value, in decimal or hexadecimal format (range: 0 - 255).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 tail 1
```

38.28 debug feppacket packet-dump port-rx rx-port count limit

Description

The **debug feppacket packet-dump port-rx rx-port count limit** command is used to set the maximum number of packets to dump.

Syntax

debug feppacket packet-dump port-rx rx-port *value* count limit *limit*

Parameter

value: Receive port number.

limit: The count limit value, ranging from 0 to 2^32. The default value is 128.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 count limit  
100
```

38.29 debug feppacket packet-dump port-rx rx-port dump-to

Description

The **debug feppacket packet-dump port-rx rx-port dump-to** command is used to specify the packet dump location.

Syntax

**debug feppacket packet-dump port-rx rx-port *value* dump-to { stdout |
txt-file | txt-ring-file | pcap-file | pcap-ring-file }**

Parameter

value: Receive port number.

tdout: (Default) Dumps packets to standard output (serial port), includes extra information (tppacket info, etc.).

txt-file: Dumps packets to a text file, includes extra information (tppacket info, etc.).

pcap-file: Dumps packets to a pcap file, contains no extra information, can be viewed with Wireshark.

txt-ring-file: Dumps packets to a ring (circular) text file. For example, if count-limit is set to 100, when the number of captured packets exceeds 100, the file is cleared and capturing starts anew.

pcap-ring-file: Dumps packets to a ring (circular) pcap file. For example, if count-limit is set to 100, when the number of captured packets exceeds 100, the file is cleared and capturing starts anew.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump port-rx rx-port 1/0/1 dump-to  
txt-file
```

38.30 debug feppacket packet-dump download-txt-file

Description

The **debug feppacket packet-dump download-txt-file** command is used to download the dumped packet text file via a TFTP server. A server IPv4 address must be specified. Note that the TFTP server must have write permission; otherwise, the transfer will fail.

Syntax

debug feppacket packet-dump download-txt-file server-ip *ipv4 address*

Parameter

ipv4 address: Specify the server IPv4 address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump download-txt-file server-ip  
192.168.1.100
```

38.31 debug feppacket packet-dump download-pcap-file

Description

The **debug feppacket packet-dump download-pcap-file** command is used to download the dumped packet pcap file via a TFTP server. A server IPv4 address must be specified. Note that the TFTP server must have write permission; otherwise, the transfer will fail.

Syntax

debug feppacket packet-dump download-pcap-file server-ip *ipv4 address*

Parameter

ipv4 address: Specify the server IPv4 address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump download-pcap-file server-ip  
192.168.1.100
```

38.32 debug feppacket packet-dump show-txt-file

Description

The **debug feppacket packet-dump show-txt-file** command is used to display the content of the dumped packet text file.

Syntax

debug feppacket packet-dump show-txt-file

Parameter

None,

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# debug feppacket packet-dump show-txt-file
```

38.33 no debug feppacket packet-dump

Description

The **no debug feppacket packet-dump** command is used to disable the packet capture functionality. Note that the existing txt and pcap files are retained and will be overwritten the next time packet capture is enabled.

Syntax

no debug feppacket packet-dump

Parameter

None,

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

```
Switch# no debug feppacket packet-dump
```

38.34 debug feppacket packet-print (only for certain devices)

Description

The **debug feppacket packet-print** command is used to enable the message printing function, which will only happen on the serial port and will affect switch performance. To disable this function, please use **no debug feppacket packet-print** command.

Syntax

debug feppacket packet-print

no tppacket packet-print

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

This command may cause network connections to be interrupted and some functions may not work properly. Please don't open it at will.

Example

Enable the message printing function:

38.35 debug spanning-tree

Description

The **debug spanning-tree** command is used to enable debugging of spanning-tree activities. To disable the debugging function, please use **no debug spanning-tree** command.

Syntax

debug spanning-tree { all | bpdud receive | bpdud transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

no debug spanning-tree { all | bpdud receive | bpdud transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

Parameters

- all — Display all the spanning-tree debug messages.
- bpdud receive — Display the debug messages of the received spanning-tree bridge protocol data unit (BPDU).
- bpdud transmit — Display the debug messages of the sent spanning-tree BPDU.
- cmpmsg — Display the message priority debug messages.
- errors — Display the MSTP error debug messages.
- flush — Display the address table flushing debug messages.
- init — Display the data structure initialization debug messages.
- migration — Display the version migration debug messages.
- proposals — Display the MSTP handshake debug messages.
- roles — Display the MSTP interface role switchling debug messages.
- state — Display the MSTP interface state change debug messages.
- tc — Display the MSTP topology event debug messages.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display all the spanning-tree debug messages:

```
Switch# debug spanning-tree all
```

Chapter 39 LLDP Commands

LLDP function enables network devices to advertise their own device information periodically to neighbors on the same LAN. The information of the LLDP devices in the LAN can be stored by its neighbor in a standard MIB, so it is possible for the information to be accessed by a Network Management System (NMS) using SNMP.

39.1 lldp

Description

The **lldp** command is used to enable LLDP function. To disable the LLDP function, please use **no lldp** command.

Syntax

lldp

no lldp

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable LLDP function globally:

```
Switch(config)#lldp
```

39.2 lldp forward_message

Description

The **lldp forward_message** command is used to enable the switch to forward LLDP messages when LLDP function is disabled. To disable the LLDP messages forwarding function, please use **no lldp forward_message** command.

Syntax

lldp forward_message

no lldp forward_message

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the switch to forward LLDP messages when LLDP function is disabled globally:

```
Switch(config)#lldp forward_message
```

39.3 lldp hold-multiplier

Description

The **lldp hold-multiplier** command is used to configure the Hold Multiplier parameter. The aging time of the local information in the neighbor device is determined by the actual TTL value used in the sending LLDPDU. $TTL = \text{Hold Multiplier} * \text{Transmit Interval}$. To return to the default configuration, please use **no lldp hold-multiplier** command.

Syntax

lldp hold-multiplier *multiplier*

no lldp hold-multiplier

Parameter

multiplier — Configure the Hold Multiplier parameter. It ranges from 2 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify Hold Multiplier as 5:

```
Switch(config)#lldp hold-multiplier 5
```

39.4 lldp timer

Description

The **lldp timer** command is used to configure the parameters about transmission. To return to the default configuration, please use **no lldp timer** command.

Syntax

lldp timer { **tx-interval** *tx-interval* / **tx-delay** *tx-delay* / **reinit-delay** *reinit-delay* / **notify-interval** *notify-interval* / **fast-count** *fast-count* }

no lldp timer { *tx-interval* | *tx-delay* | *reinit-delay* | *notify-interval* | *fast-count* }

Parameter

tx-interval—— Configure the interval for the local device to transmit LLDPDU to its neighbors. The value ranges from 5 to 32768 and the default value is 30 seconds.

tx-delay—— Configure a value from 1 to 8192 in seconds to specify the time for the local device to transmit LLDPDU to its neighbors after changes occur so as to prevent LLDPDU being sent frequently. By default, it is 2 seconds.

reinit-delay—— This parameter indicates the amount of delay from when LLDP status becomes "disable" until re-initialization will be attempted. The value ranges from 1 to 10 and the default value is 2.

notify-interval—— Specify the interval of Trap message which will be sent from local device to network management system. The value ranges from 5 to 3600 and the default value is 5 seconds.

fast-count—— When the port's LLDP state transforms from Disable (or Rx_Only) to Tx&Rx (or Tx_Only), the fast start mechanism will be enabled, that is, the transmit interval will be shorten to a second, and several LLDPDUs will be sent out (the number of LLDPDUs equals this parameter). The value ranges from 1 to 10 and the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the Transmit Interval of LLDPDU as 45 seconds and Trap message to NMS as 120 seconds:


```
Switch(config)#lldp timer tx-interval 45
Switch(config)#lldp timer notify-interval 120
```

39.5 lldp receive

Description

The **lldp receive** command is used to enable the designated port to receive LLDPDU. To disable the function, please use **no lldp receive** command.

Syntax

```
lldp receive
no lldp receive
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable port 1/0/1 to receive LLDPDU:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#lldp receive
```

39.6 lldp transmit

Description

The **lldp transmit** command is used to enable the designated port to transmit LLDPDU. To disable the function, please use **no lldp transmit** command.

Syntax

```
lldp transmit
no lldp transmit
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable Gigabit Ethernet port 1/0/1 to transmit LLDPDU:

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)#lldp transmit
```

39.7 lldp snmp-trap

Description

The **lldp snmp-trap** command is used to enable the port's SNMP notification. If enabled, the port will notify the trap event to network management system. To disable the ports' SNMP notification, please use **no lldp snmp-trap** command.

Syntax

lldp snmp-trap
no lldp snmp-trap

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the SNMP notification for Gigabit Ethernet port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#lldp snmp-trap
```

39.8 lldp tlv-select

Description

The **lldp tlv-select** command is used to configure TLVs to be included in outgoing LLDPDU. To exclude TLVs, please use **no lldp tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

```
lldp tlv-select { [ port-description ] [ system-capability ] [ system-description ]  
[ system-name ] [ management-address ] [ port-vlan ] [ protocol-vlan ]  
[ vlan-name ] [ link-aggregation ] [ mac-phy-cfg ] [ max-frame-size ] [ power ]  
[ all ] }
```

```
no lldp tlv-select { [ port-description ] [ system-capability ]  
[ system-description ] [ system-name ] [ management-address ] [ port-vlan ]  
[ protocol-vlan ] [ vlan-name ] [ link-aggregation ] [ mac-phy-cfg ]  
[ max-frame-size ] [ power ] [ all ] }
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Exclude "management-address" and "port-vlan-id" TLVs in LLDPDU outgoing from Gigabit Ethernet port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
```

```
Switch(config-if)# no lldp tlv-select management-address port-vlan
```

39.9 lldp management-address

Description

The **lldp management-address** command is used to configure the port's management address to be included in management address TLV. The NMS uses management addresses to identify the devices. To delete the port's management address, please use **no lldp management address** command.

Syntax

```
lldp management-address { ip-address }  
no lldp management-address
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the port's management address as 192.168.1.100 for port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1  
Switch(config-if)# lldp management-address 192.168.0.100
```

39.10 lldp med-fast-count

Description

The **lldp med-fast-count** command is used to configure the number of the LLDP-MED frames that will be sent out. When LLDP-MED fast start mechanism is activated, multiple LLDP-MED frames will be transmitted based on this parameter. The default value is 4. To return to the default configuration, please use **no lldp med-fast-count** command.

Syntax

```
lldp med-fast-count count  
no lldp med-fast-count
```

Parameter

count—— Configure the Fast Start Count parameter. It ranges from 1 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify Fast Start Count as 5:

```
Switch(config)# lldp med-fast-count 5
```

39.11 lldp med-status

Description

The **lldp med-status** command is used to enable the LLDP-MED feature for the corresponding port. After the LLDP-MED feature is enabled, the port's Admin Status will be changed to Tx&Rx. To disable the LLDP-MED feature for the corresponding port, please use **no lldp med-status** command.

Syntax

lldp med-status

no lldp med-status

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the LLDP-MED feature for port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# lldp med-status
```

39.12 lldp med-tlv-select

Description

The **lldp med-tlv-select** command is used to configure LLDP-MED TLVs to be included in outgoing LLDPDU for the corresponding port. To exclude LLDP-MED TLVs, please use **no lldp med-tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all] }

no lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all] }

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Exclude "network policy" and "inventory" TLVs in LLDPDU outgoing from port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# no lldp med-tlv-select network-policy inventory-
management
```

39.13 lldp med-location

Description

The lldp med-location command is used to configure the Location Identification TLV's content in outgoing LLDPDU of the port.

Syntax

```
lldp med-location { emergency-number identifier | civic-address
[ [ language language ] [ province-state province-state ] [ lci-county-name
county-name ] [ lci-city city ] [ street street ] [ house-number house-number ]
[ name name ] [ postal-zipcode postal-zipcode ] [ room-number room-number ]
[ post-office-box post-office-box ] [ additional additional ] [ country-code
country-code ] [ what { dhcp-server | endpoint | switch } ] }
```

Parameter

emergency-number — Emergency Call Service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The length of this field ranges from 10 to 25 characters.

civic-address — The civic address is defined to reuse the relevant sub-fields of the DHCP option for civic Address based Location Configuration Information as specified by IETF.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the civic address in the Location Identification TLV's content in outgoing LLDPDU of port 1/0/2. Configure the language as English and city as London:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# lldp med-location civic-address language English lci-city
London
```

39.14 show lldp

Description

The **show lldp** command is used to display the global configuration of LLDP.

Syntax

```
show lldp
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of LLDP:

```
Switch#show lldp
```

39.15 show lldp interface

Description

The **show lldp interface** command is used to display LLDP configuration of the corresponding port. By default, the LLDP configuration of all the ports will be displayed.

Syntax

```
show lldp interface [ gigabitEthernet port]
```

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP configuration of Gigabit Ethernet port 1/0/1:

```
Switch#show lldp interface gigabitEthernet 1/0/1
```

39.16 show lldp local-information interface

Description

The **show lldp local-information interface** command is used to display the LLDP information of the corresponding port. By default, the LLDP information of all the ports will be displayed.

Syntax

```
show lldp local-information interface [ gigabitEthernet port]
```

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP information of 1/0/1:

```
Switch#show lldp local-information interface gigabitEthernet 1/0/1
```


39.17 show lldp neighbor-information interface

Description

The **show lldp neighbor-information interface** command is used to display the neighbor information of the corresponding port. By default, the neighbor information of all the ports will be displayed.

Syntax

show lldp neighbor-information interface [**gigabitEthernet** *port*]

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the neighbor information of Gigabit Ethernet port 1/0/1:

```
Switch#show lldp neighbor-information interface gigabitEthernet 1/0/1
```

39.18 show lldp traffic interface

Description

The **show lldp traffic interface** command is used to display the LLDP statistic information between the local device and neighbor device of the corresponding port. By default, the LLDP statistic information of all the ports will be displayed.

Syntax

show lldp traffic interface [**gigabitEthernet** *port*]

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP statistic information of Gigabit Ethernet port 1/0/1:

```
Switch#show lldp traffic interface gigabitEthernet 1/0/1
```

Chapter 40 L2PT Commands (Only for Certain Devices)



Note: L2PT commands are only available on certain devices.

L2PT (Layer 2 Protocol Tunneling) is a feature for service providers to transmit packets from different customers across their ISP networks and maintain Layer 2 protocol configurations of each customer. The supported Layer 2 protocols are STP (Spanning Tree Protocol), GVRP (GARP VLAN Registration Protocol), CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), PAgP (Port Aggregation Protocol), UDLD (UniDirectional Link Detection) and PVST+(Per VLAN Spanning Tree Plus).

40.1 l2protocol-tunnel

Description

The **l2protocol-tunnel** command is used to enable the layer 2 protocol tunneling (L2PT) function globally. To disable the L2PT function, please use **no l2protocol-tunnel** command.

Syntax

l2protocol-tunnel

no l2protocol-tunnel

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the L2PT function globally:

```
Switch(config)# l2protocol-tunnel
```

40.2 l2protocol-tunnel type

Description

The **l2protocol-tunnel type** command is used to configure the L2PT function on a specified port. To disable the L2PT function on the specified port, please use **no l2protocol-tunnel** command.

Syntax

l2protocol-tunnel type nni

l2protocol-tunnel type uni { 01000ccccccc | 01000cccccd | gvrp | stp | lacp | all } [**threshold** *threshold*]

no l2protocol-tunnel

Parameter

nni — Specify the port type according to its connecting device in the network. Specify the port's type as NNI if it is connecting to the ISP network.

uni — Specify the port type according to its connecting device in the network. Specify the port's type as UNI if it is connecting to the user's local network.

01000ccccccc | 01000cccccd | gvrp | stp | lacp | all — Select the supported Layer 2 protocol type. Packets of the specified protocol will be encapsulated with their destination MAC address before they are sent to the ISP network. Packets will be decapsulated to restore their Layer 2 protocol and MAC address information before they are sent to the customer network.

- 01000ccccccc: Enable protocol tunneling for the packets with destination MAC address 01-00-0C-CC-CC-CC. 01-00-0CC-CC-CC-CC is used as the destination MAC address of the CDP/VTP/PAgP/UDLD packets.
- 01000cccccd: Enable protocol tunneling for the packets with destination MAC address 01-00-0C-CC-CC-CD. 01-00-0CC-CC-CC-CD is used as the destination MAC address of Cisco PVST+ BPDUs.
- gvrp: Enable protocol tunneling for the GVRP packets.
- stp: Enable protocol tunneling for the STP packets.
- lacp: Enable protocol tunneling for the LACP packets.
- all: All the above Layer 2 protocols are supported for tunneling.

- **threshold** —Configure the threshold for packets-per-second accepted for encapsulation. Packets beyond the threshold will be dropped. It ranges from 0 to 1000.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure port 1/0/3 as a UNI port for STP packets with the threshold as 1000 packets/second:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)# l2protocol-tunnel type uni stp threshold 1000
```

40.3 show l2protocol-tunnel global

Description

The **show l2protocol-tunnel global** command is used to display the global L2PT status.

Syntax

```
show l2protocol-tunnel global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global L2PT status:

```
Switch(config)# show l2protocol-tunnel global
```

40.4 show l2protocol-tunnel interface

Description

The **show l2protocol-tunnel interface** command is used to display the L2PT configuration information of a specified Ethernet port or of all Ethernet ports.

Syntax

```
show l2protocol-tunnel interface [ gigabitEthernet port | port-channel port-channel-id ]
```

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the L2PT configuration information of Gigabit Ethernet port 1/0/1:

```
Switch(config)#show l2protocol-tunnel interface gigabitEthernet 1/0/1
```

Display the L2PT configuration information of all Ethernet ports:

```
Switch(config)#show l2protocol-tunnel interface
```

40.5 l2protocol-tunnel dst-mac

Description

The **l2protocol-tunnel dst-mac** command is used to customize the dst-mac, which can come from the destination mac address of messages after l2pt encapsulation. To restore the dst-mac to default, please use the **no l2protocol-tunnel dst-mac** command.

Syntax

```
l2protocol-tunnel dst-mac mac-addr
```

```
no l2protocol-tunnel dst-mac mac-addr
```

Parameter

mac-addr—— specify a legal mac address.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Customize the l2pt destination mac address as 58-11-22-0F-6D-B1:

```
Switch(config)#l2protocol-tunnel dst-mac 58-11-22-0F-6D-B1
```

40.6 show l2protocol-tunnel dst-mac

Description

The **show l2protocol-tunnel dst-mac** command is used to display the current dst-mac.

Syntax

```
show l2protocol-tunnel dst-mac
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the current dst-mac:

```
Switch(config)#show l2protocol-tunnel dst-mac
```

Chapter 41 PPPoE ID-Insertion Commands (Only for Certain Devices)



Note: PPPoE ID-Insertion commands are only available on certain devices.

The PPPoE ID-Insertion feature provides a way to extract a Vendor-specific tag as an identifier for the authentication, authorization, and accounting (AAA) access requests on an Ethernet interface. When enabled, the switch attaches a tag to the PPPoE discovery packets, which is called the PPPoE Vendor-Specific tag and it contains a unique line identifier. There are two formats of Vendor-specific tags: Circuit-ID format and Remote-ID format. The BRAS receives the tagged packet, decodes the tag, and uses the Circuit-ID/Remote-ID field of that tag as a NAS-Port-ID attribute in the RADIUS server for PPP authentication and AAA (authentication, authorization, and accounting) access requests. The switch will remove the Circuit-ID/Remote-ID tag from the received PPPoE Active Discovery Offer and Session-confirmation packets from the BRAS.

41.1 pppoe id-insertion (global)

Description

The **pppoe id-insertion** command is used to enable the PPPoE ID-Insertion function globally. To disable the PPPoE ID-Insertion function, please use **no pppoe id-insertion** command.

Syntax

pppoe id-insertion
no pppoe id-insertion

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the PPPoE ID-Insertion function:

```
Switch(config)# pppoe id-insertion
```


41.2 pppoe circuit-id (interface)

Description

The **pppoe circuit-id** command is used to enable the PPPoE Circuit-ID Insertion function for a specified port. To disable the PPPoE Circuit-ID Insertion function on a specified port, please use **no pppoe circuit-id** command.

Syntax

pppoe circuit-id
no pppoe circuit-id

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the PPPoE Circuit-ID Insertion function for the Gigabit Ethernet port 1/0/1:

```
Switch (config)# interface gigabitEthernet 1/0/1
Switch (config-if)# pppoe circuit-id
```

41.3 pppoe circuit-id type

Description

The **pppoe circuit-id type** command is used to configure the type of PPPoE Circuit-ID for a specified port. By default, the PPPoE Circuit-ID type is "ip".

Syntax

pppoe circuit-id type { mac | ip | udf [*Value*] | udf-only [*Value*] }

Parameter

mac | ip | udf | udf-only — The type of PPPoE Circuit-ID for the port.

mac: The MAC address of the switch will be used to encode the Circuit-ID option.

ip: The IP address of the switch will be used to encode the Circuit-ID option.
This is the default value.

udf: A user specified string with the maximum length of 40 characters will be used to encode the Circuit-ID option.

udf-only: Only the user specified string with the maximum length of 40 will be used to encode the Circuit-ID option.

Value — The value of udf/udf-only. The maximum length is 40 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the type of PPPoE Circuit-ID as "mac" for the Gigabit Ethernet port 1/0/1:

```
Switch (config)# interface gigabitEthernet 1/0/1
Switch (config-if)# pppoe circuit-id type mac
```

41.4 pppoe remote-id

Description

The **pppoe remote-id** command is used to enable the PPPoE Remote-ID Insertion and configure the Remote-ID value for a specified port. To disable the PPPoE Remote-ID Insertion function on a specified port, please use **no pppoe remote-id** command. By default, the PPPoE Remote-ID Insertion is disabled.

Syntax

pppoe remote-id [*Value*]

no pppoe remote-id

Parameter

Value — The value of UDF. The maximum length is 40 characters. If not specified, the default value will be the PPPoE client's MAC address.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the remote-ID as "mac" for the Gigabit Ethernet port 1/0/1:

```
Switch (config)# interface gigabitEthernet 1/0/1
Switch (config-if)# pppoe remote-id mac
```

41.5 show pppoe global

Description

The **show pppoe global** command is used to display the global configuration of PPPoE Circuit-ID Insertion function.

Syntax

```
show pppoe global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of PPPoE Circuit-ID Insertion function globally:

```
Switch # show pppoe global
```

41.6 show pppoe interface

Description

The **show pppoe interface** command is used to display all ports' or the specified port's configuration information of PPPoE Circuit-ID Insertion function.

Syntax

show pppoe interface [gigabitEthernet *port*]

Parameter

port—— The Fast/Gigabit Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of PPPoE Circuit-ID Insertion function of all Ethernet ports:

```
Switch# show pppoe interface
```

Display the configuration of PPPoE Circuit-ID Insertion function of the Gigabit Ethernet port 1/0/1 :

```
Switch# show pppoe interface gigabitEthernet 1/0/1
```

Chapter 42 Static Routes Commands

42.1 ip routing

Description

This **ip routing** command is used to enable IPv4 routing globally. To disable IPv4 routing, please use the **no ip routing** command.

Syntax

ip routing

no ip routing

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IPv4 routing feature for the switch:

```
Switch(config)# ip routing
```

42.2 interface vlan

Description

This **interface vlan** command is used to create the VLAN interface. To delete the specified VLAN interface, please use the **no interface vlan** command.

Syntax

interface vlan { *vid* }

no interface vlan { *vid* }

Parameter

vid—— The ID of the VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the VLAN interface 2:

```
Switch(config)# interface vlan 2
```

42.3 interface loopback

Description

This **interface loopback** command is used to create the loopback interface. To delete the specified loopback interface, please use the **no interface loopback** command.

Syntax

```
interface loopback { id }  
no interface loopback { id }
```

Parameter

id — The ID of the loopback interface, ranging from 1 to 64.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the loopback interface 1:

```
Switch(config)# interface loopback 1
```

42.4 switchport

Description

This **switchport** command is used to switch the Layer 3 interface into the Layer 2 port. To switch the Layer 2 port into the Layer 3 routed port, please use the **no switchport** command.

Syntax

switchport

no switchport

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Switch port 1/0/9 into the routed port:

```
Switch(config)# interface gigabitEthernet 1/0/9
Switch(config-if)# no switchport
```

42.1 switchport

Description

This **switchport** command is used to switch the Layer 3 interface into the Layer 2 port. To switch the Layer 2 port into the Layer 3 routed port, please use the **no switchport** command.

Syntax

switchport

no switchport

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Switch port 1/0/9 into the routed port:

```
Switch(config)# interface gigabitEthernet 1/0/9
Switch(config-if)# no switchport
```

42.2 interface range port-channel

Description

This **interface range port-channel** command is used to create multiple port-channel interfaces.

Syntax

interface range port-channel *port-channel-list*

Parameter

port-channel-list—— The list of the port-channel interface, ranging from 1 to 14, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the port-channel interfaces 1, 3, 4 and 5:

```
Switch(config)# interface port-channel 1,3-5
```

42.3 description

Description

This **description** command is used to add a description to the Layer 3 interface, including routed port, port-channel interface, loopback interface and VLAN interface. To clear the description of the corresponding interface, please use the **no description** command.

Syntax

description *string*

no description

Parameter

string—— Content of an interface description, ranging from 1 to 128 characters.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a description system-if to the routed port 1/0/9 :

```
Switch(config)# interface gigabitEthernet 1/0/9
Switch(config-if)# no switchport
Switch(config-if)# description system-if
```

42.4 shutdown

Description

This **shutdown** command is used to shut down the specified interface. The interface type include: routed port, port-channel interface, loopback interface and VLAN interface. To enable the specified interface, please use the **no shutdown** command.

Syntax

shutdown

no shutdown

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Shut down the routed port 1/0/9:

```
Switch(config)# interface gigabitEthernet 1/0/9
Switch(config-if)# no shutdown
```

```
Switch(config-if)# shutdown
```

42.5 interface port-channel

Description

This **interface port-channel** command is used to create the port-channel interface. To delete the specified port-channel interface, please use the **no interface port-channel** command.

Syntax

```
interface port-channel { port-channel-id }  
no interface port-channel { port-channel-id }
```

Parameter

port-channel-id—— The ID of the port-channel interface, ranging from 1 to 64.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the port-channel interface 1:

```
Switch(config)# interface port-channel 1
```

42.6 ip route

Description

This **ip route** command is configure the static route. To clear the corresponding entry, please use the **no ip route** command.

Syntax

```
ip route [vrf vrf-name] { dest-address } { mask } [nexthop-vrf vrf-name]  
{ next-hop-address } [ distance ][metric][description]  
no ip route [vrf vrf-name] { dest-address } { mask } [nexthop-vrf vrf-name]  
{ next-hop-address }
```

Parameter

vrf-name—— VRF instance name.

dest-address—— The destination IP address.

mask—— The subnet mask.

next-hop-address—— The address of the next-hop.

distance—— The distance metric of this route, ranging from 1 to 255. The smaller the distance is, the higher the priority is.

metric—— The inner metric for this route, range from 1 to 4294967295. The smaller the metric is, the higher the priority is.

description—— Description for static route, ranging from 1 to 128 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a static route with the destination IP address as 192.168.2.0, the subnet mask as 255.255.255.0 and the next-hop address as 192.168.0.2:

```
Switch(config)# ip route 192.168.2.0 255.255.255.0 192.168.0.2
```

42.7 ipv6 routing

Description

This **ipv6 routing** command is enable the IPv6 routing feature globally. To disable IPv6 routing, please use the **no ipv6 routing** command.

Syntax

ipv6 routing

no ipv6 routing

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IPv6 routing globally:

```
Switch(config)# ipv6 routing
```

42.8 ipv6 route

Description

This **ipv6 route** command is configure the IPv6 static route. To clear the corresponding entry, please use the **no ipv6 route** command.

Syntax

```
ipv6 route [vrf vrf-name] { ipv6-dest-address } [nexthop-vrf vrf-name]  
{ next-hop-address } [ distance ][metric][description]  
no ipv6 route [vrf vrf-name] { ipv6-dest-address } [nexthop-vrf vrf-name]  
{ next-hop-address }
```

Parameter

vrf-name—— VRF instance name.

ipv6-dest-address—— Destination IPv6 address and mask length.

next-hop-address—— Next hop IPv6 address.

distance—— Routing metric, value range 1~255.

metric—— The inner metric for this route, range from 1 to 4294967295. The smaller the metric is, the higher the priority is.

description—— Description for static route, ranging from 1 to 128 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a static route with a destination IP of 3200::/64, a prefix vrf of vrf1, a next hop IP of 3100::1234, and a next hop vrf of vrf2:

```
Switch(config)# ipv6 route vrf vrf1 3200::/64 nexthop-vrf vrf2 3100::1234
```

42.9 show interface vlan

Description

The **show interface vlan** command is used to display the information of the specified interface VLAN.

Syntax

```
show interface vlan vid
```

Parameter

vid—— The VLAN ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of VLAN 2:

```
Switch(config)#show interface vlan 2
```

42.10 show ip interface

Description

This **show ip interface** command is used to display the detailed information of the specified Layer 3 interface.

Syntax

```
show ip interface [ gigabitEthernet port / port-channel port-channel-id /  
loopback id | vlan vlan-id ]
```

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel. Member ports in this port channel should all be routed ports.

id—— The loopback interface ID.

vlan-id—— The VLAN interface ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the detailed information of the VLAN interface 2:

```
Switch(config)# show ip interface vlan 2
```

42.11 show ip interface brief

Description

This **show ip interface brief** command is used to display the summary information of the Layer 3 interfaces.

Syntax

```
show ip interface brief
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of the Layer 3 interfaces:

```
Switch(config)# show ip interface brief
```

42.12 show ip route

Description

This **show ip route** command is used to display IPv4 routing table information, and can be expanded to display routing table information of a certain VRF.

Syntax

show ip route [vrf *vrf-name*]

Parameter

vrf-name—— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv4 routing table information under VRF1:

```
Switch(config)# show ip route vrf vrf1
```

42.13 show ip route specify

Description

This **show ip route specify** command is used to display the valid routing information to the specified IP address or network segments.

Syntax

show ip route specify { *ip* } [*mask*] [**longer-prefixes]**

Parameter

ip—— Specify the destination IP address.

mask—— Specify the destination IP address together with the parameter *ip*.

longer-prefixes —— Specify the destination subnets that match the network segment determined by the *ip* and *mask* parameters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the shortest route to 192.168.0.100:

```
Switch(config)# show ip route specify 192.168.0.100
```

Look up the route entry with the destination as 192.168.0.0/24:

```
Switch(config)# show ip route specify 192.168.0.0 255.255.255.0
```

Display the routes to all the subnets that belongs to 192.168.0.0/16:

```
Switch(config)# show ip route specify 192.168.0.0 255.255.0.0  
longer-prefixes
```

42.14 show ip route summary

Description

This **show ip route summary** command is used to display the summary information of the route entries classified by their sources.

Syntax

```
show ip route summary
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of route entries:

```
Switch(config)# show ip route summary
```

42.15 show ip route static

Description

This **show ip route static** command is used to display the information of the active IPv4 static route entries.

Syntax

```
show ip route static
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of active IPv4 static route entries:

```
Switch(config)# show ip route static
```

42.16 show ip route static description

Description

This **show ip route static description** command is used to display the description of the IPv4 static route entries.

Syntax

```
show ip route static description
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the description of the IPv4 static route entries:

```
Switch(config)# show ip route static description
```

42.17 show ipv6 interface

Description

This command is used to display the configured IPv6 information of the management interface, including ipv6 function status, link-local address and global address, IPv6 multicast groups etc.

Syntax

```
show ipv6 interface
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 information of the management interface:

```
Switch(config)# show ipv6 interface
```

42.18 show ipv6 route

Description

This **show ipv6 route** command is used to display IPv6 routing table information, and can be expanded to display routing table information of a certain VRF.

Syntax

```
show ipv6 route [vrf vrf-name]
```

Parameter

vrf-name—— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 routing table information under VRF1:

```
Switch(config)# show ipv6 route vrf vrf1
```

42.19 show ipv6 route summary

Description

This **show ipv6 route summary** command is used to display the summary information of the IPv6 route entries classified by their sources.

Syntax

```
show ipv6 route summary
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of IPv6 route entries:

```
Switch(config)# show ipv6 route summary
```

42.20 show ipv6 route static

Description

This **show ipv6 route static** command is used to display the information of the active IPv6 static route entries.

Syntax

```
show ipv6 route static
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of active IPv6 static route entries:

```
Switch(config)# show ipv6 route static
```

42.21 show ipv6 route static description

Description

This **show ipv6 route static description** command is used to display the description of the IPv6 static route entries.

Syntax

```
show ipv6 route static description
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the description of the IPv6 static route entries:

```
Switch(config)# show ipv6 route static description
```

Chapter 43 RIP Configuration Commands (Only for Certain Devices)

RIP (Routing Information Protocol) is a routing protocol suitable for small networks and has lower requirements in terms of bandwidth, configuration, and management. As a routing protocol based on distance vector algorithm, RIP uses hop count as the measurement standard.

43.1 router rip

Description

This **router rip** command is used to enable the RIP function on the switch. To disable this function, please use the **no router rip** command. You can specify to create a RIP instance under a certain VRF.

Syntax

router rip [**vrf** *vrf-name*]

no router rip [**vrf** *vrf-name*]

Parameter

vrf-name: VRF instance name

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the RIP function of the switch in VRF v1:

```
Switch(config)#router rip vrf v1
```

43.2 network

Description

The **network** command is used to enable the RIP function on the corresponding interface of the configured network segment. To disable the

RIP function on the corresponding interface, please use **no network** command.

Syntax

network *ip* [mask]

no network *ip* [mask]

Parameter

ip: Network IP address, the format is 192.168.0.0. If you enter an IP address, the network number will be automatically obtained based on the mask length of the natural network segment. Entering 0.0.0.0 means enabling the RIP function on all interfaces.

mask: The mask that controls the subnetting.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable RIP on the 255.255.255.0 subnet of 192.168.0.1:

```
Switch(config-router)#network 192.168.0.1 255.255.255.0
```

43.3 version

Description

The **version** command is used to configure the version of packets sent and received by RIP. By default, the switch sends RIPv2 packets and receives RIPv1 and RIPv2 packets. To restore the default message version settings, please use the **no version** command.

Syntax

version {1|2}

no version

Parameter

1: Send and receive RIPv1 messages.

2: Send and receive RIPv2 messages.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the RIP message version as RIPv1:

```
Switch(config-router)#version 1
```

43.4 timer basic

Description

The **timer basic** command is used to configure the RIP timer. To restore the timer configuration to its default, please use the **no timer basic** command.

Syntax

timer basic *update-value timeout-value garbage-collect-value*

timer basic {**update** *update-value* | **timeout** *timeout-value* | **garbage** *garbage-collect-value*}

no timer basic [**update** | **timeout** | **garbage**]

Parameter

update-value: Routing table update time, ranging from 5 to 86400 seconds. The default value is 30.

timeout-value: Routing table aging time, ranging from 5 to 86400 seconds. The default value is 180.

garbage-collect-value: The expiration time after the routing entry is unreachable. When the entry is unreachable, the routing entry is removed from the routing table after the expiration time. The range is 5~86400 seconds, and the default value is 120.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the routing table update time to 50 seconds, the routing table aging time to 100 seconds, and the routing entry expiration time to 100 seconds:

```
Switch(config-router)#timer basic 50 100 100
```

Set the routing table update time to 50 seconds:

```
Switch(config-router)#timer basic update 50
```

43.5 distance

Description

The **distance** command is used to configure the management distance of RIP routing. To restore the default configuration, please use the **no distance** command.

Syntax

distance *distance*

no distance

Parameter

distance: Management distance of RIP routing, ranging from 1 to 255. The default value is 120.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the management distance of RIP routing to 100:

```
Switch(config-router)#distance 100
```

43.6 auto-summary

Description

The **auto-summary** command is used to enable the automatic summary function of RIP. After this function is enabled, routing entries will be automatically summarized into natural network segments, which can reduce the number of routing entries issued for each update. To disable this function, use the **no auto-summary** command.

Syntax

auto-summary

no auto-summary

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the automatic summary function of RIP:

```
Switch(config-router)#auto-summary
```

43.7 default-metric

Description

The **default-metric** command is used to set the default metric for redirection routes. To restore the default configuration, please use the **no default-metric** command.

Syntax

default-metric *metric*

no default-metric

Parameter

metric: The default metric of the redirect route, ranging from 1 to 15, and the default value is 1.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the default metric for redirection routes to 5:

```
Switch(config-router)#default-metric 5
```

43.8 redistribute

Description

The **redistribute** command is used to set the metric for redirection routes. To restore the default configuration, please use the **no redistribute** command.

Syntax

redistribute { ospf *process-id* | connected | static } [**metric** *metric-value*]

no redistribute { ospf *process-id* | connected | static } [**metric**]

Parameter

ospf: Enable RIP redirect OSPF routing function.

process-id: Redirected OSPF process number.

connected: Enable RIP redirect direct routing function.

static: Enable RIP redirect static routing function.

metric-value: The metric of the redirect route.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set RIP to redirect ospf process 1, and set metric to 3:

```
Switch(config-router)#redistribute ospf 1 metric 3
```

43.9 allow-ecmp

Description

The **allow-ecmp** command is used to enable the ECMP function. To disable this function, please use the **no allow-ecmp** command.

Syntax

allow-ecmp

no allow-ecmp

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the ECMP function of RIP:

```
Switch(config-router)#allow-ecmp
```

43.10 default-information originate

Description

The **default-information originate** command is used to introduce a default route into RIP. To disable this function, please use the **no default-information originate** command.

Syntax

default-information originate
no default-information originate

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Introduce a default route into RIP:

```
Switch(config-router)#default-information originate
```

43.11 neighbor

Description

The **neighbor** command is used to configure the neighbor of RIP. After configuring the neighbor, RIP will send RIP packets to the neighbor through unicast packets. To clear the neighbor configuration, please use the **no neighbor** command.

Syntax

neighbor *ip-address*
no neighbor *ip-address*

Parameter

ip-address: IP address of RIP's neighbor.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify 192.168.0.100 as the RIP neighbor:

```
Switch(config-router)#neighbor 192.168.0.100
```

43.12 passive-interface

Description

The **passive-interface** command is used to configure the interface not to send RIP packets but only to receive RIP packets. A unicast response will be sent out when a neighbor is configured at the same time. To disable this function, please use the **no passive-interface** command.

Syntax

```
passive-interface interface { fastEthernet | gigabitEthernet |  
hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet |  
twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } interface-value
```

```
no passive-interface interface { fastEthernet | gigabitEthernet |  
hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet |  
twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } interface-value
```

Parameter

interface-value: Specify the interface to be configured as passive-interface.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure VLAN 2 as passive-interface:

```
Switch(config-router)# passive-interface interface vlan 2
```

43.13 ip rip authentication mode

Description

The **ip rip authentication mode** command is used to configure the authentication mode of RIP messages, and its no command is used to clear the configuration of authentication mode. The authentication function only takes effect when the authentication mode and password are configured.

Syntax

ip rip authentication mode { md5 | simple }

no ip rip authentication mode

Parameter

md5: Configure the authentication mode of RIP to md5 authentication.

simple: Configure the authentication mode of RIP to plain text authentication.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the RIP authentication mode of VLAN 2 to md5 authentication:

```
Switch(config)#interface vlan 2
```

```
Switch(config-if)#ip rip authentication mode md5
```

43.14 ip rip authentication string

Description

The **ip rip authentication string** command is used to configure the password and key ID for RIP authentication. The key ID is only used for md5 authentication. This command cannot be configured at the same time as the ip rip authentication key-chain command. To clear the password and key ID of RIP authentication, please use the **no ip rip authentication string** command.

Syntax

ip rip authentication string [0 | 6 | 7] *string* [**key-id** *id*]

no ip rip authentication string

Parameter

[0 | 6 | 7]: Key form. 0 represents plaintext, 6 represents ciphertext (type 6), and 7 represents ciphertext (type 7).

string: RIP authentication password, 16 characters at most.

id: Key ID for RIP authentication, ranging from 1 to 255. The default value is 1.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the rip authentication password of interface VLAN 2 as tplink and the key ID as 2:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip rip authentication string 7 tplink key-id 2
```

43.15 ip rip authentication key-chain

Description

The **ip rip authentication key-chain** command is used to configure the password and key ID for RIP authentication by binding key-chain. This command cannot be configured at the same time as the ip rip authentication string command. To clear key-chain binding, please use the **no ip rip authentication key-chain** command.

Syntax

```
ip rip authentication key-chain key-chain-name
no ip rip authentication key-chain
```

Parameter

key-chain-name: The name of the key-chain to be bound.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure key chain as 1, set key as 0, the corresponding password as tplink, and bind the RIP authentication of VLAN 1 to key chain 1:

```
Switch(config)#key chain 1
Switch (config-keychain)#key 0 key-string tplink
Switch (config-keychain)#exit
Switch (config)#interface vlan 1
```

```
Switch (config-if)#ip rip authentication key-chain 1
```

43.16 ip rip receive version

Description

The **ip rip receive version** command is used to configure the version of RIP packets received by the interface. If the receive version of an interface is not configured, it will be determined by the global configuration. To restore the default configuration, please use the **no ip rip receive version** command.

Syntax

```
ip rip receive version { 1 | 2 }
```

```
no ip rip receive version
```

Parameter

1: Configure the receive version of the interface to RIPv1.

2: Configure the receive version of the interface to RIPv2.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the receive version of VLAN 1 to RIPv1:

```
Switch (config)#interface vlan 1
```

```
Switch (config-if)#ip rip receive version 1
```

43.17 ip rip send version

Description

The **ip rip send version** command is used to configure the version of RIP packets sent by the interface. If the send version of an interface is not configured, it will be determined by the global configuration. To restore the default configuration, please use the **no ip rip receive version** command.

Syntax

```
ip rip send version { 1 | 2 }
```

```
no ip rip send version
```

Parameter

- 1: Configure the send version of the interface to RIPv1.
- 2: Configure the send version of the interface to RIPv2.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the send version of VLAN 1 to RIPv1:

```
Switch (config)#interface vlan 1
Switch (config-if)#ip rip send version 1
```

43.18 ip rip split-horizon

Description

The **ip rip split-horizon** command is used to configure the split horizon function of the interface. This function is enabled by default. When this function is enabled, RIP will not send routing entries learned from this interface out of this interface. When this function is disabled, RIP will only send routing entries according to the routing table. To disable this function, please use the **no ip rip split-horizon** command.

Syntax

ip rip split-horizon [poison-reverse]

no ip rip split-horizon

Parameter

poison-reverse: Enable the poison-reverse function of the interface. After this function is enabled, the entries learned from the interface will have the metric set to 16 before being sent out. Disable the poison reversal function by configuring the ip rip split-horizon command.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the poison-reverse function of VLAN 1:

```
Switch (config)#interface vlan 1
Switch (config-if)#ip rip split-horizon poison-reverse
```

43.19 ip rip v2-broadcast

Description

The **ip rip v2-broadcast** command is used to enable the RIPv2 packet broadcast function of the interface. By default, RIPv2 messages are sent through multicast. After this function is enabled on an interface, RIPv2 messages on the interface are sent through broadcast. To disable this function, please use the **no ip rip v2-broadcast** command.

Syntax

```
ip rip v2-broadcast
no ip rip v2-broadcast
```

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the RIPv2 packet broadcast function of VLAN 1:

```
Switch (config)#interface vlan 1
Switch (config-if)#ip rip v2-broadcast
```

43.20 show ip rip

Description

The **show ip rip** command is used to display the RIP routing table.

Syntax

```
show ip rip [vrf vrf-name]
```

Parameter

vrf-name: VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIP routing table of VRF v1:

```
Switch#show ip rip vrf v1
```

43.21 show ip rip status

Description

The **show ip rip status** command is used to display the RIP status.

Syntax

```
show ip rip [vrf vrf-name] status
```

Parameter

vrf-name: VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIP status of VRF v1:

```
Switch#show ip rip status vrf v1
```

43.22 clear ip rip

Description

The **clear ip rip** command is used to clear the routing entries for RIP learning and re-request routing information from other devices.

Syntax

```
clear ip rip [vrf vrf-name]
```

Parameter

vrf-name: VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the routing entries for RIP learning and rerequest routing information from of VRF v1:

```
Switch#clear ip rip vrf v1
```

Chapter 44 RIPng Configuration Commands (Only for Certain Devices)

RIPng (RIP next generation) is a routing protocol that improves the RIP protocol in order to solve the compatibility problem between the RIP protocol and IPv6.

44.1 router ripng

Description

This **router ripng** command is used to enable the RIPng function. Only when the RIPng function is enabled can the global configuration of the RIPng function be performed. When the RIPng function is disabled, the global configuration of the RIPng function will be cleared. To disable this function, please use the **no router ripng** command. You can specify to create a RIPng instance under a certain VRF.

Syntax

router ripng [**vrf** *vrf-name*]

no router ripng [**vrf** *vrf-name*]

Parameter

vrf-name: VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the RIPng function in VRF v1:

```
Switch(config)#router ripng vrf v1
```

44.2 ipv6 rip enable

Description

The **ipv6 rip enable** command is used to enable the ripng function of the interface. This command only takes effect after the global switch of RIPng is enabled. To disable this function, please use **no ipv6 rip enable** command.

Syntax

ipv6 rip enable

no ipv6 rip enable

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the RIPng function of VLAN 1:

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)# ipv6 rip enable
```

44.3 timer basic

Description

The **timer basic** command is used to configure the RIPng timer. To restore the timer configuration to its default, please use the **no timer basic** command.

Syntax

timer basic *update-value timeout-value garbage-collect-value*

timer basic {**update** *update-value* | **timeout** *timeout-value* | **garbage** *garbage-collect-value*}

no timer basic [**update** | **timeout** | **garbage**]

Parameter

update-value: Routing table update time, ranging from 5 to 86400 seconds. The default value is 30.

timeout-value: Routing table aging time, ranging from 5 to 86400 seconds. The default value is 180.

garbage-collect-value: The expiration time after the routing entry is unreachable. When the entry is unreachable, the routing entry is removed from the routing table after the expiration time. The range is 5~86400 seconds, and the default value is 120.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the routing table update time to 50 seconds, the routing table aging time to 100 seconds, and the routing entry expiration time to 100 seconds:

```
Switch(config-router)#timer basic 50 100 100
```

Set the routing table update time to 50 seconds:

```
Switch(config-router)#timer basic update 50
```

44.4 default-metric

Description

The **default-metric** command is used to set the default metric for redirect routes. To restore the default configuration, please use the **no default-metric** command.

Syntax

default-metric *metric*

no default-metric

Parameter

metric: The default metric of the redirect route, ranging from 1 to 15, and the default value is 1.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the default metric for redirection routes to 5:

```
Switch(config-router)#default-metric 5
```

44.5 redistribute

Description

The **redistribute** command is used to set RIPv3 to redirect external routes. Its no command has two forms: if it does not contain the metric parameter, it is used to disable the redirection function of the corresponding external route. If it contains the metric parameter, it is used to restore the metric used for redirect routes to the default value.

Syntax

```
redistribute { connected | ospfv3 | static } [ metric metric-value ]  
no redistribute { ospfv3 | static } [ metric ]
```

Parameter

connected: Enable RIPv3 redistribution of directly connected routes.

ospfv3: Enable RIPv3 redirect OSPFv3 routing function.

static: Enable RIPv3 redirect static routing function.

metric-value: The metric of the redirect route.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set RIPv3 to redirect OSPFv3, and set metric to 3:

```
Switch(config-router)#redistribute ospfv3 metric 3
```

44.6 allow-ecmp

Description

The **allow-ecmp** command is used to enable the ECMP function. To disable this function, please use the **no allow-ecmp** command.

Syntax

```
allow-ecmp  
no allow-ecmp
```

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the ECMP function of RIPng:

```
Switch(config-router)#allow-ecmp
```

44.7 default-information originate

Description

The **default-information originate** command is used to introduce a default route into RIPng. To disable this function, please use the **no default-information originate** command.

Syntax

default-information originate

no default-information originate

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Introduce a default route into RIPng:

```
Switch(config-router)#default-information originate
```

44.8 passive-interface

Description

The **passive-interface** command is used to configure the interface not to send RIPng packets but only to receive RIPng packets. A unicast response will be sent out when a neighbor is configured at the same time. To disable this function, please use the **no passive-interface** command.

Syntax

passive-interface interface { fastEthernet | gigabitEthernet | hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } *interface-value*

no passive-interface interface { fastEthernet | gigabitEthernet | hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } *interface-value*

Parameter

interface-value: Specify the interface to be configured as passive-interface.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure VLAN 2 as passive-interface:

```
Switch(config-router)# passive-interface interface vlan 2
```

44.9 ipv6 rip split-horizon

Description

The **ipv6 rip split-horizon** command is used to configure the split horizon function of the interface. This function is enabled by default. When this function is enabled, RIPv6 will not send routing entries learned from this interface out of this interface. When this function is disabled, RIPv6 will only send routing entries according to the routing table. To disable this function, please use the **no ipv6 rip split-horizon** command.

Syntax

ipv6 rip split-horizon [poison-reverse]

no ipv6 rip split-horizon

Parameter

poison-reverse: Enable the poison-reverse function of the interface. After this function is enabled, the entries learned from the interface will have the metric set to 16 before being sent out. Disable the poison reversal function by configuring the ipv6 rip split-horizon command.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the poison-reverse function of VLAN 1:

```
Switch (config)#interface vlan 1
```

```
Switch (config-if)#ipv6 rip split-horizon poison-reverse
```

44.10 ipv6 rip summary-address

Description

The **ipv6 rip summary-address** command is used to configure the interface route aggregation function of the interface. To disable this function, please use the **no ipv6 rip summary-address** command.

Syntax

ipv6 rip summary-address *ipv6-prefix*

no ipv6 rip summary-address

Parameter

ipv6-prefix: IPv6 prefix.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable route aggregation for interface 2000::1/64:

```
Switch (config)#interface vlan 1
```

```
Switch (config-if)# ipv6 rip summary-address 2000::1/64
```

44.11 show ipv6 rip

Description

The **show ipv6 rip** command is used to display the RIPng routing table.

Syntax

show ipv6 rip [**vrf** *vrf-name*]

Parameter

vrf-name: VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIPng routing table in VRF v1:

```
Switch#show ipv6 rip vrf v1
```

44.12 show ipv6 rip status

Description

The **show ipv6 rip status** command is used to display the RIPng status.

Syntax

show ipv6 rip [**vrf** *vrf-name*] **status**

Parameter

vrf-name: VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIPng status in VRF v1:

```
Switch#show ipv6 rip status vrf v1
```

44.13 clear ipv6 rip

Description

The **clear ipv6 rip** command is used to clear the routing entries for RIPng learning and re-request routing information from other devices.

Syntax

clear ipv6 rip [**vrf** *vrf-name*]

Parameter

vrf-name: VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the routing entries for RIPv6 learning and rerequest routing information from other devices:

```
Switch#clear ipv6 rip vrf v1
```

Chapter 45 OSPF Configuration Commands (Only for Certain Devices)

OSPF is an Interior Gateway Protocol (IGP) designed expressly for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

Currently, OSPF Version 2 (RFC2328) is used for the IPv4 protocol; Use OSPF Version 3 (RFC2740) for IPv6 protocol. Unless otherwise specified, the OSPF referred to in this chapter is OSPF Version 2.

45.1 router ospf

Description

When the OSPFv2 instance specified by the process-id has not been created, this command is used to create an OSPFv2 instance and enter Router configuration mode. If a vrf name is specified when using the command, it indicates that this OSPFv2 instance belongs to the specified VRF instance. If the vrf parameter is not specified, the created OSPFv2 instance will belong to the public network. When the OSPFv2 instance specified by the process-id already exists, using this command with the correct vrf name (or without the vrf parameter) will allow entry into Router configuration mode. The `no` command is used to delete the OSPFv2 instance. When the vrf parameter is not specified, the corresponding instance will be deleted based on the process-id.

Syntax

```
router ospf process-id [vrf vrf-name]  
no router ospf process-id [vrf vrf-name]
```

Parameter

process-id: Process ID, ranging from 1 to 65535. Sixteen processes can be created at most.

vrf-name: VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an OSPFv2 instance with process ID 1 and add it to vrf1:

```
Switch(config)#router ospf 1 vrf vrf1
```

45.2 router-id

Description

The **router-id** command is used to configure the router ID. To delete the configured router-id, please use the **no router-id** command.

Syntax

Router-id *router-id*

no router-id

Parameter

router-id: The route ID in the format of dotted decimal notation. 0.0.0.0 is illegal.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the router ID of OSPF routing process 1 as 1.1.1.1:

```
Switch(config)#router ospf 1
Switch(config-router)#router-id 1.1.1.1
```

45.3 network

Description

This **network** command is used to configure the network of a specified area. All the interfaces fallen into the configured network will belong to this area. To

delete the specified network and its corresponding interfaces from this area, please use the **no network** command.

Syntax

network *ip-address wildcard-mask area area-id*

no network *ip-address wildcard-mask area area-id*

Parameter

ip-address: The IP address of the network.

wildcard-mask: The wildcard mask of the network (such as 0.0.0.255). The subnet mask is also compatible (such as 255.0.0.0).

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the network 192.168.0.0/24 in the area 0.0.0.0:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)# network 192.168.0.0 255.255.255.0 area 0.0.0.0
```

45.4 maximum-paths

Description

The **maximum-paths** command is used to configure the maximum number of the equal-cost multipath routings. To restore to default value, please use the **no maximum-paths** command.

Syntax

maximum-paths *number*

no maximum-paths

Parameter

number: The maximum number of the equal-cost multipath routings, ranging from 1 to 32. The default value is 32.

Command Mode

Router Configuration Mode

Example

Configure the maximum number of the equal-cost multipath routings as 2:

```
Switch(config)#router ospf 1
Switch(config-router)#maximum-paths 2
```

45.5 redistribute

Description

The **redistribute** command is used to configure the ASBR to redistribute the external routes from other routing protocols to the OSPF domain in type-5 LSAs. To restore the certain optional parameters to default values, please use the **no redistribute** command with corresponding parameters.

Syntax

```
redistribute { connected | static /rip | ospf process-id } [ metric cost ]
[ metric-type type ]

no redistribute { connected | static /rip | ospf process-id } [ metric cost ]
[ metric-type type ]
```

Parameter

connected: Specify the external route type as connected.

static: Specify the external route type as static.

rip: Specify the external route type as RIP.

ospf: Specify the external route type as OSPF.

process-id: The OSPF routing process ID, ranging from 1 to 65535. It's not allowed to

redirect to the own process, for example, OSPF process 1 cannot redirect itself.

cost: The cost of the external routes, ranging from 1 to 16777214. Its default value is

defined in the command `default-metric`.

type: The type of the external routes, either 1 or 2. The default value is 2.

Command Mode

Router Configuration Mode

Example

Redistribute the RIP routes from the external and advertise them as type 1 external routes in the OSPF domain:

```
Switch(config)#router ospf 1
Switch(config-router)#redistribute rip metric-type 1
```

45.6 default-metric

Description

The **default-metric** command is used to configure the default cost of the redistributing external route. To restore to the default value, please use the **no default-metric** command.

Syntax

```
default-metric cost
no default-metric
```

Parameter

cost: The default cost of the redistributing external route, ranging from 1 to 16777214.

Command Mode

Router Configuration Mode

Example

Configure the default cost of the redistributing external route as 12:

```
Switch(config)#router ospf 1
Switch(config-router)#default-metric 12
```

45.7 default-information originate

Description

The **default-information originate** command is used to advertise the default route as AS-External LSA. To cancel the advertisement of the default route, please use the **no default-information originate** command without any optional parameters. To restore the certain parameters to default values, please use the **no default-information originate** command with corresponding parameters.

Syntax

```
default-information originate [ always ] [ metric cost ] [ metric-type type ]  
no default-information originate [ always ] [ metric cost ] [ metric-type type ]
```

Parameter

always: OSPF will advertise the default route whether there is default route is the IP routing table or not. If the parameter is not configured, OSPF will advertise the default route only when there is default route in the IP routing table.

cost: The default cost of the default route, ranging form 1 to 16777214. Its default value is 1.

type: The type of the external routes, either 1 or 2. The default value is 2.

Command Mode

Router Configuration Mode

Example

Configure OSPF to advertise the default route whether there is default route is the IP routing table or not:

```
Switch(config)#router ospf 1  
Switch(config-router)#default-information originate always
```

45.8 passive-interface default

Description

The **passive-interface default** command is used to prevent all interface from sending OSPF packets. All interface area allowed to send OSPF packets by default. To restore to the default settings, use the **no passive-interface default** command.

Syntax

passive-interface default

no passive-interface default

Parameter

None.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Suppress route updates by default:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)# passive-interface default
```

45.9 auto-cost

Description

The **auto-cost** command is used to enable the auto computing function of the interface cost and configure the reference bandwidth. The interface cost is the ratio of the reference bandwidth to the interface bandwidth. To restore the reference bandwidth to default value, please use the **no auto-cost reference-bandwidth** command.

Syntax

auto-cost reference-bandwidth *bandwidth*

no auto-cost reference-bandwidth

Parameter

bandwidth. The reference bandwidth, ranging from 1 to 4294967 Mbps. Its default value is 100Mbps.

Command Mode

Router Configuration Mode

Example

Enable the auto computing function of the interface cost and configure the reference bandwidth as 10000 Mbps:

```
Switch(config)#router ospf 1
Switch(config-router)#auto-cost reference-bandwidth 10000
```

45.10 distance

Description

The **distance** command is used to configure the OSPF administrative distance. To restore to the default distance, please use the **no distance** command. The administrative distance represents the priority of the routes. The smaller administrative distance corresponds to higher priority. When different routing protocols possess the same route to the same destination, the route with the highest priority will be selected to add to the IP routing table according to the administrative distance.

Syntax

distance *administrative-distance*

no distance

Parameter

administrative-distance: Routing administrative distance, ranging from 1 to 255. Its default value is 110. When this value is set to 255, it indicates that the source of routing information is unreliable and all related routes are ignored.

Command Mode

Router Configuration Mode

Example

Configure the OSPF routing administrative distance as 100:

```
Switch(config)#router ospf 1
Switch(config-router)#distance 100
```

45.11 timers throttle spf

Description

The **timers throttle spf** command is used to configure the computing delay and interval of the SPF, thus preventing the consumption of the CPU and memory caused by frequent SPF computing. To restore to the default value, please use the **no timers throttle spf** command.

Syntax

```
timers throttle spf spf-delay spf-holdtime spf-max-holdtime
no timers throttle spf
```

Parameter

spf-delay: The delay time of the SPF computing, ranging from 1 to 600000 milliseconds. The default value is 0 milliseconds.

spf-holdtime: The minimum interval between two SPF computings, ranging from 1 to 600000 milliseconds. The default value is 50 milliseconds.

spf-max-holdtime: The Maximum interval between two SPF computings, ranging from 1 to 600000 milliseconds. The default value is 5000 milliseconds.

Command Mode

Router Configuration Mode

Example

Configure the computing delay and interval of the SPF as 10 seconds:

```
Switch(config)#router ospf 1
Switch(config-router)#timers throttle spf 10000 10000 50000
```

45.12 compatible rfc1583

Description

The **compatible rfc1583** command is used to configure the OSPF's compatibility for the routing rules in the RFC 1583. To cancel the

compatibility, please use the **no compatible rfc1583** command. It is compatible by default.

Syntax

compatible rfc1583

no compatible rfc1583

Command Mode

Router Configuration Mode

Example

Configure the OSPF's compatibility for the routing rules in RFC1583:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#compatible rfc1583
```

45.13 area stub

Description

The **area stub** command is used to define an area as a stub area. To restore the stub area to a normal one, please use the **no area stub** command. To restore the certain parameters to default values, please use the **no area stub** command with corresponding parameters.

Syntax

area *area-id* stub [no-summary]

no area *area-id* stub [no-summary]

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

no-summary: Configure the stub are as a totally stub area, where the ABR advertises neither the destinations in other areas nor the external routes. The stub area is not a totally stub area by default

Command Mode

Router Configuration Mode

Example

Configure the area 1 as a totally stub area:

```
Switch(config)#router ospf 1
Switch(config-router)# area 1 stub no-summary
```

45.14 area nssa

Description

The **area nssa** command is used to define an area as a NSSA area. To restore the NSSA area to a normal one, please use the **no area nssa** command without any optional parameters. To restore the certain parameters to default values, please use the **no area nssa** command with corresponding parameters.

Syntax

```
area area-id nssa [no summary | default-information-originate [metric cost] [metric-type type]]
no area-id nssa [no summary | default-information-originate [metric cost] [metric-type type]]
```

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

no-summary: Configure the NSSA area as a totally NSSA area, where the ABR advertises neither the destinations in other areas nor the external routes. The NSSA area is not a totally NSSA area by default.

default-information-originate: Enable or disable advertising default route into NSSA area by sending a NSSA-External LSA. OSPF will not advertise default route if this parameter is not specified

cost: The default cost of the default route, ranging from 1 to 16777214. Its default value is 1.

type: The type of the external routes, either 1 or 2. The default value is 2.

Command Mode

Router Configuration Mode

Example

Configure the Area 1 as a totally NSSA area:

```
Switch(config)#router ospf 1
Switch(config-router)# area 1 nssa no-summary
```

45.15 area default-cost

Description

The **area default-cost** command is used to configure the cost of default route sent from ABR to stub or NSSA area.

Syntax

```
area area-id default-cost cost
no area area-id default-cost
```

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

cost: The cost value. It ranges from 1 to 16777214 and the default value is 1.

Command Mode

Router Configuration Mode

Example

Configure the cost of default route sent to Area 1 as 10:

```
Switch(config)#router ospf 1
Switch(config-router)#area 1 nssa
Switch(config-router)#area 1 default-cost 10
```

45.16 area range

Description

The **area range** command is used to configure a summary route. To delete this route, please use the **no area range** command. By default no route is summarized.

This command is only used with the ABR to summarize the route information of a certain area. The ABR only sends one summarized route of the routes in the aggregated segment to the other areas. An area can be configured with multiple summary segments, which can be aggregated by OSPF.

If the no area range command is configured, the formally summarized routes will be redistributed.

Syntax

```
area area-id range ip-address mask [ advertise ] [ cost cost ]  
[ not-advertise ]
```

```
no area area-id range ip-address mask [ advertise ] [ cost cost ]  
[ not-advertise ]
```

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

ip-address: The destination of the aggregated route.

mask: The network mask of the aggregated route, in the format of dotted decimal notation.

advertise: Allow route aggregation of ABR broadcast.

not-advertise: Suppress route aggregation of ABR broadcast.

cost: The cost of the aggregated route, ranging from 1 to 16777214. The default value is the maximum one of all the aggregated routes. The cost parameter can be configured only when the advtise parameter is enabled. When configured as not-advtise, the cost parameter will be restored to the default value.

Command Mode

Router Configuration Mode

Example

Configure one aggregated route 100.100.0.0/16 with the cost 10 in the Area 0:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#area 0 range 100.100.0.0 255.255.0.0 cost 10
```

45.17 area authentication

Description

The **area authentication** command is used to configure the authentication type of the ospf process. The process is not authenticated by default. To restore to default value, please use the **no area authentication** command.

Syntax

area *area-id* **authentication** [message-digest]

no area *area-id* **authentication**

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

message-digest: Configure the configuration type as MD5.

If no authentication mode is specified here, the default mode will be simple authentication.

Command Mode

Router Configuration Mode

Example

Configure the authentication method to MD5 in the Area 0:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#area 0 authentication message-digest
```

45.18 area virtual-link

Description

The **area virtual-link** command is used to configure the virtual-link. To delete the configured virtual-link, please use the **no area virtual-link** without any optional parameters. To restore the certain parameters to default values, please use the **no area virtual-link** command with corresponding parameters.

Syntax

```
area transit-area virtual-link router-id [dead-interval dead-interval]  
[ hello-interval hello-interval] [ retransmit-interval rtx-interval]  
[ transmit-delay trans-delay]  
no area transit-area virtual-link router-id
```

Parameter

transit-area: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id: The ID of the neighboring router on the opposite end of the virtual link, in the format of dotted decimal notation.

hello-interval: The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

dead-interval: The time after which the neighbor becomes invalid. It ranges from 1 to 65535 seconds and the default value is 4 times as the hello-interval.

rtx-interval: The retransmission interval of the LSA, DD and LSR packets. It ranges from 1 to 65535 seconds and the default value is 5 seconds.

trans-delay: The LSA transmission delay. It ranges from 1 to 65535 seconds and the default value is 1 seconds.

Command Mode

Router Configuration Mode

Example

Configure a virtual-link with the transmission area as Area 1 and the ID of the neighboring router on the other endpoint as 1.1.1.1:

```
Switch(config)#router ospf 1  
Switch(config-router)#area 1 virtual-link 1.1.1.1
```

45.19 area virtual-link authentication

Description

The **area virtual-link authentication** command is used to configure the authentication type of the virtual link. The virtual link is not authenticated by

default. To restore to default value, please use the **no area virtual-link authentication** command.

Syntax

area *transit-area* **virtual-link** *router-id* **authentication** [message-digest | null]

no area *transit-area* **virtual-link** *router-id* **authentication**

Parameter

transit-area: The transition area ID in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id: The ID of the neighboring router on the other endpoint of the virtual link, in the format of dotted decimal notation.

message-digest: Configure the configuration type as MD5.

null: No authentication. By default it is no authentication.

If no authentication mode is specified here, the default mode will be simple authentication.

Command Mode

Router Configuration Mode

Example

Configure simple authentication as the authentication mode of a virtual-link with the transmission area as Area 2 and the ID of the neighboring router on the other endpoint as 3.3.3.3:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#area 2 virtual-link 3.3.3.3 authentication
```

45.20 area virtual-link authentication-key

Description

The **area virtual-link authentication-key** command is used to configure the simple authentication key. To delete the key, please use the **no area virtual-link authentication-key** command.

Syntax

area *transit-area* **virtual-link** *router-id* **authentication-key** [0|7] *password*

no area *transit-area* **virtual-link** *router-id* **authentication-key**

Parameter

transit-area: The transition area ID in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id: The ID of the neighboring router on the other endpoint of the virtual link, in the format of dotted decimal notation.

[0|7]: Key form, 0 represents plaintext, 7 represents ciphertext.

password: A string from 1 to 8 alphanumeric characters or symbols. The password is case-sensitive, and cannot contain question marks. By default, it is empty.

Command Mode

Router Configuration Mode

Example

Configure the authentication mode of a virtual-link as simple authentication, with the transmission area as Area 2 and the ID of the neighboring router on the other endpoint as 3.3.3.3, and the authentication key as 123456:

```
Switch(config)#router ospf 1
Switch(config-router)#area 2 virtual-link 3.3.3.3 authentication-key
123456
```

45.21 area virtual-link message-digest-key

Description

The **area virtual-link message-digest-key** is used to configure the MD5 authentication ID and key of the virtual-link. To delete the specified configuration, please use the **no area virtual-link message-digest-key** command.

Syntax

area *transit-area* **virtual-link** *router-id* **message-digest-key** *id* **md5** [**0|7**]
password

no area *transit-area* **virtual-link** *router-id* **message-digest-key** *id*

Parameter

transit-area: The transition area ID in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id: The ID of the neighboring router on the other endpoint of the virtual link, in the format of dotted decimal notation.

id: The key ID of the MD5, ranging from 1 to 255.

[0|7]: Key form, 0 represents plaintext, 7 represents ciphertext.

password: A string from 1 to 16 alphanumeric characters or symbols. The password is case-sensitive, and cannot contain question marks. By default, it is empty.

Command Mode

Router Configuration Mode

Example

Configure the authentication mode of a virtual-link as md5 authentication, with the transmission area as Area 2 and the ID of the neighboring router on the other endpoint as 3.3.3.3, with the authentication ID as 2 and the authentication key as 123456:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#area 2 virtual-link 3.3.3.3 message-digest-key 2
```

```
md5 123456
```

45.22 capability opaque

Description

The **capability opaque** is used to enable the Opaque LSA feature. To disable this feature, please use the **no capability opaque** command.

Syntax

capability opaque

no capability opaque

Parameter

None

Command Mode

Router Configuration Mode

Example

Enable the Opaque LSA feature:

```
Switch(config)#router ospf 1
Switch(config-router)#capability opaque
```

45.23 graceful-restart

Description

The **graceful-restart** is used to enable the OSPF GR feature. Before performing a graceful restart, ensure that the GR Restarter is configured with this feature. To disable this feature, please use the **no graceful-restart** command.

Syntax

```
graceful-restart
no graceful-restart
```

Parameter

None

Command Mode

Router Configuration Mode

Example

Enable the OSPF GR feature:

```
Switch(config)#router ospf 1
Switch(config-router)#graceful-restart
```

45.24 graceful-restart

grace-period

Description

The **graceful-restart grace-period** is used to configure the graceful restart period, that is, the maximum time required for the graceful restart process. If the actual restart time exceeds this value, the graceful restart will fail. To restore the default configuration, please use the **no graceful-restart grace-period** command.

Syntax

graceful-restart grace-period *period*

no graceful-restart grace-period *period*

Parameter

period: Graceful restart period, ranging from 1 to 1800 seconds, and the default value is 120.

Command Mode

Router Configuration Mode

Example

Configure the graceful restart period to 180 seconds:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#graceful-restart grace-period 180
```

45.25 graceful-restart helper

Description

The **graceful-restart helper** is used to enable the GR Helper feature to assist the GR Restarter in its graceful restart process. To restore the default configuration, please use the **no graceful-restart helper** command.

Syntax

graceful-restart helper [*rid*]

no graceful-restart helper [*rid*]

Parameter

rid: GR Helper is supported for the neighboring GR Restarter whose router-id is rid. If rid is not specified, GR Helper is supported for all neighboring GR Restarters by default.

Command Mode

Router Configuration Mode

Example

Configure GR Helper to support graceful restart for all neighboring GR Restarters:

```
Switch(config)#router ospf 1
Switch(config-router)#graceful-restart helper
```

45.26 graceful-restart helper planned-only

Description

The **graceful-restart helper planned-only** is used to configure the GR Helper to only support planned-only restart function, which is disabled by default. To restore the default configuration, please use the **no graceful-restart helper planned-only** command.

Syntax

```
graceful-restart helper planned-only
no graceful-restart helper planned-only
```

Parameter

None.

Command Mode

Router Configuration Mode

Example

Enable the GR Helper to support planned-only restart function:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#graceful-restart helper planned-only
```

45.27 graceful-restart helper strict-lsa-checking

Description

The **graceful-restart helper strict-lsa-checking** is used to configure the GR Helper to strictly check LSA, which is disabled by default. When this function is configured, once the LSAs of the GR Restarter and the GR Helper do not match, the graceful restart will be failed. To restore the default configuration, please use the **no graceful-restart helper strict-lsa-checking** command.

Syntax

```
graceful-restart helper strict-lsa-checking
```

```
no graceful-restart helper strict-lsa-checking
```

Parameter

None.

Command Mode

Router Configuration Mode

Example

Configure the GR Helper to strictly check LSA:

```
Switch(config)#router ospf 1
```

```
Switch(config-router)#graceful-restart helper strict-lsa-checking
```

45.28 ip ospf area

Description

The **ip ospf area** is used to enable the interface in the area of OSPF. This command has higher priority than network command. To restore to the default value, please use the **no ip ospf area** command.

Syntax

```
ip ospf area area-id [instance-id instance-id]  
no ip ospf area area-id [instance-id instance-id]  
ip ospf process-id area area-id  
no ip ospf process-id area area-id
```

Parameter

process-id: Process ID, ranging from 1 to 65535. Sixteen processes can be created at most.

area-id—— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

Command Mode

Interface Configuration Mode

Example

Configure the Process ID and area ID of interface VLAN 2:

```
Switch(config)#interface vlan 2  
Switch(config-if)#ip ospf 1 area 10
```

45.29 ip ospf cost

Description

The **ip ospf cost** is used to configure the interface cost. To restore to the default value, please use the **no ip ospf cost** command.

Syntax

```
ip ospf cost cost  
no ip ospf cost
```

Parameter

cost—— The interface cost, ranging from 1 to 65535. The default value is calculated according to the bandwidth.

Command Mode

Interface Configuration Mode

Example

Configure the cost of interface VLAN 2 as 10:

```
Switch(config)#interface vlan 2
Switch(config-if)# ip ospf cost 10
```

45.30 ip ospf retransmit-interval

Description

The **ip ospf retransmit-interval** command is used to configure the interval to retransmit the LSA, DD and LSR packets on the specified interface. To restore to default value, please use the **no ip ospf retransmit-interval** command.

Syntax

```
ip ospf retransmit-interval interval
no ip ospf retransmit-interval
```

Parameter

interval— The retransmit interval, ranging from 1 to 65535 seconds. The default value is 5 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the retransmission interval of interface VLAN 2 as 10 seconds:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf retransmit-interval 10
```

45.31 ip ospf transmit-delay

Description

The **ip ospf transmit-delay** is used to configure the transmission delay of LSA on the specified interface. To restore to default value, please use the **no ip ospf transmit-delay**.

Syntax

ip ospf transmit-delay *delay*
no ip ospf transmit-delay

Parameter

delay— The LSA transmission delay, ranging from 1 to 65535 seconds. The default value is 1 second.

Command Mode

Interface Configuration Mode

Example

Configure the LSA transmission delay of interface VLAN 2 as 2 seconds.

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf retransmit-delay 2
```

45.32 ip ospf priority

Description

The **ip ospf priority** is used to configure the priority of the specified interface. To restore to the default value, please use the **no ip ospf priority** command.

Syntax

ip ospf priority *pri*
no ip ospf priority

Parameter

pri— The priority of the interface, ranging from 0 to 255 and the default value is 1. Interface with the priority 0 cannot be elected as DR or BDR.

Command Mode

Interface Configuration Mode

Example

Configure the priority of the interface VLAN 2 as 1:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf priority 1
```

45.33 ip ospf hello-interval

Description

The **ip ospf hello-interval** is used to configure the hello intervals on the specified interface. To restore to the default value, please use the **no ip ospf hello-interval** command.

Syntax

```
ip ospf hello-interval interval  
no ip ospf hello-interval
```

Parameter

Interval—— The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the interval of the hello packets sent on interface VLAN 2 as 20 seconds:

```
Switch(config)#interface vlan 2  
Switch(config-if)#ip ospf hello-interval 20
```

45.34 ip ospf dead-interval

Description

The **ip ospf dead-interval** command is used to set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down. To restore to default value, please use the **no ip ospf dead-interval** command.

Syntax

```
ip ospf dead-interval interval  
no ip ospf dead-interval
```

Parameter

Interval—— The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the neighbor's failure interval on interface VLAN 2 as 50 seconds:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf dead-interval 50
```

45.35 ip ospf authentication

Description

The **ip ospf authentication** command is used to configure the authentication mode of the specified interface. To restore to default value, please use the **no ip ospf authentication** command.

Syntax

```
ip ospf authentication [ message-digest ] [ null ]
no ip ospf authentication
```

Parameter

message-digest—— Specify the authentication type as MD5.

null —— No authentication. By default it is no authentication.

If no authentication mode is specified here, the default mode will be simple authentication.

Command Mode

Interface Configuration Mode

Example

Configure the authentication type of interface VLAN 2 as MD5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf authentication message-digest
```

45.36 ip ospf authentication-key

Description

The **ip ospf authentication-key** command is used to configure the key of the simple authentication. To cancel this configuration, please use the **no ip ospf authentication-key** command.

Syntax

ip ospf authentication-key *password*
no ip ospf authentication-key

Parameter

password—— Super password, a string from 1 to 8 alphanumeric characters or symbols. The password is case sensitive, allows spaces but ignores leading spaces, and cannot contain question marks. By default, it is empty.

Command Mode

Interface Configuration Mode

Example

Configure the authentication mode of interface VLAN 2 as simple authentication, and the password as 123:

```
Switch(config)#interface vlan 2  
  
Switch(config-if)#ip ospf authentication-key 123
```

45.37 ip ospf message-digest-key

Description

The **ip ospf message-digest-key** is used to configure the ID and password of the md5 authentication on the specified interface. To cancel the configuration, please use **no ip ospf message-digest-key** command.

Syntax

ip ospf message-digest-key *id md5 password*
no ip ospf message-digest-key *id*

Parameter

id—— The ID of the md5 authentication key, ranging from 1 to 255.

password—— A string from 1 to 16 alphanumeric characters or symbols.
The password is case sensitive, and cannot contain question marks. Key configuration is required to take effect.

Command Mode

Interface Configuration Mode

Example

Configure md5 authentication key ID as 1 and password as abc on interface VLAN 2:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf message-digest-key 1 md5 abc
```

45.38 ip ospf network

Description

The **ip ospf network** command is used to configure the network type on the specified interface. To restore to default, please use the **no ip ospf network** command.

Syntax

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint |  
point-to-point }  
no ip ospf network
```

Parameter

broadcast —— The broadcast network type. It is the default value.

non-broadcast —— The NBMA network type.

point-to-multipoint —— The point-to-multipoint network type.

point-to-point —— The point-to-point network type.

Command Mode

Interface Configuration Mode

Example

Configure the network type on interface VLAN 2 as broadcast:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf network broadcast
```

45.39 ip ospf mtu-ignore

Description

The **ip ospf mtu-ignore** command is used to ignore the MTU check in the DD exchanging process. This check is scheduled by default and the adjacency relationship will not establish if the MTUs are not matched. To restore to the default value, please use the **no ip ospf mtu-ignore** command.

Syntax

```
ip ospf mtu-ignore
no ip ospf mtu-ignore
```

Command Mode

Interface Configuration Mode

Example

Configure interface VLAN 2 to ignore the MTU field check in the DD exchange process:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf mtu-ignore
```

45.40 ip ospf passive

Description

The **ip ospf passive** command is used to prevent an interface from sending OSPF packets. To restore to the default settings, please use **no ip ospf passive** command. The interface is allowed to send OSPF packets by default.

Syntax

```
ip ospf passive
no ip ospf passive
```

Command Mode

Interface Configuration Mode

Example

Prevent interface VLAN 2 from sending OSPF packets:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip ospf passive
```

45.41 clear ip ospf

Description

The **clear ip ospf** command is used to reset the OSPF process, which will clear all the dynamic information. The **clear ip ospf process** command will reset all the OSPF processes.

Syntax

```
clear ip ospf [process-id]
clear ip ospf process
```

Parameter

process-id — The process ID, ranging from 1 to 65535.

Command Mode

Privileged EXEC Mode

Example

Reset all the OSPF processes:

```
Switch#clear ip ospf process
Reset selected OSPF processes? (Y/N):y
```

45.42 show ip ospf

Description

The **show ip ospf** is used to display the global information of the OSPF process.

Syntax

show ip ospf [*process-id*]

Parameter

process-id—— The process ID, ranging from 1 to 65535. The global information of all the OSPF processes will be displayed if no process-id is specified.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the global information of all the OSPF processes:

```
Switch#show ip ospf
```

45.43 show ip ospf database

Description

The **show ip ospf database** command is used to display the LSDB. The detailed LSA information will be displayed if the LSA type is specified. The LSDB summary information will be displayed if the LSA type is not specified.

Syntax

show ip ospf [*process-id*] **database** [asbr-summary | external | network | nssa-external | router | summary]

Parameter

process-id—— The process ID, ranging from 1 to 65535. The LSDBs of all processes will be displayed if no process ID is specified.

asbr-summary | external | network | nssa-external | router | summary —— The LSA type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the detailed information of router-LSA in process 1:

```
Switch#show ip ospf 1 database router
```

45.44 show ip ospf interface

Description

The **show ip ospf interface** command is used to display the interface information.

Syntax

show ip ospf [*process-id*] **interface** [*interface-name interface-number*]

Parameter

process-id—— The process ID. The information of all the processes will be displayed if process ID is not specified.

interface-name interface-number—— Specify the interface name and number to display the interface's detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the information of the interfaces in all the OSPF processes:

```
Switch#show ip ospf interface
```

45.45 show ip ospf neighbor

Description

The **show ip ospf neighbor** command is used to display information of the OSPF neighbor.

Syntax

show ip ospf [*process-id*] **neighbor** [**detail** | *interface-name interface-number*]

Parameter

process-id—— The process ID, ranging from 1 to 65535. The neighbors' information of all processes will be displayed if no process ID is specified.

detail—— The detailed information of the neighbor.

interface-name interface-number——Specify the interface name and number to display the neighbor's detailed information on this interface.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the neighbors' detailed information in process 1:

```
Switch#show ip ospf 1 neighbor detail
```

45.46 show ip ospf border-routers

Description

The **show ip ospf border-routers** is used to display the routing tables of the ABR/ASBR.

Syntax

```
show ip ospf [ process-id ] border-routers
```

Parameter

process-id—— The process ID, ranging from 1 to 65535. The ABR/ASBR routing tables of all processes will be displayed if no process ID is specified.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ABR/ASBR routing tables of all the OSPF processes:

```
Switch#show ip ospf border-routers
```

45.47 show ip ospf route

Description

The **show ip ospf route** command is used to display the OSPF routing table.

Syntax

```
show ip ospf route
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the routing tables of OSPF:

```
Switch#show ip ospf route
```

45.48 show ip ospf [process-id] graceful-restart helper

Description

The **show ip ospf [process-id] graceful-restart helper** command is used to view the status and configuration information of the GR Helper and the reason of last exit.

Syntax

```
show ip ospf [process-id] graceful-restart helper
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the status and configuration information of the GR Helper and the reason of last exit:

```
Switch# show ip ospf graceful-restart helper
```

Chapter 46 OSPFv3 Configuration Commands (Only for Certain Devices)

OSPF is an Interior Gateway Protocol (IGP) designed expressly for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

Currently, OSPF Version 2 (RFC2328) is used for the IPv4 protocol; Use OSPF Version 3 (RFC2740) for IPv6 protocol. OSPFv3 is short for OSPF Version 3 and is the OSPF routing protocol running on IPv6 (RFC5340, same as RFC2740).

46.1 ipv6 router ospf

Description

The **ipv6 router ospf** command is used to enable an OSPFv3 routing process and enter the router configuration mode. To delete the specified OSPFv3 routing process, please use the **no ipv6 router ospf** command.

When the OSPFv3 instance has not been created, this command is used to create an OSPFv3 instance and enter the Router configuration mode. When the command has a VRF name, it means that the OSPFv3 instance belongs to the VRF instance; if the VRF parameter is not specified, the OSPFv3 instance belongs to the public network after it is created. When the OSPFv3 instance has been created, using this command with or without the correct VRF name can enter the Router configuration mode.

Syntax

```
ipv6 router ospf [vrf vrf-name]  
no ipv6 router ospf [vrf vrf-name]
```

Parameter

vrf-name —— VRF instance name.

Command Mode

Global Configuration Mode

Example

Create an OSPFv3 instance and add it to vrf1:

```
Switch(config)#ipv6 router ospf vrf vrf1
```


46.2 router-id

Description

The **router-id** command is used to configure the router ID. The **no router-id** command is used to delete the configured router ID. If no router ID is configured manually or the configured router ID is deleted, the highest IPv4 address among all loopback interfaces will be chosen as the router ID.

Syntax

Router-id *router-id*

no router-id

Parameter

router-id——The route ID in the format of dotted decimal notation. 0.0.0.0 is illegal.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the router ID of OSPFv3 routing process 1 as 1.1.1.1:

```
Switch(config)# ipv6 router ospf  
Switch(config-router)#router-id 1.1.1.1
```

46.3 maximum-paths

Description

The **maximum-paths** command is used to configure the maximum number of the equal-cost multipath routings. To restore to default value, please use the **no maximum-paths** command.

Syntax

maximum-paths *number*

no maximum-paths

Parameter

number — The maximum number of the equal-cost multipath routings, ranging from 1 to 32. The default value is 32.

Command Mode

Router Configuration Mode

Example

Configure the maximum number of the equal-cost multipath routings as 2:

```
Switch(config)#ipv6 router ospf
Switch(config-router)#maximum-paths 2
```

46.4 redistribute

Description

The **redistribute** command is used to configure the ASBR to redistribute the external routes from other routing protocols to the OSPFv3 domain in type-5 LSAs. To restore the certain optional parameters to default values, please use the **no redistribute** command with corresponding parameters.

Syntax

```
redistribute { connected | static | ripng }
no redistribute { connected | static | ripng }
```

Parameter

connected — Specify the external route type as connected.

static — Specify the external route type as static.

ripng — Specify the external route type as RIPNG.

Command Mode

Router Configuration Mode

Example

Redistribute the RIPNG routes from the external in the OSPFv3 domain.

```
Switch(config)#ipv6 router ospf
Switch(config-router)#redistribute ripng
```

46.5 default-information originate

Description

The **default-information originate** command is used to advertise the default route as AS-External LSA. To cancel the advertisement of the default route, please use the **no default-information originate** command without any optional parameters. To restore the certain parameters to default values, please use the **no default-information originate** command with corresponding parameters.

Syntax

```
default-information originate [ always ] [ metric cost ] [ metric-type type ]  
no default-information originate [ always ] [ metric cost ] [ metric-type type ]
```

Parameter

always — OSPFv3 will advertise the default route whether there is default route is the IPV6 routing table or not. If the parameter is not configured, OSPFv3 will advertise the default route only when there is default route in the IPV6 routing table.

cost — The default cost of the default route, ranging form 1 to 16777214. Its default value is 1.

type — The type of the external routes, either 1 or 2. The default value is 2.

Command Mode

Router Configuration Mode

Example

Configure OSPF to advertise the default route whether there is default route is the IP routing table or not:

```
Switch(config)# ipv6 router ospf  
Switch(config-router)#default-information originate always
```

46.6 auto-cost

Description

The **auto-cost** command is used to enable the auto computing function of the interface cost and configure the reference bandwidth. The interface cost is the ratio of the reference bandwidth to the interface bandwidth. To restore the reference bandwidth to default value, please use the **no auto-cost reference-bandwidth** command.

Syntax

auto-cost reference-bandwidth *bandwidth*

no auto-cost reference-bandwidth

Parameter

bandwidth—— The reference bandwidth, ranging from 1 to 4294967 Mbps. Its default value is 100Mbps.

Command Mode

Router Configuration Mode

Example

Enable the auto computing function of the interface cost and configure the reference bandwidth as 10000 Mbps:

```
Switch(config)#ipv6 router ospf
```

```
Switch(config-router)#auto-cost reference-bandwidth 10000
```

46.7 distance

Description

The **distance** command is used to configure the OSPFv3 administrative distance. To restore to the default distance, please use the **no distance** command. The administrative distance represents the priority of the routes. The smaller administrative distance corresponds to higher priority. When different routing protocols possess the same route to the same destination, the route with the highest priority will be selected to add to the IPv6 routing table according to the administrative distance.

Syntax

distance *administrative-distance*

no distance

Parameter

administrative-distance—— Routing administrative distance, ranging from 1 to 254. Its default value is 110.

Command Mode

Router Configuration Mode

Example

Configure the OSPFV3 routing administrative distance as 100:

```
Switch(config)#ipv6 router ospf
Switch(config-router)#distance 100
```

46.8 distance ospfv3

Description

The **distance ospfv3** command is used to configure the OSPFv3 distance for different types of routes. To restore to the default distance, please use the **no distance** command.

Syntax

distance ospfv3 { external *distance* | inter-area *distance* | intra-area *distance* }

no distance

Parameter

external —— External type 5 and type 7 routes.

inter-area —— Inter-area routes.

intra-area —— Intra-area routes.

distance—— Distance for different types of routes, ranging from 1 to 254. Its default value is 110.

Command Mode

Router Configuration Mode

Example

Configure the administrative distances of OSPFV3 routing as 100:

```
Switch(config)#ipv6 router ospf
Switch(config-router)#distance ospfv3 external 100 inter-area 100
intra-area 100
```

46.9 timers throttle spf

Description

The **timers throttle spf** command is used to configure the computing delay and interval of the SPF, thus preventing the consumption of the CPU and memory caused by frequent SPF computing. To restore to the default value, please use the **no timers throttle spf** command.

Syntax

```
timers throttle spf spf-delay spf-holdtime spf-max-holdtime
no timers throttle spf
```

Parameter

spf-delay—— The delay time of the SPF computing, ranging from 1 to 600000 milliseconds. The default value is 0 milliseconds.

spf-holdtime—— The minimum interval between two SPF computings, ranging from 1 to 600000 milliseconds. The default value is 50 milliseconds

spf-max-holdtime—— The Maximum interval between two SPF computings, ranging from 1 to 600000 milliseconds. The default value is 5000 milliseconds

Command Mode

Router Configuration Mode

Example

Configure the computing delay and interval of the SPF as 10 seconds:

```
Switch(config)#ipv6 router ospf
Switch(config-router)#timers throttle spf 10000 10000 50000
```

46.10 timers lsa arrival

Description

The **timers lsa arrival** command is used to configure the time interval for OSPFv3 LSA reception. To restore to the default value, please use the **no timers lsa arrival** command.

Syntax

```
timers lsa arrival delay-time  
no timers lsa arrival
```

Parameter

delay-time—— The time interval for OSPFv3 LSA reception, ranging from 1 to 600000 milliseconds. The default value is 1000 milliseconds.

Command Mode

Router Configuration Mode

Example

Configure the time interval for OSPFv3 LSA reception as 10 seconds:

```
Switch(config)#ipv6 router ospf  
Switch(config-router)#timers lsa arrival 10000
```

46.11 distance ospf

Description

The **distance ospf** command is used to configure the OSPF distance for different types of routes. To restore to the default distance, please use the **no distance** command.

Syntax

```
distance ospf { external distance | inter-area distance | intra-area distance }  
no distance
```

Parameter

external —— External type 5 and type 7 routes.

inter-area — Inter-area routes.

intra-area — Intra-area routes.

distance — Distance for different types of routes, ranging from 1 to 254. Its default value is 110.

Command Mode

Router Configuration Mode

Example

Configure the administrative distances of OSPF routing as 100:

```
Switch(config)# router ospf 1
Switch(config-router)#distance ospf external 100 inter-area 100
intra-area 100
```

46.12 area stub

Description

The **area stub** command is used to define an area as a stub area. To restore the stub area to a normal one, please use the **no area stub** command. To restore the certain parameters to default values, please use the **no area stub** command with corresponding parameters.

Syntax

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

no-summary — Configure the stub area as a totally stub area, where the ABR advertises neither the destinations in other areas nor the external routes. The stub area is not a totally stub area by default.

Command Mode

Router Configuration Mode

Example

Configure the area 1 as a totally stub area:


```
Switch(config)#ipv6 router ospf
Switch(config-router)#area 1 stub no-summary
```

46.13 area nssa

Description

The **area nssa** command is used to define an area as a NSSA area. To restore the NSSA area to a normal one, please use the **no area nssa** command without any optional parameters. To restore the certain parameters to default values, please use the **no area nssa** command with corresponding parameters.

Syntax

```
area area-id nssa [ no-summary ]
no area area-id nssa [ no-summary ]
```

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

no-summary — Select to not send summary LSAs into the NSSA.

Command Mode

Router Configuration Mode

Example

Configure the Area 1 as a totally NSSA area:

```
Switch(config)# ipv6 router ospf
Switch(config-router)# area 1 nssa no-summary
```

46.14 area range

Description

The **area range** is to configure a summary route. To delete this route, please use the **no area range** command. By default no route is summarized.

This command is only used with the ABR to summarize the route information of a certain area. The ABR only sends one summarized route of the routes in

the aggregated segment to the other areas. An area can be configured with multiple summary segments, which can be aggregated by OSPF.

If the **no area range** command is configured, the formally summarized routes will be redistributed.

Syntax

```
area area-id range ipv6-address/mask-num [ advertise ] [ cost cost ]  
[ not-advertise ]  
no area area-id range ip-address mask [ advertise ] [ cost cost ]  
[ not-advertise ]
```

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

ipv6-address—— The destination of the aggregated route.

mask-num—— The network mask for aggregated route, in the format of mask bits.

cost—— The cost of the aggregated route, ranging from 1 to 16777214. The default value is the maximum one of all the aggregated routes.

Command Mode

Router Configuration Mode

Example

Configure one aggregated route 2001::1/64 with the cost 10 in the Area 0:

```
Switch(config)# ipv6 router ospf  
Switch(config-router)# area 0 range 2001::1/64 cost 10
```

46.15 ipv6 ospf area

Description

The **ipv6 ospf area** is used to assign the interface to different regions. By default, the interface does not belong to any area. Only the interface attached to a certain area can receive ospfv3 packets normally. To restore to the default value, please use the **no ipv6 ospf area** command.

Syntax

```
ipv6 ospf area area-id [instance-id instance-id]  
no ipv6 ospf area area-id [instance-id instance-id]
```

Parameter

area-id: The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

instance-id—— The instance ID, ranging from 0 to 255. OSPFv3 supports running multiple instances on a single link, using the optional parameter *instance-id* as the instance identifier. The instance number only affects the reception of OSPFv3 messages. By default, this parameter value is 0. To restore the default value, use the **no ipv6 ospf area** *area-id* *instance-id* command.

Command Mode

Interface Configuration Mode

Example

Assign interface VLAN 2 to area 10:

```
Switch(config)#interface vlan 2  
Switch(config-if)#ipv6 ospf area 10
```

46.16 ipv6 ospf cost

Description

The **ipv6 ospf cost** is used to configure the interface cost. To restore to the default value, please use the **no ipv6 ospf cost** command.

Syntax

```
ipv6 ospf cost cost  
no ipv6 ospf cost
```

Parameter

cost—— The interface cost, ranging from 1 to 65535. The default value is calculated according to the bandwidth.

Command Mode

Interface Configuration Mode

Example

Configure the cost of interface VLAN 2 as 10:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf cost 10
```

46.17 ipv6 ospf retransmit-interval

Description

The **ipv6 ospf retransmit-interval** command is used to configure the interval to retransmit the LSA, DD and LSR packets on the specified interface. To restore to default value, please use the **no ipv6 ospf retransmit-interval** command.

Syntax

```
ipv6 ospf retransmit-interval interval
no ipv6 ospf retransmit-interval
```

Parameter

interval— The retransmit interval, ranging from 1 to 65535 seconds. The default value is 5 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the retransmission interval of interface VLAN 2 as 10 seconds:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf retransmit-interval 10
```

46.18 ipv6 ospf transmit-delay

Description

The **ipv6 ospf transmit-delay** is used to configure the transmission delay of LSA on the specified interface. To restore to default value, please use the **no ipv6 ospf transmit-delay**.

Syntax

```
ipv6 ospf transmit-delay delay  
no ipv6 ospf transmit-delay
```

Parameter

delay—— The LSA transmission delay, ranging from 1 to 3600 seconds. The default value is 1 second.

Command Mode

Interface Configuration Mode

Example

Configure the LSA transmission delay of interface VLAN 2 as 2 seconds.

```
Switch(config)#interface vlan 2  
Switch(config-if)#ipv6 ospf retransmit-delay 2
```

46.19 ipv6 ospf priority

Description

The **ipv6 ospf priority** is used to configure the priority of the specified interface. To restore to the default value, please use the **no ipv6 ospf priority** command.

Syntax

```
ipv6 ospf priority pri  
no ipv6 ospf priority
```

Parameter

pri—— The priority of the interface, ranging from 0 to 255 and the default value is 1. Interface with the priority 0 cannot be elected as DR or BDR.

Command Mode

Interface Configuration Mode

Example

Configure the priority of the interface VLAN 2 as 1:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf priority 1
```

46.20 ipv6 ospf hello-interval

Description

The **ipv6 ospf hello-interval** is used to configure the hello intervals on the specified interface. To restore to the default value, please use the **no ipv6 ospf hello-interval** command.

Syntax

```
ipv6 ospf hello-interval interval
no ipv6 ospf hello-interval
```

Parameter

Interval—— The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the interval of the hello packets sent on interface VLAN 2 as 20 seconds:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf hello-interval 20
```

46.21 ipv6 ospf dead-interval

Description

The **ipv6 ospf dead-interval** command is used to set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPFv3 router to be down. To restore to default value, please use the **no ipv6 ospf dead-interval** command.

Syntax

ipv6 ospf dead-interval *interval*
no ipv6 ospf dead-interval

Parameter

Interval—— The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the neighbor's failure interval on interface VLAN 2 as 50 seconds:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf dead-interval 50
```

46.22 ipv6 ospf network

Description

The **ipv6 ospf network** command is used to configure the network type on the specified interface. To restore to default, please use the **no ipv6 ospf network** command.

Syntax

ipv6 ospf network { broadcast | point-to-point }
no ipv6 ospf network

Parameter

broadcast —— The broadcast network type. It is the default value.

point-to-point — The point-to-point network type.

Command Mode

Interface Configuration Mode

Example

Configure the network type on interface VLAN 2 as broadcast:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf network broadcast
```

46.23 ipv6 ospf mtu-ignore

Description

The **ipv6 ospf mtu-ignore** command is used to ignore the MTU check in the DD exchanging process. This check is scheduled by default and the adjacency relationship will not establish if the MTUs are not matched. To restore to the default value, please use the **no ipv6 ospf mtu-ignore** command.

Syntax

```
ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore
```

Command Mode

Interface Configuration Mode

Example

Configure interface VLAN 2 to ignore the MTU field check in the DD exchange process:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf mtu-ignore
```

46.24 ipv6 ospf passive

Description

The **ipv6 ospf passive** command is used to prevent an interface from sending OSPFv3 packets. To restore to the default settings, please use **no**

ipv6 ospf passive command. The interface is allowed to send OSPFv3 packets by default.

Syntax

ipv6 ospf passive
no ipv6 ospf passive

Command Mode

Interface Configuration Mode

Example

Prevent interface VLAN 2 from sending OSPFv3 packets:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 ospf passive
```

46.25 clear ipv6 ospf

Description

The **clear ipv6 ospf** command is used to reset the OSPFv3 process, which will clear all the dynamic information. The **clear ipv6 ospf process** command will reset the OSPFv3 process. The **clear ipv6 ospf interface** command will reset the configuration of the interface in the OSPFv3 process.

Syntax

clear ipv6 ospf { process | interface }

Command Mode

Privileged EXEC Mode

Example

Reset the OSPFv3 process:

```
Switch#clear ipv6 ospf process
Reset selected OSPFv3 processes? (Y/N):y
```

46.26 show ipv6 ospf

Description

The **show ipv6 ospf** is used to display the global information of the OSPFv3 process.

Syntax

```
show ipv6 ospf
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the global information of the OSPFv3 processes:

```
Switch#show ipv6 ospf
```

46.27 show ipv6 ospf database

Description

The **show ipv6 ospf database** command is used to display the LSDB.

Syntax

```
show ipv6 ospf database
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the LSDB in OSPFv3 process:

```
Switch#show ipv6 ospf database
```

46.28 show ipv6 ospf interface

Description

The **show ipv6 ospf interface** command is used to display the interface information.

Syntax

show ipv6 ospf interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the information of the interfaces in the OSPFv3 process:

```
Switch#show ipv6 ospf interface
```

46.29 show ipv6 ospf neighbor

Description

The **show ipv6 ospf neighbor** command is used to display information of the OSPFv3 neighbor.

Syntax

show ipv6 ospf neighbor

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the neighbors' detailed information in OSPFv3 process:

```
Switch#show ipv6 ospf neighbor
```

46.30 show ipv6 ospf border-routers

Description

The **show ipv6 ospf border-routers** is used to display the routing tables of the ABR/ASBR.

Syntax

show ipv6 ospf border-routers

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ABR/ASBR routing tables of the OSPFv3 process:

```
Switch#show ipv6 ospf border-routers
```

46.31 show ipv6 ospf rib

Description

The **show ipv6 ospf rib** command is used to display the OSPFv3 routing table.

Syntax

```
show ipv6 ospf route
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the routing tables of OSPFv3:

```
Switch#show ipv6 ospf rib
```

Chapter 47 BFD Configuration Commands (Only for Certain Devices)

Bidirectional Forwarding Detection (BFD) is a unified network detection mechanism used for rapidly detecting and monitoring the forwarding connectivity status of links or IP routes in a network.

In order to minimize the impact of device failures on business operations and enhance network reliability, network devices need to promptly detect communication failures with neighboring devices to take timely action and ensure uninterrupted services. In existing networks, some links are often monitored for faults through hardware detection signals such as SDH alarms; however, not all mediums can provide hardware detection. In such cases, applications rely on the upper-layer protocol's own Hello message mechanism for fault detection. The fault detection time of upper-layer protocols typically exceeds 1 second, which is intolerable for certain applications. In L3 networks, the Hello message detection mechanism cannot detect faults for all routes, such as static routes, posing challenges in diagnosing faults in interconnection between systems.

BFD facilitates rapid detection and monitoring of forwarding connectivity status for links or IP routes in a network, thereby improving network performance. By swiftly identifying communication failures between neighboring systems, users can establish backup channels promptly for communication recovery, ensuring network reliability.

47.1 bfd-template

Description

This command is used to create a BFD template. To delete the BFD template, please use the **no bfd-template** command.

Syntax

```
bfd-template template  
no bfd-template template
```

Parameter

template—— Template name, the value range is 1 to 32 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a BFD template named b1:

```
Switch(config)#bfd-template b1
```

47.2 detect-multiplier

Description

This command is used to specify the detect-multiplier of the BFD template. To restore the detect-multiplier of the BFD template to the default, please use the **no detect-multiplier** command.

Syntax

detect-multiplier *multiplier*
no detect-multiplier

Parameter

multiplier — The detect-multiplier of the BFD template. The value range is an integer between 3 to 50, and the default value is 3.

Command Mode

BFD Template Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the detect-multiplier of BFD template b1 to 10:

```
Switch(config)#bfd-template b1  
Switch(config-bfd)#detect-multiplier 10
```

47.3 receive-interval

Description

This command is used to configure the receive interval for BFD packets. To restore the default value, please use the **no receive-interval** command.

Syntax

receive-interval *interval*
no receive-interval

Parameter

interval—— The receive interval for BFD packets. The value range is an integer between 100 to 1000 milliseconds, and the default value is 300.

Command Mode

BFD Template Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the receive interval of BFD template b1 to 500 milliseconds:

```
Switch(config)#bfd-template b1
Switch(config-bfd)#receive-interval 500
```

47.4 transmit-interval

Description

This command is used to configure the transmit interval for BFD packets. To restore the default value, please use the **no transmit-interval** command.

Syntax

transmit-interval *interval*
no transmit-interval

Parameter

interval—— The transmit interval for BFD packets. The value range is an integer between 100 to 1000 milliseconds, and the default value is 300.

Command Mode

BFD Template Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the transmit interval of BFD template b1 to 500 milliseconds:

```
Switch(config)#bfd-template b1
Switch(config-bfd)#transmit-interval 500
```

47.5 transmit-interval

Description

This command is used to disable BFD session detection (enabled by default) and put it into AdminDown state. To enable the session, please use the **no shutdown** command

Syntax

```
shutdown
no shutdown
```

Parameter

none

Command Mode

BFD Template Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the BFD session detection of BFD template b1:

```
Switch(config)#bfd-template b1
Switch(config-bfd)#shutdown
```

47.6 passive-mode

Description

This command is used to enable the passive mode of the BFD session (disabled by default). When it is enabled, the local BFD will not actively send BFD packets. To disable the passive mode of the BFD session, please use the **no passive-mode** command.

Syntax

passive-mode
no passive-mode

Parameter

None

Command Mode

BFD Template Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the passive mode of BFD template b1:

```
Switch(config)#bfd-template b1  
Switch(config-bfd)#passive mode
```

47.7 ip ospf bfd

Description

This command is used to enable the BFD feature on a specific OSPF interface (disabled by default). When it is enabled, the default BFD session parameters are used. To disable BFD feature on the interface, please use the **no ip ospf bfd** command.

Syntax

passive-mode
no passive-mode

Parameter

None

Command Mode

interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable BFD on interface vlan 10:

```
Switch(config)#interface vlan 10
Switch (config-if)#ip ospf bfd
```

47.8 ip ospf bfd template

Description

This command is used to bind a BFD template to a specific interface with OSPF enabled. The BFD template to be bound must exist. To cancel the binding and restore the BFD session parameters to the default values, please use the **no ip ospf bfd template** command. By default, no BFD template is bound to a specific interface with OSPF enabled.

Syntax

```
ip ospf bfd template template
no ip ospf bfd template
```

Parameter

template—— Template name. It should be configured BFD template

Command Mode

interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create BFD template b1, set the minimum sending interval to 400 ms, the minimum receiving interval to 400 ms, and the local detection multiplier to 4, enable BFD on interface vlan 10, and bind BFD template b1:

```
Switch(config)#bfd-template b1
Switch(config-bfd)#detect-multiplier 4
Switch(config-bfd)#receive-interval 400
Switch(config-bfd)#transmit-interval 400
Switch(config-bfd)#exit
Switch(config)#interface vlan 10
```

```
Switch(config-if)#ip ospf bfd
```

```
Switch(config-if)#ip ospf bfd template b1
```

47.9 ipv6 ospf bfd

Description

This command is used to enable the BFD feature on a specific OSPFv3 interface (disabled by default). When it is enabled, the default BFD session parameters are used. To disable BFD feature on the interface, please use the **no ipv6 ospf bfd** command.

Syntax

```
ipv6 ospf bfd
```

```
no ipv6 ospf bfd
```

Parameter

template—— Template name. It should be configured BFD template

Command Mode

interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable BFD on interface vlan 10:

```
Switch(config)#interface vlan 10
```

```
Switch(config-if)#ipv6 ospf bfd
```

47.10 ipv6 ospf bfd

Description

This command is used to bind a BFD template to a specific interface with OSPF enabled. The BFD template to be bound must exist. To cancel the binding and restore the BFD session parameters to the default values, please use the **no ipv6 ospf bfd template** command. By default, no BFD template is bound to a specific interface with OSPF enabled.

Syntax

```
ipv6 ospf bfd template template  
no ipv6 ospf bfd template
```

Parameter

None

Command Mode

interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create BFD template b1, set the minimum sending interval to 400 ms, the minimum receiving interval to 400 ms, and the local detection multiplier to 4, enable BFD on interface vlan 10, and bind BFD template b1:

```
Switch(config)#bfd-template b1  
Switch(config-bfd)#detect-multiplier 4  
Switch(config-bfd)#receive-interval 400  
Switch(config-bfd)#transmit-interval 400  
Switch(config-bfd)#exit  
Switch(config)#interface vlan 10  
Switch(config-if)#ip ospfv6 bfd  
Switch(config-if)#ip ospfv6 bfd template b1
```

47.11 isis bfd

Description

This command is used to configure BFD features or bind a BFD template on a specific interface with IS-IS enabled. The BFD template to be bound must exist. To disable the BFD features on the interface or cancel the binding to restore the BFD session parameters to default values, please use the **no isis bfd** command. By default, the BFD feature is disabled on a specific interface with IS-IS enabled.

Syntax

```
isis bfd [template]  
no isis bfd [template]
```

Parameter

template—— Template name. It should be configured BFD template.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a BFD template b1, set the minimum sending interval to 400 ms, the minimum receiving interval to 400 ms, and the local detection multiplier to 4, enable BFD on interface vlan 10, and bind BFD template b1 to the interface:

```
Switch(config)#bfd-template b1  
Switch(config-bfd)#detect-multiplier 4  
Switch((config-bfd)#receive-interval 400  
Switch((config-bfd)#transmit-interval 400  
Switch((config-bfd)#exit  
Switch((config)#interface vlan 10  
Switch((config-if)#ipv6 enable  
Switch((config-if)#isis bfd  
Switch((config-if)#isis bfd b1  
Switch(config)#end
```

47.12 show bfd counters

Description

This command is used to view the statistics of BFD sessions (such as the number of sent and received packets).

Syntax

```
show bfd counters
```

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the statistics of BFD sessions:

```
Switch# show bfd counters
```

47.13 show bfd neighbors

Description

This command is used to display the information of BFD sessions. The **details** command is used to display the detailed information. The **ipv4** command is used to display the neighbor information of a BFD session.

Syntax

show bfd neighbors

show bfd neighbors details

show bfd neighbors ipv4 [*ip*]

Parameter

ip — IPv4 address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the neighbor information of 192.168.0.100:

```
Switch# show bfd neighbors ipv4 192.168.0.100
```

Chapter 48 BGP Configuration Commands (Only for Certain Devices)

Border Gateway Protocol (BGP) is a distance vector routing protocol that enables routing reachability between Autonomous Systems (AS) and selects the best route.

BGP establishes a unique unicast-based connection for each BGP neighbor. To enhance the reliability of peer connections, BGP uses TCP (port 179) as the underlying transmission mechanism. Since tasks like acknowledgment, retransmission, and sequencing are handled by the TCP layer, the session maintenance and update mechanisms of BGP are greatly simplified. As BGP operates over TCP, a separate point-to-point session needs to be established for each peer.

Each BGP node passes routes from the routing table via downstream neighbors. BGP nodes perform route calculations based on the routes they advertise and pass the calculated results to upstream neighbors, so it's the primary task for routing BGP routes to successfully establish BGP neighbors.

The three earlier versions are BGP-1, BGP-2, and BGP-3, which are mainly used to exchange reachable routing information between ASs, build inter-AS propagation paths, prevent routing loops, and apply some routing policies at the AS level. The current version is BGP-4.

48.1 router bgp

Description

This command is used to enable the BGP function and enter the Router BGP configuration mode. To disable BGP and clear BGP instances, please use the **no router bgp** command.

Syntax

```
router bgp as-number  
no router bgp as-number
```

Parameter

as-number—— BGP AS number.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BGP function on the switch:

```
Switch(config)# router bgp 100
```

48.2 address-family {ipv4 | ipv6} unicast

Description

This command is used to enable the BGP IP address family function, and create the address-family configuration view. The IPv4 unicast address family is enabled by default and cannot be removed. To disable this function, please use the **no address-family ipv6 unicast** command.

Syntax

```
address-family {ipv4 | ipv6} unicast  
no address-family ipv6 unicast
```

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the public BGP IPv6 unicast address family functionality:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family ipv6 unicast
```


48.3 address-family {ipv4 | ipv6} vrf

Description

This command is used to create a private VRF BGP instance and enable the corresponding IP address family functionality. To disable this function, please use the **no address-family {ipv4 | ipv6} vrf** command.

Syntax

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

Parameter

name: VRF name.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a private VRF a BGP and enable its IPv4 unicast function:

```
Switch(config)#router bgp 100  
Switch(config-router)#address-family ipv4 vrf a
```

48.4 address-family targeted-peer evpn

Description

This command is used to enable the BGP L2VPN EVPN address family function. To disable this function, please use the **no address-family l2vpn evpn** command.

Syntax

```
address-family l2vpn evpn  
no address-family l2vpn evpn
```

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the public network BGP L2VPN EVPN address family functionality:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family l2vpn evpn
```

48.5 advertise l2vpn evpn

Description

This command is used to redistribute routes from the current address family into the L2VPN EVPN address family.

Syntax

advertise l2vpn evpn

no advertise l2vpn evpn

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Redistribute public network BGP IPv4 unicast address family routes into the L2VPN EVPN address family:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family ipv4 unicast
```

```
Switch (config-router-af)# advertise l2vpn evpn
```

Redistribute private network VRF a BGP IPv4 address family routes into the L2VPN EVPN address family:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# advertise l2vpn evpn
```

48.6 aggregate-address

Description

This command is used to create an aggregate route in the BGP routing table. To delete an aggregate route in the BGP routing table, please use the **no aggregate-address** command.

Syntax

aggregate-address *ipv4-address ipv4-mask* [as-set | summary-only]
no aggregate-address *ipv4-address ipv4-mask*

Parameter

ipv4-address: Specifies the IPv4 address of the aggregated route.

ipv4-mask: The network mask of the aggregated route.

as-set: Specifies the generation of routes with AS-SET.

summary-only: Neighbors will not learn the aggregated source detailed routes.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an aggregate route. The path advertised by this route is an AS set segment that contains all aggregate path information:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#aggregate-address 1.1.1.0 255.255.255.0 as-set
```

48.7 distance bgp

Description

This command is used to specify the management distance.

Syntax

distance bgp *external-distance internal-distance local-distance*

Parameter

external-distance: Management distance of internal routes

internal-distance: Management distance of external routes

local-distance: Management distance of local routes

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the BGP management distance:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#distance bgp 120 100 100
```

48.8 maximum-paths

Description

This command is used to configure the number of paths for BGP to perform load balancing.

Syntax

maximum-paths *path-number* [**ibgp**]

Parameter

path-number: Specifies the number of paths

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the number of load-balanced paths to 12 when the next-hop neighbors of multiple paths are all iBGP:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# maximum-paths 12 ibgp
```

48.9 network

Description

This command is used to advertise a specified route from the local routing table into the BGP routing table.

Syntax

network *ipv4-address* [mask] [*ipv4-mask*] [backdoor]

no network *ipv4-address* [mask] [*ipv4-mask*]

Parameter

ipv4-address: IPv4 address to be announced

ipv4-mask: IPv4 mask to be announced

backdoor: Declare as backdoor link and change ebgp route to ibgp route (advanced BGP feature)

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Advertise the route 1.1.1.1/32 into the local public BGP IPv4 unicast address family routing table:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#network 1.1.1.1 mask 255.255.255.0 backdoor
```

48.10 redistribute

Description

This command is used to enable the route redistribution feature to allow routing information of other routing protocols to be published to BGP. The no command without optional parameters can cancel external route redistribution, and the no command with optional parameters can restore the optional parameters to their default values.

Syntax

```
redistribute { connected | static | rip | isis | ospf process-id | isis [ tag  
area-name ] } [ metric cost ]  
no redistribute { connected | static | rip | isis | ospf process-id | isis [ tag  
area-name ] }
```

Parameter

connected | static | rip | ospf | isis: Select the source routing protocol.

Differentiated metrics can be defined when the routing information learned by the routing protocol is published to BGP.

process-id: Configure the instance number for redistributing OSPF routes.

area-name: Configure the area name for redistributing IS-ISf routes.

cost: Configure the metric for redistributing routes. The valid value is from 0 to 4294967295. This parameter is optional and defaults to the value specified by the default-metric command.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Redistribute RIP routing information to BGP:

```
Switch(config)#router bgp 100  
Switch(config-router)#redistribute rip
```

48.11 slow-peer detection

Description

This command is used to configure the BGP slow-peer detection function. To disable this function, please use the **no slow-peer detection** command.

Syntax

```
slow-peer detection {threshold time | disable}  
no slow-peer detection {threshold | disable}
```

Parameter

time: The slow-peer detection threshold, in seconds. The value ranges from 12 to 360 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the public network BGP slow-peer detection threshold to 60 seconds:

```
Switch(config)#router bgp 100
```

```
Switch(config)#slow-peer detection threshold 60
```

Set the private network VRF a BGP slow-peer detection threshold to 60 seconds:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# slow-peer detection threshold 60
```

48.12 timers bgp

Description

This command is used to configure the interval for sending keepalive messages and the neighbor hold time. To restore the default value, please use the **no timers bgp** command.

Syntax

```
timers bgp keepalive hold
```

```
no timers bgp
```

Parameter

keepalive: The interval between for sending keepalive messages between neighbors, ranging from 1-65535 seconds. The default value is 60.

hold: Neighbor hold time, ranging from 1-65535 seconds. The default value is 180.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the keepalive message sending interval to 10 seconds and the hold time to 30 seconds:

```
Switch(config)#router bgp 100
Switch(config-router)#timers bgp 10 30
```

48.13 bgp always-compare-med

Description

This command is used to allow the comparison of MED attribute values of routing paths from different AS neighbors. To restore the default value, please use the **no bgp always-compare-med** command.

Syntax

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

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Allow the comparison of MED attribute values of routing paths from different AS neighbors:

```
Switch(config)#router bgp 100
Switch(config-router)#bgp always-compare-med
```


48.14 bgp bestpath as-path confed

Description

This command is used to configure BGP routing to use as-path information for routes obtained from confederation neighbors. To cancel this configuration, please use the **no bgp bestpath as-path confed** command.

Syntax

bgp bestpath as-path confed
no bgp bestpath as-path confed

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP routing to use as-path information for routes obtained from confederation neighbors:

```
Switch(config)#router bgp 100  
Switch(config-router)#bgp bestpath as-path confed
```

48.15 bgp bestpath as-path ignore

Description

This command is used to configure BGP to ignore AS path information when selecting routes. To cancel this configuration, please use the **no bgp bestpath as-path ignore** command.

Syntax

bgp bestpath as-path ignore
no bgp bestpath as-path ignore

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to ignore AS path information when selecting routes:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp bestpath as-path ignore
```

48.16 bgp bestpath as-path multipath-relax

Description

This command is used to configure the BGP multipath decision process to consider paths with the same AS_PATH length. If not configured, the entire AS_PATH must match the multipath calculation. To cancel this configuration, please use the **no bgp bestpath as-path multipath-relax** command.

Syntax

bgp bestpath as-path multipath-relax

no bgp bestpath as-path multipath-relax

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the BGP multipath decision process to consider paths with the same AS_PATH length:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#bgp bestpath as-path multipath-relax
```

48.17 bgp bestpath compare-routerid

Description

This command is used to enable the router ID information comparison when selecting EBGp routes. To disable this configuration, please use the **no bgp bestpath compare-routerid** command.

Syntax

```
bgp bestpath compare-routerid  
no bgp bestpath compare-routerid
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the router ID information comparison when selecting EBGp routes:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#bgp bestpath as-path compare-routerid
```

48.18 bgp bestpath med confed

Description

This command is used to allow MED comparison between BGP confederation paths. To disable this configuration, please use the **no bgp bestpath med**

confed command. Note that confed and missing-as-worst can be configured and effective simultaneously.

Syntax

```
bgp bestpath med confed [ missing-as-worst ]  
no bgp bestpath med [confed] [missing-as-worst]
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the router ID information comparison when selecting EBGp routes:

```
Switch(config)#router bgp 100  
Switch(config-router)#bgp bestpath med confed
```

48.19 bgp bestpath med missing-as-worst

Description

This command is used to configure BGP to treat a route without a MED value as having a MED value of 4,294,967,295 during path selection. To disable this configuration, please use the **no bgp bestpath med missing-as-worst** command. Note that confed and missing-as-worst can be configured and effective simultaneously.

Syntax

```
bgp bestpath med missing-as-worst [ confed ]  
no bgp bestpath med [missing-as-worst] [confed]
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to treat routes without a MED value as having a MED value of 4,294,967,295:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp bestpath med missing-as-worst
```

48.20 bgp client-to-client reflection

Description

This command is used to configure the client-to-client route reflection. To disable this configuration, please use the **no bgp client-to-client reflection** command.

Syntax

```
bgp client-to-client reflection
no bgp client-to-client reflection
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the client-to-client route reflection:

```
Switch(config)#router bgp 100
Switch(config-router)#bgp client-to-client reflection
```

48.21 bgp cluster-id

Description

This command is used to configure the cluster ID of the route reflector. To disable this configuration, please use the **no bgp cluster-id** command.

Syntax

bgp cluster-id *ip-address*
no bgp cluster-id

Parameter

ip-address: IP address

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the reflector's cluster ID to be 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp cluster-id 1.1.1.1
```

48.22 bgp confederation identifier

Description

This command is used to configure the confederation ID. To disable this configuration, please use the **no bgp confederation identifier** command.

Syntax

bgp confederation identifier *as*
no bgp confederation identifier

Parameter

as: The confederation ID of the route reflector, ranging from 1 to 4294967295.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the confederation ID to 1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp confederation identifier 1
```

48.23 bgp confederation peers

Description

This command is used to configure a sub-AS belonging to the confederation. To disable this configuration, please use the **no bgp confederation peers** command.

Syntax

bgp confederation peers *as*

no bgp confederation peers

Parameter

as: The sub-AS number of the confederation, ranging from 1 to 4294967295.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the sub-AS belonging to the confederation to 1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp confederation peers 1
```

48.24 bgp dampening

Description

This command is used to configure route dampening. To disable this configuration, please use the **no bgp dampening** command.

Syntax

bgp dampening *half-life reuse suppress max-suppress-time*
no bgp dampening

Parameter

half-life: half-life: The time it takes for the penalty value to be halved. The range is 1-45 minutes, and the default value is 15.

reuse: The value at which the oscillating route can be reused. The range is 1-20000, and the default value is 750.

suppress: The value at which the oscillating route is suppressed. The range is 1-20000, and the default value is 2000.

max-suppress-time: The maximum duration of route suppression. The range is 1-255, and the default value is 4.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time required for the route attenuation penalty value to be halved to 30 minutes, the reuse value to 500, the suppression value to 500, and the maximum suppression duration to 10:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp dampening 30 500 500 10
```

48.25 bgp default ipv4-unicast

Description

This command is used to configure IPv4 unicast to be activated for neighbors by default. To disable this configuration, please use the **no bgp default ipv4-unicast** command.

Syntax

bgp default ipv4-unicast
no bgp default ipv4-unicast

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure IPv4 unicast to be activated for neighbors by default:

```
Switch(config)#router bgp 100
Switch(config-router)#bgp default ipv4-unicast
```

48.26 bgp default local-preference

Description

This command is used to configure the local preference. To disable this configuration, please use the **no bgp default local-preference** command.

Syntax

bgp bgp default local-preference *preference*
no bgp default local-preference

Parameter

preference: Local preference, ranging from 0 to 4294967295, and the default value is 100.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the local preference to 200:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp default local-preference 200
```

48.27 bgp deterministic-med

Description

This command is used to configure BGP to select the path with the best MED from the paths advertised from the adjacent AS. To disable this configuration, please use the **no bgp deterministic-med** command.

Syntax

```
bgp deterministic-med
no bgp deterministic-med
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to select the path with the best MED from the paths advertised from the adjacent AS:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp deterministic-med
```

48.28 bgp

disable-ebgp-connected-route-check

Description

This command is used to disable the connected route check for EBGp peers. By default, EBGp requires a direct connection to establish a peer relationship. After enabling this feature, EBGp peers can be established even without a direct connection. To disable this function, please use the **no bgp disable-ebgp-connected-route-check** command.

Syntax

```
bgp disable-ebgp-connected-route-check
no bgp disable-ebgp-connected-route-check
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to establish EBGp peers in a non-directly-connected scenario

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp disable-ebgp-connected-route-check
```

48.29 bgp fast-external-failover

Description

This command is used to configure BGP to reset the session immediately after the directly connected external neighbor is disconnected. To disable this configuration, please use the **no bgp fast-external-failover** command.

Syntax

```
bgp fast-external-failover
```

no bgp fast-external-failover

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to reset the session immediately after the directly connected external neighbor is disconnected:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp fast-external-failover
```

48.30 bgp graceful-restart

Description

This command is used to configure graceful restart of BGP, which applies to both the global BGP instance and private VRF BGP instances. To cancel the configuration, use the **no bgp graceful-restart** command.

Syntax

bgp graceful-restart

no bgp graceful-restart

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the graceful restart of the BGP:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp graceful-restart
```

48.31 bgp graceful-restart restart-time

Description

This command is used to configure the maximum wait time that neighbor devices will allow for the local device to restart and re-establish BGP sessions during a BGP Graceful Restart event. This configuration applies to both the global BGP instance and private VRF BGP instances. To cancel the configuration, use the **no bgp graceful-restart restart-time** command.

Syntax

```
bgp graceful-restart restart-time time
```

```
no bgp graceful-restart restart-time
```

Parameter

time: The maximum wait time for the local BGP neighbor to establish successfully during a graceful restart, ranging from 1 to 4095 seconds, and the default value is 120 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum wait time for neighbors to re-establish BGP sessions as 240 seconds during a Graceful Restart:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#bgp graceful-restart restart-time 240
```

48.32 bgp graceful-restart rib-stale-time

Description

This command is used to configure the maximum time for which the local Routing Information Base (RIB) retains stale routes during a local BGP Graceful Restart event. This configuration applies to both the global BGP instance and private VRF BGP instances. To cancel the configuration, use the **no bgp graceful-restart rib-stale-time** command.

Syntax

bgp graceful-restart rib-stale-time *time*
no bgp graceful-restart rib-stale-time

Parameter

time: The maximum duration to retain stale BGP routing information during a graceful restart, ranging from 1-3600 seconds, and the default value is 120 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum time for the local RIB to retain stale routes as 240 seconds during a Graceful Restart:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp graceful-restart rib-stale-time 240
```

48.33 bgp graceful-restart select-defer-time

Description

This command is used to configure the delay time before executing the route selection algorithm to update the local routing table after the local BGP device has performed a Graceful Restart and re-established its connections.

This configuration applies to both the global BGP instance and private VRF BGP instances. To cancel the configuration, use the **no bgp graceful-restart select-defer-time** command.

Syntax

bgp graceful-restart select-defer-time *time*
no bgp graceful-restart select-defer-time

Parameter

time: The time neighbor routers wait after receiving updated routing information from the restarting router before performing route selection, ranging from 0-3600 seconds, and the default value is 90 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the delay time for executing the route selection algorithm as 240 seconds after a Graceful Restart:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp graceful-restart select-defer-time 240
```

48.34 bgp graceful-restart stalepath-time

Description

This command is used to configure the maximum time for which the local router will retain routes learned from a neighbor when that neighbor experiences a control-plane failure (e.g., a BGP process restart). This configuration applies to both the global BGP instance and private VRF BGP instances. To cancel the configuration, use the **no bgp graceful-restart stalepath-time** command.

Syntax

bgp graceful-restart stalepath-time *time*
no bgp graceful-restart stalepath-time

Parameter

time: The maximum duration to retain stale BGP path information during a graceful restart, ranging from 1 to 4095 seconds, and the default value is 120 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum time for the local router to retain routes learned from a neighbor as 240 seconds when the neighbor has a control-plane failure:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp graceful-restart stalepath-time 240
```

48.35 bgp graceful-shutdown

Description

This command is used to enable the BGP Graceful Shutdown function. To disable this function, use the **no bgp graceful-shutdown** command.

Syntax

```
bgp graceful-shutdown  
no bgp graceful-shutdown
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BGP Graceful Shutdown function:

```
Switch(config)#router bgp 100
```



```
Switch(config-router)# bgp graceful-shutdown
```

48.36 bgp listen limit

Description

This command is used to configure the maximum number of dynamic BGP neighbor sessions that can be established. This configuration applies to both the global BGP instance and private VRF BGP instances. To cancel the configuration, use the **no bgp listen limit** command.

Syntax

```
bgp listen limit num  
no bgp listen limit
```

Parameter

num: The maximum number. The range is 1 to 256. The default value is 100.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of dynamic BGP neighbor sessions as 10:

```
Switch(config)#router bgp 100  
Switch(config-router)# bgp listen limit 10
```

48.37 bgp listen range

Description

This command is used to configure a listening range for BGP dynamic neighbors and add the dynamically established neighbors to a specified peer group. This configuration applies to both the global BGP instance and private VRF BGP instances. To disable this configuration, please use the **no bgp listen range** command.

Syntax

```
bgp listen range address Neighbor tag  
no bgp listen range address Neighbor tag
```

Parameter

address: The network range to listen on.

name: Peer group name.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a listening range for dynamic BGP neighbors as the 1.1.1.0/24 subnet and add them to the peer group named "aaa":

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp listen range 1.1.1.0/24 peer-group aaa
```

48.38 bgp log-neighbor-changes

Description

This command is used to enable logging for BGP neighbor state changes. This configuration applies to both the global BGP instance and private VRF BGP instances. To disable this function, please use the **no bgp log-neighbor-changes** command.

Syntax

bgp log-neighbor-changes

no bgp log-neighbor-changes

Parameter

None.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable logging for BGP neighbor state changes:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp log-neighbor-changes
```

48.39 bgp max-med administrative

Description

This command is used to configure the MED value for BGP routes advertised by this device. To disable this function, please use the **no bgp max-med administrative** command.

Syntax

```
bgp max-med administrative [med]
```

```
no bgp max-med administrative
```

Parameter

med: MED value.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MED value for BGP routes advertised by this device as 200:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp max-med administrative 200
```

48.40 bgp max-med on-startup

Description

This command is used to configure the MED value for BGP routes advertised by this device for a specified period after BGP startup. The MED reverts to its default value after this timer expires. To disable this function, please use the **no bgp max-med on-startup** command.

Syntax

```
bgp max-med on-startup time [med]
```

no bgp max-med on-startup

Parameter

Time: The duration, in seconds. The range is 5 to 86400.

med: MED value.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MED value for BGP routes advertised by this device as 200 for the first 5 seconds after BGP startup::

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# bgp max-med on-startup 5 200
```

48.41 bgp network import-check

Description

This command is used to configure BGP to check the reachability of the routes configured by the network command. To disable this configuration, please use the **no bgp network import-check** command.

Syntax

bgp network import-check

no bgp network import-check

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to check the reachability of the routes configured by the network command:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp network import-check
```

48.42 bgp reject-as-sets

Description

This command is used to configure BGP to filter out routes that contain the AS_SET or AS_CONFED_SET attributes. To disable this function, use the **no bgp reject-as-sets** command.

Syntax

```
bgp reject-as-sets
no bgp reject-as-sets
```

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to filter out routes containing the AS_SET or AS_CONFED_SET attributes:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp reject-as-sets
```

48.43 bgp router-id

Description

This command is used to set the router ID. If you do not manually configure the router ID, or cancel the configured router ID, BGP will automatically select an interface IP address as the router ID. To delete the router ID, please use the **no bgp router-id** command.

Syntax

bgp router-id *router-id*
no bgp router-id

Parameter

router-id: Router ID, which is a 32-bit unsigned integer in dotted decimal format, excluding 0.0.0.0. To avoid multiple routers using the same router ID during automatic election, it is recommended to configure this manually.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the BGP route ID to 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# bgp router-id 1.1.1.1
```

48.44 no neighbor

Description

This command is used to delete a specified BGP neighbor and all its associated configurations.

Syntax

no neighbor *ip-address*

Parameter

ip-address: Neighbor IP address.

Command Mode

Router Configuration Mode

BGP VRF Address Family Configuration Mode (config-router-vrf-af). Note that the configuration takes effect for all address families under the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete the global BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# no neighbor 1.1.1.1
```

Delete the BGP neighbor 1.1.1.1 for the private VRF named "a":

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch (config-router-vrf-af)# no neighbor 1.1.1.1
```

48.45 neighbor activate

Description

This command is used to configure BGP to enable the address family for the neighbor. To disable this configuration, please use the **no neighbor activate** command.

Syntax

```
neighbor ip-address / tag activate
no neighbor ip-address / tag activate
```

Parameter

ip-address. Neighbor IP address.

tag. Neighbor tag.

Command Mode

Router Configuration Mode. Note: Configuration in this mode takes effect in the IPv4 unicast address family context.

BGP Address Family Configuration Mode (config-router-af)

BGP VRF Address Family Configuration Mode (config-router-vrf-af)

BGP L2VPN EVPN Address Family Configuration Mode (address-family l2vpn evpn)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IPv4 unicast address family for global BGP neighbor 1.1.1.1 in router configuration mode:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 activate
```

Enable the IPv4 unicast address family for global BGP neighbor 1.1.1.1 in address family configuration mode:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 unicast
```

```
Switch (config-router-af)# neighbor 1.1.1.1 activate
```

Enable the IPv4 unicast address family for BGP neighbor 1.1.1.1 in VRF "a":

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch (config-router-af)# neighbor 1.1.1.1 activate
```

Enable the L2VPN EVPN address family for global BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family l2vpn evpn
```

```
Switch (config-router-af)# neighbor 1.1.1.1 activate
```

48.46 neighbor

addpath-tx-all-paths

Description

This command is used to allow the gateway to advertise all learned feasible paths to a specified neighbor. To disable this configuration, please use the **no neighbor addpath-tx-all-paths** command.

Syntax

```
neighbor ip-address / tag addpath-tx-all-paths
```

```
no neighbor ip-address / tag addpath-tx-all-paths
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

BGP Address Family Configuration Mode (config-router-af)

BGP VRF Address Family Configuration Mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Allow the global BGP IPv4 address family to send all learned feasible paths to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 unicast
```

```
Switch (config-router-af)# neighbor 1.1.1.1 addpath-tx-all-paths
```

Allow the private VRF "a" BGP IPv4 address family to send all learned feasible paths to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch (config-router-vrf-af)# neighbor 1.1.1.1 addpath-tx-all-paths
```

48.47 neighbor addpath-tx-bestpath-per-AS

Description

This command is used to allow the gateway to advertise one best path per AS to a specified neighbor. To disable this configuration, please use the **no neighbor addpath-tx-bestpath-per-AS** command.

Syntax

```
neighbor ip-address / tag addpath-tx-bestpath-per-AS
```

```
no neighbor ip-address / tag addpath-tx-bestpath-per-AS
```

Parameter

ip-address: Neighbor IP address.

tag. Neighbor tag.

Command Mode

BGP Address Family Configuration Mode (config-router-af)

BGP VRF Address Family Configuration Mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Allow the global BGP IPv4 address family to advertise one best path per AS to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch (config-router-af)# neighbor 1.1.1.1 addpath-tx-bestpath-per-AS
```

Allow the private VRF "a" BGP IPv4 address family to advertise one best path per AS to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch (config-router-vrf-af)# neighbor 1.1.1.1
addpath-tx-bestpath-per-AS
```

48.48 neighbor advertisement-interval

Description

This command is used to configure the minimum interval for advertising BGP route updates. To disable this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag advertisement-interval interval
no neighbor ip-address / tag advertisement-interval
```

Parameter

ip-address. Neighbor IP address.

tag. Neighbor tag.

interval: The minimum interval for advertising BGP routing updates, ranging from 0-600 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to advertise BGP routing updates for neighbor 1.1.1.1 at a minimum interval of 10 seconds:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 advertisement-interval 10
```

48.49 neighbor allowas-in

Description

This command is used to configure the maximum number of ASs in the AS path sent by the neighbor, including its own AS. To disable this configuration, please use the no command.

Syntax

neighbor *ip-address / tag* **allowas-in** *number*

no neighbor *ip-address / tag* **allowas-in**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

number: AS number, ranging from 1 to 10.

Command Mode

Router Configuration Mode. Note: Configuration in this mode takes effect in the IPv4 unicast address family context.

BGP Address Family Configuration Mode (config-router-af)

BGP VRF Address Family Configuration Mode (config-router-vrf-af)

BGP L2VPN EVPN Address Family Configuration Mode (address-family l2vpn evpn)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the global BGP IPv4 address family to accept routes from neighbor 1.1.1.1 even if the AS_PATH contains the local AS, allowing the local AS to appear up to 10 times:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 allowas-in 10
```

Configure the global BGP IPv4 address family to accept routes from neighbor 1.1.1.1 even if the AS_PATH contains the local AS, allowing the local AS to appear up to 10 times (in address family mode):

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 1.1.1.1 allowas-in 10
```

Configure the private VRF "a" BGP IPv4 address family to accept routes from neighbor 1.1.1.1 even if the AS_PATH contains the local AS, allowing the local AS to appear up to 10 times:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 allowas-in 10
```

Configure the global BGP L2VPN EVPN address family to accept routes from neighbor 1.1.1.1 even if the AS_PATH contains the local AS, allowing the local AS to appear up to 10 times:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family l2vpn evpn
Switch (config-router-af)# neighbor 1.1.1.1 allowas-in 10
```

48.50 neighbor as-override

Description

This command is used to allow the local device to override the original AS number in received routes with its local AS number when advertising those routes. To disable this configuration, please use the **no neighbor as-override** command.

Syntax

neighbor *ip-address* / *tag* **as-override**
no neighbor *ip-address* / *tag* **as-override**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

BGP Address Family Configuration Mode (config-router-af)

BGP VRF Address Family Configuration Mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Allow the global BGP instance to override the original AS number with the local AS number when advertising IPv4 address family routes to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch (config-router-af)# neighbor 1.1.1.1 as-override
```

Allow the private VRF "a" BGP instance to override the original AS number with the local AS number when advertising IPv4 address family routes to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch (config-router-vrf-af)# neighbor 1.1.1.1 as-override
```

48.51 neighbor attribute-unchanged

Description

This command is used to configure BGP attributes to be sent to neighbors without change. To disable this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **attribute-unchanged** [*as-path*] [*med*] [*next-hop*]
no neighbor *ip-address* / *tag* **attribute-unchanged**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

as-path: AS path attribute.

med: MED attribute.

next-hop: Next hop attribute.

Command Mode

Router Configuration Mode (router bgp): Note: Configuration in this mode takes effect in the IPv4 unicast address family context.

BGP Address Family Configuration Mode (config-router-af)

BGP VRF Address Family Configuration Mode (config-router-vrf-af)

BGP L2VPN EVPN Address Family Configuration Mode (address-family l2vpn evpn)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the global BGP IPv4 address family to send routes with the AS_PATH attribute unchanged to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 attribute-unchanged as-path
```

Configure the global BGP IPv4 address family to send routes with the AS_PATH attribute unchanged to neighbor 1.1.1.1 (in address family mode):

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 unicast
```

```
Switch (config-router-af)# neighbor 1.1.1.1 attribute-unchanged as-path
```

Configure the private VRF "a" BGP IPv4 address family to send routes with the AS_PATH attribute unchanged to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 attribute-unchanged  
as-path
```

Configure the global BGP L2VPN EVPN address family to send routes with the AS_PATH attribute unchanged to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family l2vpn evpn
```

```
Switch(config-router-af)# neighbor 1.1.1.1 attribute-unchanged as-path
```

48.52 neighbor bfd

Description

This command is used to BGP to use BFD for detecting link status with a neighbor. To disable this configuration, please use the **no neighbor bfd** command.

Syntax

```
neighbor ip-address / tag bfd [profile]
```

```
no neighbor ip-address / tag bfd
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

as-path: AS path attribute.

med: MED attribute.

profile: BFD profile name.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure BGP to use BFD to detect link status with neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 bfd
```

48.53 neighbor capability dynamic

Description

This command is used to announce dynamic capabilities to neighbors. To disable this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **capability dynamic**
no neighbor *ip-address* / *tag* **capability dynamic**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to dynamically advertise capabilities to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 capability dynamic
```

Configure private VRF 'a' BGP to dynamically advertise capabilities to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 capability dynamic
```


48.54 neighbor dampening

Description

This command is used to configure route flap dampening for a neighbor. To disable this configuration, please use the **no neighbor dampening** command.

Syntax

neighbor *ip-address* / *tag* **dampening** *half-life* *reuse* *suppress*
max-suppress-time

no neighbor *ip-address* / *tag* **dampening**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

half-life: Time required for the penalty value to halve, in the range of 1 to 45 minutes. Default is 15 minutes.

reuse: Threshold at which a flapping route can be reused, in the range of 1 to 20000. Default is 750.

suppress: Threshold at which a flapping route is suppressed, in the range of 1 to 20000. Default is 2000.

max-suppress-time: Maximum duration a route can be suppressed, in the range of 1 to 255. Default is 4 times the half-life.

Command Mode

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP neighbor 1.1.1.1 route dampening for the IPv4 address family with a half-life of 30 minutes, reuse limit of 500, suppress limit of 500, and maximum suppress time of 10 times the half-life:

```
Switch(config)# address-family ipv4 unicast
```

```
Switch(config-router-af)# neighbor 1.1.1.1 dampening 30 500 500 10
```

Configure private VRF 'a' BGP neighbor 1.1.1.1 route dampening for the IPv4 address family with a half-life of 30 minutes, reuse limit of 500, suppress limit of 500, and maximum suppress time of 10 times the half-life:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 dampening 30 500 500 10
```

48.55 neighbor default-originate

Description

This command is used to advertise a default route to a neighbor. To disable this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag default-originate
no neighbor ip-address / tag default-originate
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode (router bgp): Note: Configuration in this mode actually takes effect in the IPv4 unicast address family.

BGP Address Family Configuration Mode (config-router-af)

BGP VRF Address Family Configuration Mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to advertise an IPv4 address family default route to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 default-originate
```

Configure public BGP to advertise an IPv4 address family default route to neighbor 1.1.1.1 (within the address family):

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 unicast
Switch (config-router-af)# neighbor 1.1.1.1 default-originate
```

Configure private VRF a BGP to advertise an IPv4 address family default route to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 default-originate
```

48.56 neighbor description

Description

This command is used to configure the neighbor description. To delete the neighbor description, please use the no command.

Syntax

```
neighbor ip-address / tag description description
no neighbor ip-address / tag description
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

description: Neighbor description.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the description for public BGP neighbor 1.1.1.1 as internet:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 description internet
```

Configure the description for private VRF a BGP neighbor 1.1.1.1 as internet:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)#neighbor 1.1.1.1 description internet
```

48.57 neighbor

disable-connected-check

Description

This command is used to configure the use of loopback address for one-hop EBGP neighbors. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **disable-connected-check**
no neighbor *ip-address* / *tag* **disable-connected-check**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to disable the directly-connected check for the connection with neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 disable-connected-check
```

Configure private VRF a BGP to disable the directly-connected check for the connection with neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 disable-connected-check
```

48.58 neighbor

dont-capability-negotiate

Description

This command is used to disable the negotiation on capabilities with neighbors. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **dont-capability-negotiate**
no neighbor *ip-address* / *tag* **dont-capability-negotiate**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP not to perform capability negotiation with neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 dont-capability-negotiate
```

Configure private VRF a BGP not to perform capability negotiation with neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 dont-capability-negotiate
```

48.59 neighbor ebgp-multihop

Description

This command is used to allow establishing connections with EBGP neighbors that are not on a directly connected network. To cancel this configuration, please use the **no neighbor ebgp-multihop** command.

Syntax

```
neighbor ip-address / tag ebgp-multihop hops  
no neighbor ip-address / tag ebgp-multihop
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

hops: The maximum number of hops to reach an EBGP neighbor. The default value is 1, which means only directly connected neighbors are allowed.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to set the maximum hop count to neighbor 1.1.1.1 as 10:

```
Switch(config)#router bgp 100  
Switch(config-router)# neighbor 1.1.1.1 ebgp-multihop 10
```

Configure private VRF a BGP to set the maximum hop count to neighbor 1.1.1.1 as 10:

```
Switch(config)#router bgp 100  
Switch(config-router)# address-family ipv4 vrf a  
Switch(config-router-vrf-af)# neighbor 1.1.1.1 ebgp-multihop 10
```

48.60 neighbor enforce-first-as

Description

This command is used to configure strict validation that the first AS number in the AS_PATH attribute of route updates received from an EBGP neighbor must exactly match the locally configured neighbor AS number. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **enforce-first-as**
no neighbor *ip-address* / *tag* **enforce-first-as**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure neighbor 1.1.1.1 to enforce first AS validation:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 enforce-first-as
```

48.61 neighbor graceful-restart

Description

This command is used to configure the graceful restart of BGP neighbors. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **graceful-restart**
no neighbor *ip-address* / *tag* **graceful-restart**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP Graceful Restart capability for neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 graceful-restart
```

Configure private VRF a BGP Graceful Restart capability for neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 graceful-restart
```

48.62 neighbor graceful-restart-helper

Description

This command is used to configure BGP to gracefully restart neighbor routers. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **graceful-restart-helper**

no neighbor *ip-address* / *tag* **graceful-restart-helper**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP Graceful Restart helper capability for neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 graceful-restart-helper
```

Configure private VRF a BGP Graceful Restart helper capability for neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 graceful-restart-helper
```

48.63 neighbor local-as

Description

This command is used to prepend the specified local AS to the AS path when BGP sends or receives the AS path from the specified neighbor. This configuration applies to EBGp neighbors. To cancel this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag local-as as
```

```
no neighbor ip-address / tag local-as
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

as: The AS number to advertise externally.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the AS number that public BGP advertises itself as to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 local-as 5
```

Configure the AS number that private VRF a BGP advertises itself as to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 local-as 5
```

48.64 neighbor maximum-prefix

Description

This command is used to specify the maximum number of routes received from a specific neighbor. To cancel this configuration, please use the `no` command.

Syntax

neighbor *ip-address* / *tag* **maximum-prefix** *number*

no neighbor *ip-address* / *tag* **maximum-prefix**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

number: The maximum number of routes that can be received from this neighbor.

Command Mode

Router Configuration Mode. Note that configuration in this mode actually takes effect in the IPv4 unicast address family.

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to receive a maximum of 100 IPv4 address family routes from neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 maximum-prefix 100
```

Configure public BGP to receive a maximum of 100 IPv4 address family routes from neighbor 1.1.1.1 (within the address family context):

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 unicast
```

```
(config-router-af)# neighbor 1.1.1.1 maximum-prefix 100
```

Configure private VRF a BGP to receive a maximum of 100 IPv4 address family routes from neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 maximum-prefix 100
```

48.65 neighbor maximum-prefix-out

Description

This command is used to configure the maximum number of routes to be advertised to a neighbor. To cancel this configuration, please use the `no` command.

Syntax

```
neighbor ip-address / tag maximum-prefix-out limit
```

```
no neighbor ip-address / tag maximum-prefix-out
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Limit: Maximum number of route prefixes.

Command Mode

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP IPv4 address family to advertise a maximum of 1000 route prefixes to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 unicast
Switch(config-router-af)# neighbor 1.1.1.1 maximum-prefix-out 1000
```

Configure private VRF a BGP IPv4 address family to advertise a maximum of 1000 route prefixes to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf a
(config-router-vrf-af)# neighbor 1.1.1.1 maximum-prefix-out 1000
```

48.66 neighbor next-hop-self

Description

This command is used to modify the next-hop attribute of BGP routes advertised to a specified neighbor, replacing it with the local router's interface IP address. To cancel this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag next-hop-self [all]
no neighbor ip-address / tag next-hop-self [all]
```

Parameter

ip-address: Neighbor IP address.
tag: Neighbor tag.

Command Mode

Router Configuration Mode. Configuration in this mode actually takes effect in the IPv4 unicast address family.

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

BGP L2VPN EVPN address family configuration mode (address-family l2vpn evpn)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to use its own address as the next-hop for IPv4 address family routes sent to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 next-hop-self
```

Configure public BGP to use its own address as the next-hop for IPv4 address family routes sent to neighbor 1.1.1.1 (within the address family):

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 unicast
Switch (config-router-af)# neighbor 1.1.1.1 next-hop-self
```

Configure private VRF a BGP to use its own address as the next-hop for IPv4 address family routes sent to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf a
(config-router-vrf-af)# neighbor 1.1.1.1 next-hop-self
```

Configure public BGP to use its own address as the next-hop for L2VPN EVPN address family routes sent to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family l2vpn evpn
Switch(config-router-af)# neighbor 1.1.1.1 next-hop-self
```

48.67 neighbor nexthop-local unchanged

Description

This command is used to specify that the next-hop link-local address of BGP IPv6 routes advertised by a neighbor should not be changed. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* nexthop-local unchanged

no neighbor *ip-address* / *tag* nexthop-local unchanged

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

BGP IPv6 address family configuration mode (address-family ipv6 unicast

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to not change the next-hop link-local address for IPv6 address family routes sent to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family ipv6 unicast
```

```
Switch(config-router-af)# neighbor 1.1.1.1 nexthop-local unchanged
```

48.68 neighbor override-capability

Description

This command is used to ignore neighbor capability negotiation information and use the default capability information. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* override-capability

no neighbor *ip-address* / *tag* override-capability

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to ignore the capability negotiation result with neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 override-capability
```

Configure private VRF a BGP to ignore the capability negotiation result with neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 override-capability
```

48.69 neighbor passive

Description

This command is used to disable the OPEN message sent to the neighbor. To cancel this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag passive
no neighbor ip-address / tag passive
```

Parameter

ip-address: Neighbor IP address.
tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af). Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP not to actively send OPEN messages to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 passive
```

Configure private VRF a BGP not to actively send OPEN messages to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 passive
```

48.70 neighbor password

Description

This command is used to configure the neighbor password. To cancel this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag password password
no neighbor ip-address / tag password
```

Parameter

ip-address: Neighbor IP address.
tag: Neighbor tag.
password: Neighbor password.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the password for public BGP neighbor 1.1.1.1 as abc:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 password abc
```


48.71 neighbor peer-group

Description

This command is used to configure neighbors to join the specified neighbor group. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **Neighbor tag**
no neighbor *ip-address* / *tag* **peer-group**

Parameter

ip-address: Neighbor IP address.
tag: Neighbor tag.
name: Neighbor group name.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP neighbor 1.1.1.1 to join peer group abc:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 peer-group abc
```

Configure private VRF a BGP neighbor 1.1.1.1 to join peer group abc:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
(config-router-vrf-af)# neighbor 1.1.1.1 peer-group abc
```

48.72 neighbor port

Description

This command is used to configure the BGP port number of the neighbor. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* | *tag* **port** *port*
no neighbor *ip-address* | *tag* **port**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

port: TCP port number, ranging from 0-65535.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the BGP port number for neighbor 1.1.1.1 as 200:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 port 200
```

48.73 neighbor remote-as

Description

This command is used to configure BGP neighbors. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **remote-as** *as*
no neighbor *ip-address* / *tag* **remote-as**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

as: AS number of the neighbor.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a public BGP neighbor 1.1.1.1 located in AS 2:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 remote-as 2
```

Configure a private VRF a BGP neighbor 1.1.1.1 located in AS 2:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)#address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 remote-as 2
```

48.74 neighbor remove-private-AS

Description

This command is used to remove the private AS number from outbound updates. To cancel this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag remove-private-AS
```

```
no neighbor ip-address / tag remove-private-AS
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode. Configuration in this mode actually takes effect in the IPv4 unicast address family.

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to remove private AS numbers from IPv4 updates sent to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 remove-private-AS
```

Configure public BGP to remove private AS numbers from IPv4 updates sent to neighbor 1.1.1.1 (within the address family):

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 unicast
```

```
Switch(config-router-af)# neighbor 1.1.1.1 remove-private-AS
```

Configure private VRF a BGP to remove private AS numbers from IPv4 updates sent to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 remove-private-AS
```

48.75 neighbor route-reflector-client

Description

This command is used to configure a neighbor as a client of a route reflector. To cancel this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag route-reflector-client
```

```
no neighbor ip-address / tag route-reflector-client
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode. Configuration in this mode actually takes effect in the IPv4 unicast address family.

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

BGP L2VPN EVPN address family configuration mode (address-family l2vpn evpn)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP neighbor 1.1.1.1 as an IPv4 address family route reflector client:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 route-reflector-client
```

Configure public BGP neighbor 1.1.1.1 as an IPv4 address family route reflector client (within the address family):

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 1.1.1.1 route-reflector-client
```

Configure private VRF a BGP neighbor 1.1.1.1 as an IPv4 address family route reflector client:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)#neighbor 1.1.1.1 route-reflector-client
```

Configure public BGP neighbor 1.1.1.1 as an L2VPN EVPN address family route reflector client:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family l2vpn evpn
Switch(config-router-af)# neighbor 1.1.1.1 route-reflector-client
```

48.76 neighbor route-server-client

Description

This command is used to configure a neighbor as a route server client. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **route-server-client**
no neighbor *ip-address* / *tag* **route-server-client**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

BGP address family configuration mode (config-router-af)

BGP L2VPN EVPN address family configuration mode (address-family l2vpn evpn)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP neighbor 1.1.1.1 as an IPv4 address family route server client:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 1.1.1.1 route-server-client
```

Configure public BGP neighbor 1.1.1.1 as an L2VPN EVPN address family route server client:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family l2vpn evpn
Switch(config-router-af)# neighbor 1.1.1.1 route-server-client
```

48.77 neighbor sender-as-path-loop-detection

Description

This command is used to configure the enabling of sender AS_PATH loop detection, preventing the router from advertising a route containing the

neighbor's AS number to that same neighbor AS. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **sender-as-path-loop-detection**
no neighbor *ip-address* / *tag* **sender-as-path-loop-detection**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure sender AS_PATH loop detection for neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 sender-as-path-loop-detection
```

48.78 neighbor send-community

Description

This command is used to configure the permission to send the community attribute to a neighbor. To cancel this configuration, please use the no command.

Syntax

neighbor *ip-address* / *tag* **send-community**
no neighbor *ip-address* / *tag* **send-community**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP to allow sending the COMMUNITY attribute to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 1.1.1.1 send-community
```

Configure private VRF a BGP to allow sending the COMMUNITY attribute to neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 send-community
```

48.79 neighbor shutdown

Description

This command is used to manually shut down a neighbor. To cancel this configuration, please use the no command.

Syntax

```
neighbor ip-address / tag shutdown
no neighbor ip-address / tag shutdown
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Manually shut down public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 shutdown
```

Manually shut down private VRF a BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
(config-router-vrf-af)# neighbor 1.1.1.1 shutdown
```

48.80 neighbor soft-reconfiguration inbound

Description

This command is used to enable inbound soft reconfiguration on a BGP peer. Its main purpose is to allow the router to store all original updates received from the specified neighbor (including routes rejected by inbound route policies), so that inbound policies can be reapplied without requiring the neighbor to resend routing updates. To disable this feature, please use the `no` command.

Syntax

```
neighbor ip-address / tag soft-reconfiguration inbound  
no neighbor ip-address / tag soft-reconfiguration inbound
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

BGP L2VPN EVPN address family configuration mode (address-family l2vpn evpn)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable inbound soft reconfiguration for the IPv4 address family for public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 1.1.1.1 soft-reconfiguration inbound
```

Enable inbound soft reconfiguration for the IPv4 address family for private VRF a BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 soft-reconfiguration inbound
```

Enable inbound soft reconfiguration for the L2VPN EVPN address family for public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family l2vpn evpn
Switch(config-router-af)# neighbor 1.1.1.1 soft-reconfiguration inbound
```

48.81 neighbor strict-capability-match

Description

This command is used to strictly match the capability negotiation between neighbors. To disable this feature, please use the no command.

Syntax

```
neighbor ip-address / tag strict-capability-match
no neighbor ip-address / tag strict-capability-match
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enforce strict capability negotiation matching with public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 strict-capability-match
```

Enforce strict capability negotiation matching with private VRF a BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 strict-capability-match
```

48.82 neighbor timers

Description

This command is used to configure the interval for sending keepalive messages between neighbors and the neighbor hold time. To use to global configuration value, please use the **no neighbor timers** command.

Syntax

neighbor *ip-address* / *tag* **timers** *keepalive* *hold*

no neighbor *ip-address* / *tag* **timers**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

keepalive: The interval between for sending keepalive messages between neighbors, ranging from 1-65535 seconds. The default value is 60.

hold: Neighbor hold time, ranging from 1-65535 seconds. The default value is 180.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the keepalive interval to 10 seconds and hold time to 30 seconds for public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 timers 10 30
```

Set the keepalive interval to 10 seconds and hold time to 30 seconds for private VRF a BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 timers 10 30
```

48.83 neighbor timers connect

Description

This command is used to configure the interval of the neighbor reconnecting to the timer. To disable this feature, please use the no command.

Syntax

neighbor *ip-address* / *tag* **timers connect** *connect*

no neighbor *ip-address* / *tag* **timers connect**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

connect: Interval of the neighbor reconnecting to the timer.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the reconnection timer to 100 seconds for public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 timers connect 100
```

Configure the reconnection timer to 100 seconds for private VRF a BGP neighbor 1.1.1.1:

```
Switch(config)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 timers connect 100
```

48.84 neighbor tracking

Description

This command is used to configure neighbor tracking functionality, specifying the delay time for route updates when real-time detection indicates a neighbor state change. To disable this feature, please use the no command.

Syntax

```
neighbor ip-address / tag tracking [delay time ]
no neighbor ip-address / tag tracking
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

time: Delay time for route updates, in seconds (range 0-65535, default is 10 seconds).

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure link state tracking for neighbor 1.1.1.1 and specify a route update delay time of 100 seconds:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 tracking delay 100
```

48.85 neighbor ttl-security hops

Description

This command is used to configure the interval of the neighbor reconnecting to the timer. To disable this feature, please use the no command.

Syntax

```
neighbor ip-address / tag ttl-security hops hops
no neighbor ip-address / tag ttl-security hops
```

Parameter

ip-address: Neighbor IP address.
tag: Neighbor tag.
hops: Maximum hop count.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a maximum hop count of 10 for public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 ttl-security hops 10
```

Configure a maximum hop count of 10 for private VRF a BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 ttl-security hops 10
```

48.86 neighbor update-group converge

Description

This command is used to configure the synchronous convergence feature of a neighbor update group. After configuration, convergence is only considered complete after all neighbors within the group have finished their updates. To disable this feature, please use the no command.

Syntax

```
neighbor ip-address / tag update-group converge
no neighbor ip-address / tag update-group converge
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the synchronous convergence feature for the update group of public BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 update-group converge
```

Configure the synchronous convergence feature for the update group of private VRF a BGP neighbor 1.1.1.1:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 update-group converge
```

48.87 neighbor update-group independent

Description

This command is used to forcibly designate a neighbor as a separate update group, causing its route updates to be processed completely independently. To disable this feature, please use the no command.

Syntax

```
neighbor ip-address / tag update-group independent
no neighbor ip-address / tag update-group independent
```

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure public BGP neighbor 1.1.1.1 as a separate update group:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 update-group independent
```

Configure private VRF a BGP neighbor 1.1.1.1 as a separate update group:

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 vrf a
Switch(config-router-vrf-af)# neighbor 1.1.1.1 update-group independent
```


48.88 neighbor update-source

Description

This command is used to specify the source IP address used when establishing a BGP session. To disable this feature, please use the no command.

Syntax

neighbor *ip-address* / *tag* **update-source** *source*
no neighbor *ip-address* / *tag* **update-source**

Parameter

ip-address: Neighbor IP address.

tag: Neighbor tag.

source: Specify the IP address used as the source interface for route updates.

Command Mode

Router Configuration Mode

BGP VRF address family configuration mode (config-router-vrf-af): Note that the configuration applies to all address families in the VRF.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the source IP for establishing a BGP session with public BGP neighbor 1.1.1.1 as 2.2.2.2:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# neighbor 1.1.1.1 update-source 2.2.2.2
```

Configure the source IP for establishing a BGP session with private VRF a BGP neighbor 1.1.1.1 as 2.2.2.2:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
```

```
Switch(config-router-vrf-af)# neighbor 1.1.1.1 update-source 2.2.2.2
```

48.89 neighbor weight

Description

This command is used to set the default weight for routes from this neighbor.
To delete the weight, please use the no command.

Syntax

neighbor *ip-address* / *tag* **weight** *weight*
no neighbor *ip-address* / *tag* **weight**

Parameter

ip-address: Neighbor IP address.
tag: Neighbor tag.
weight: Default weight, ranging from 0-65535.

Command Mode

Router Configuration Mode. Configuration in this mode actually takes effect in the IPv4 unicast address family.

BGP address family configuration mode (config-router-af)

BGP VRF address family configuration mode (config-router-vrf-af)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the default weight for routes received from public BGP neighbor 1.1.1.1 as 10:

```
Switch(config)#router bgp 100
Switch(config-router)# neighbor 1.1.1.1 weight 10
```

Configure the default weight for routes received from public BGP neighbor 1.1.1.1 as 10 (within the address family):

```
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 1.1.1.1 weight 10
```

Configure the default weight for routes received from private VRF a BGP neighbor 1.1.1.1 as 10:

```
Switch(config)#router bgp 100
```

```
Switch(config-router)# address-family ipv4 vrf a
(config-router-vrf-af)# neighbor 1.1.1.1 weight 10
```

48.90 show ip bgp

Description

This command is used to view the BGP routing table.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] [ip-address/ ip-address/mask-len]
```

Parameter

vrfname: VRF name.

ip-address: Network segment to display.

ip-address/mask-len: The network segment IP address and mask length to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the BGP routing table for the network segment 2.2.2.0:

```
Switch#show ip bgp 2.2.2.0
```

48.91 show ip bgp attribute-info

Description

This command is used to view all BGP attribute information.

Syntax

```
show ip bgp attribute-info
```

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View all BGP attribute information:

```
Switch# show ip bgp attribute-info
```

48.92 show ip bgp cidr-only

Description

This command is used to view only routes with non-natural network masks.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] cidr-only
```

Parameter

vrfname: VRF name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View only routes with non-natural network masks:

```
Switch# show ip bgp cidr-only
```

48.93 show ip bgp dampening flap-statistics

Description

This command is used to view the statistics of route flap penalty.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] dampening flap-statistics
```

Parameter

vrfname: VRF name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the statistics of route flap penalty:

```
Switch# show ip bgp dampening flap-statistics
```

48.94 show ip bgp dampening dampened-paths

Description

This command is used to view the information about dampened paths due to flapping.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] dampening dampened-paths
```

Parameter

vrfname: VRF name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the information about dampened paths due to flapping:

```
Switch# show ip bgp dampening dampened-paths
```

48.95 show ip bgp dampening parameters

Description

This command is used to view the parameters related to route flapping.

Syntax

show ip bgp [vrf *vrfname*] [ipv4 | ipv6] dampening parameters

Parameter

vrfname: VRF name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the parameters related to route flapping:

```
Switch# show ip bgp dampening parameters
```

48.96 show ip bgp {ipv4 | ipv6 | l2vpn evpn} all

Description

This command is used to view the BGP routing table for the corresponding address family.

Syntax

show ip bgp {ipv4 | ipv6 | l2vpn evpn} all

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View all BGP IPv4 address family routing tables:

```
Switch# show ip bgp ipv4 all
```

48.97 show ip bgp l2vpn evpn rd

Description

This command is used to view the routing table for the corresponding BGP L2VPN EVPN RD.

Syntax

show ip bgp l2vpn evpn rd [*rd*|all]

Parameter

rd: ASN:NN or ipaddress:NN.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the routing tables for all BGP L2VPN EVPN RDs:

```
Switch# show ip bgp l2vpn evpn rd all
```

48.98 show ip bgp memory

Description

This command is used to view the BGP memory information.

Syntax

show ip bgp memory

Parameter

None,

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the BGP memory information.:

```
Switch# show ip bgp memory
```

48.99 show ip bgp neighbors

Description

This command is used to view the BGP neighbor information.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] neighbors ip-address
```

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the BGP neighbor information:

```
Switch# show ip bgp neighbors
```

48.100 show ip bgp neighbors advertised-routes

Description

This command is used to view the routing information advertised to neighbors.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] neighbors ip-address  
advertised-routes
```

```
show ip bgp [[2vpn evpn] neighbors ip-address advertised-routes
```

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the routing information advertised to neighbor 1.1.1.1:

```
Switch# show ip bgp neighbors 1.1.1.1 advertised-routes
```

48.101 show ip bgp neighbors bestpath-routes

Description

This command is used to view the best-path route information learned from a specified neighbor

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] neighbors ip-address bestpath-routes
```

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the best-path route information learned from neighbor 1.1.1.1:

```
Switch# show ip bgp neighbors 1.1.1.1 bestpath-routes
```

48.102 show ip bgp neighbors dampened-routes

Description

This command is used to view the dampened routes received from neighbors.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] neighbors ip-address  
dampened-routes
```

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the dampened routes received from neighbor 1.1.1.1:

```
Switch# show ip bgp neighbors 1.1.1.1 dampened-routes
```

48.103 show ip bgp neighbors flap-statistics

Description

This command is used to view the flapping route information of a neighbor.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] neighbors ip-address flap-statistics
```

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

view the flapping route information of neighbor 1.1.1.1:

```
Switch# show ip bgp neighbors 1.1.1.1 flap-statistics
```

48.104 show ip bgp neighbors prefix-counts

Description

This command is used to view the detailed prefix counts of a neighbor.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] neighbors ip-address prefix-counts
```

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the detailed prefix counts of neighbor 1.1.1.1:

```
Switch# show ip bgp neighbors 1.1.1.1 prefix-counts
```

48.105 show ip bgp neighbors received-routes

Description

This command is used to view the routes received from neighbors.

Syntax

**show ip bgp [vrf *vrfname*] [ipv4 | ipv6] neighbors *ip-address*
received-routes**

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the routes received from neighbor 1.1.1.1:

```
Switch# show ip bgp neighbors 1.1.1.1 received-routes
```

48.106 show ip bgp neighbors routes

Description

This command is used to view the routes learned from neighbors.

Syntax

show ip bgp [vrf *vrfname*] [ipv4 | ipv6] neighbors *ip-address* routes

Parameter

vrfname: VRF name.

ip-address: Neighbor IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the routes learned from neighbor 1.1.1.1:

```
Switch# show ip bgp neighbors 1.1.1.1 routes
```

48.107 show ip bgp nexthop

Description

This command is used to view the next hop information.

Syntax

show ip bgp nexthop *ip-address*

Parameter

ip-address: Network segment to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the BGP next hop information:

```
Switch# show ip bgp nexthop
```

48.108 show ip bgp peer-group

Description

This command is used to view the peer group information.

Syntax

show ip bgp [**vrf** *vrfname*] **peer-group** [*name*]

Parameter

vrfname: VRF name.

name: Peer group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the BGP peer group information:

```
Switch# show ip bgp peer group
```

48.109 show ip bgp statistics

Description

This command is used to view the route prefix statistical information for the corresponding BGP address family.

Syntax

```
show ip bgp {[vrf vrfname] [ipv4 | ipv6]} statistics
```

```
show ip bgp l2vpn evpn statistics
```

Parameter

vrfname: VRF name.

name: Peer group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the route prefix statistical information for all BGP IPv4 address families:

```
Switch# show ip bgp ipv4 statistics
```

48.110 show ip bgp statistics-all

Description

This command is used to view the route prefix statistical count information for all address families.

Syntax

```
show ip bgp statistics-all
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the route prefix statistical count information for all address families::

```
Switch# show ip bgp statistics-all
```

48.111 show ip bgp summary

Description

This command is used to view the summary of BGP neighbors.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] summary [established | falied]  
[neighbor ip-address | remote-as as]
```

Parameter

vrfname: VRF name.

as: as——AS number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the summary of BGP neighbors:

```
Switch# show ip bgp summary
```

48.112 show ip bgp update-groups

Description

This command is used to view the BGP update group information.

Syntax

```
show ip bgp [vrf vrfname] [ipv4 | ipv6] update-groups [group-id]  
show ip bgp l2vpn evpn update-groups [group-id]
```

Parameter

vrfname: VRF name.

group-id: as—— Update group ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the BGP update group information:

```
Switch# show ip bgp update-groups
```

48.113 show ip bgp vrfs

Description

This command is used to view the information for all BGP VRF instances.

Syntax

```
show ip bgp vrfs
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the information for all BGP VRF instances:

```
Switch# show ip bgp vrfs
```

48.114 clear ip bgp

Description

This command is used to reset BGP neighbors.

Syntax

```
clear ip bgp [vrf vrfname] as  
clear ip bgp [vrf vrfname] ip-address
```

Parameter

vrfname: VRF name.
as: AS number of the neighbor.
ip-address: Neighbor's IP.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Reset BGP neighbor 1.1.1.1:

```
Switch# clear ip bgp 1.1.1.1
```

48.115 clear ip bgp all

Description

This command is used to reset all BGP neighbors.

Syntax

```
clear ip bgp [vrf vrfname] all
```

Parameter

vrfname: VRF name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Reset all BGP neighbors:

```
Switch# clear ip bgp all
```

48.116 clear ip bgp dampening

Description

This command is used to reset BGP route dampening.

Syntax

clear ip bgp dampening *ip-address* [mask]

Parameter

ip-address: Network segment IP address.

mask: Network segment mask.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Reset route dampening for network segment 1.1.1.0/24:

```
Switch# clear ip bgp dampening 1.1.1.0 255.255.255.0
```

48.117 clear ip bgp external

Description

This command is used to reset reset all EBGp neighbors.

Syntax

clear ip bgp [*vrf vrfname*] **external**

Parameter

vrfname: VRF name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Reset all EBGp neighbors:

```
Switch# clear ip bgp external
```

48.118 clear ip bgp peer-group

Description

This command is used to reset a specified BGP peer group.

Syntax

```
clear ip bgp [vrf vrfname] peer-group name
```

Parameter

vrfname: VRF name.

name: Peer group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Reset all neighbors within BGP peer group a:

```
Switch# clear ip bgp peer-group a
```

Privileged EXEC Mode and Any Configuration Mode

Chapter 49 L2VPN Configuration Commands (Only for Certain Devices)

VPWS (Virtual Private Wire Service) is a point-to-point Layer 2 Virtual Private Network (L2VPN) technology. By establishing a logical connection between two Customer Edge (CE) devices, it enables communication similar to a traditional leased line connection.

VPLS (Virtual Private LAN Service) is a Layer 2 Virtual Private Network (L2VPN) solution based on MPLS and Ethernet technologies. It is designed to simulate a local area network (LAN) over a wide area network (WAN) environment. Unlike the point-to-point communication of VPWS, VPLS provides point-to-multipoint communication.

In a VPLS network, the PE device learns source MAC addresses while forwarding packets to establish a MAC address forwarding table. This maps MAC addresses to user-side Access Circuits (AC interfaces) and Pseudo Wires (PW). VPLS uses VSI instances to differentiate between forwarding domains, requiring MAC address table management based on these VSI instances.

49.1 xconnect vc-id

Description

This command is used to create a VPWS connection under an interface and bind it to that interface. The no version of this command is used to delete the configuration information and cancel the configured VPWS connection on the device. When creating a VPWS connection, label values can be manually assigned or dynamically negotiated using the LDP protocol.

Syntax

```
xconnect vc-id peer peer-ip [in-label in-label out-label out-label]  
raw/tagged  
no xconnect
```

Parameter

vc-id—— The index value of the VPWS connection, an integer ranging from <1-4294967295>.

peer-ip—— The IP address of the peer device for the VPWS connection, in dotted-decimal format.

in-label—— The value of the incoming label for the VPWS connection on this device, an integer ranging from <16-1024>.

out-label—— The value of the outgoing label for the VPWS connection on this device, an integer ranging from <16-1048575>.

raw—— The encapsulation mode of the VPWS connection is Ethernet.

tagged—— The encapsulation mode of the VPWS connection is VLAN.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a VPWS connection under the Interface VLAN 10:

```
Switch(config)# interface vlan10
```

```
Switch(config-if)# xconnect 10 peer 2.2.2.2 in-label 30 out-label 40 raw
```

49.2 show mpls vc

Description

This command is used to display the forwarding information and status information of the VPWS connections already created on the device.

Syntax

```
show mpls vc [ statistics | vc-id ]
```

Parameter

statistics—— Displays statistical information for VPWS connections.

vc-id—— The index value of the VPWS connection, used to display specific information for the corresponding connection.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

The device displays the specific information for VPWS connection 10:

```
Switch(config)# show mpls vc 10
```

49.3 vsi name vsi-id vpls-id

Description

This command is used to create a VSI (Virtual Switch Instance) for VPLS forwarding. The no version of this command is used to delete the configuration and cancel the configured VSI instance.

Syntax

vsi *vpls-name* **vsi-id** *vpls-id*
no vsi *vpls-name* **vsi-id** *vpls-id*

Parameter

vsi-name—— The name of the VSI instance being created, in string format, with a length range of <1-32>.

vpls-id—— The index of the VSI instance being created, in integer format, with a range of <1-4294967295>.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a VSI instance named a1 with a vsi-id of 200:

```
Switch(config)# vsi a1 vsi-id 200
```

49.4 description

Description

This command is used to configure a description for the VSI instance. The no version is used to delete the description.

Syntax

description *vpls-description*

Parameter

vpls-description—— Description information for the VSI instance, string format, length <1-32>.

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VSI instance a1 and add a description:

```
Switch(config)# vsi a1 vsi-id 200
Switch(l2vpn-vpls)# description instance
```

49.5 signaling

Description

This command is used to configure the signaling protocol for the VSI instance. Signaling protocols are used to negotiate label values; by default, no protocol is used (static labels).

Syntax

signaling [ldp | static]

Parameter

ldp —— Sets the signaling protocol to LDP.

static —— Configures the instance to use no signaling protocol (static).

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the signaling protocol of VSI instance a1 to LDP:

```
Switch(config)# vsi a1 vsi-id 200
```

49.6 encapsulation

Description

This command is used to configure the encapsulation mode (Ethernet or VLAN) for the VSI instance. This applies to every VPLS connection in the instance unless overridden by specific connection settings.

Syntax

encapsulation [raw | tagged]

no encapsulation

Parameter

raw — Sets the encapsulation mode to Ethernet.

tagged — Sets the encapsulation mode to VLAN.

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the encapsulation mode of VSI instance a1 to VLAN:

```
Switch(config)# vsi a1 vsi-id 200
```

```
Switch(l2vpn-vpls)# encapsulation tagged
```

49.7 peer

Description

This command is used to create a VPLS connection under a VSI instance.

When creating a VPLS connection, you can manually specify static label values or rely on signaling protocols for dynamic negotiation. Note that dynamic negotiation depends on the signaling protocol configured for the VSI instance.

The default encapsulation mode is tagged. If no specific encapsulation is configured for the connection, it adopts the global configuration of the VSI

instance. However, a specific connection-level configuration will override the global setting.

Two types of VPLS connections can be created (Mesh peer is the default):

- Mesh peer: Used for full-mesh connectivity between devices and features split horizon functionality.
- Spoke peer: Used for connecting to a single device without split horizon; suitable for H-VPLS services.

The `no` version of this command deletes the configuration and cancels the existing VPLS connection.

Syntax

```
peer peer-ip [encapsulation raw | tagged] [in-label in-label out-label out-label] [spoke]  
no peer peer-ip
```

Parameter

peer-ip—— The IP address of the VPLS peer, in dotted-decimal format.

in-label—— The incoming label value for this device, an integer ranging from <16-1024>.

out-label—— The outgoing label value for this device, an integer ranging from <16-1048575>.

raw—— Sets the encapsulation mode to Ethernet.

tagged—— Sets the encapsulation mode to VLAN.

spoke—— Designates the connection as a spoke type.

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VSI instance a1, and configure a mesh peer with peer IP 3.3.3.3, in-label 120, out-label 220, and raw encapsulation:

```
Switch(config)# vsi a1 vsi-id 200  
Switch(l2vpn-vpls)# peer 3.3.3.3 encapsulation raw in-label 120 out-label 220
```

49.8 shutdown

Description

This command is used to disable forwarding for all VPLS connections under the VSI instance. Use `no shutdown` to re-enable forwarding.

Syntax

shutdown
no shutdown

Parameter

None.

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable forwarding for VSI instance a1:

```
Switch(config)# vsi a1 vsi-id 200
Switch(l2vpn-vpls)# shutdown
```

49.9 show vpls

Description

This command is used to display the information of VSI instances created on the device, including the VPLS connection forwarding information and status information under the VSI instance.

Syntax

show vpls name *vpls-name* [*peer*] **spoke** *spoke-peer*]

Parameter

vpls-name — The name of the VSI instance, in string format, with a length range of <1-32>.

peer — The IP address of the mesh peer connection's remote end, in dotted-decimal format; used to filter mesh peer information.

spoke peer—— The IP address of the spoke peer connection's remote end, in dotted-decimal format; used to filter spoke peer information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

The device displays all information under VSI instance a1:

```
Switch(config)# show vpls name a1
```

49.10 mac learning

Description

This command is used to control the MAC address learning function of a VSI instance. MAC learning is enabled for VSI by default. The no version of this command is used to delete the configuration and disable MAC address learning for the VSI.

Syntax

mac learning
no mac learning

Parameter

None.

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VSI instance a1 and enable its MAC address learning function:

```
Switch(config)# vsi a1 vsi-id 10
```

```
Switch(l2vpn-vpls)# mac learning
```

49.11 mac aging-time

Description

This command is used to configure the aging time for dynamic MAC addresses learned by the VSI instance. If the aging time is set to 0, the addresses will never age out. The no version deletes the configuration and restores the aging time to the default value.

Syntax

mac aging-time *aging-time*

no mac aging-time

Parameter

aging-time — The MAC address aging time, in integer format. The default value is 300s, with a range of <0 | 10-63000 >

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VSI instance a1 and set the MAC address aging time to 400s:

```
Switch(config)# vsi a1 vsi-id 10
```

```
Switch(l2vpn-vpls)# mac aging time 400
```

49.12 mac security

Description

This command is used to configure security functions for MAC address learning in a VSI instance, including the maximum number of learned MAC addresses and the handling behavior for packets with unknown source MAC addresses once the limit is reached. The no version restores settings to default.

Syntax

mac security max-learn *max-learn*

mac security drop

no mac security max-learn
no mac security drop
no mac security

Parameter

max-learn—— The maximum number of learned MAC addresses, in integer format. Default is 1000, range <0-2000>.

drop—— Drops packets with unknown source MAC addresses after the learning limit is reached. The default behavior is to forward them.

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VSI instance a1, set the learning limit to 300, and enable the MAC drop function:

```
Switch(config)# vsi a1 vsi-id 10
Switch(l2vpn-vpls)# mac security max-learn 300
Switch(l2vpn-vpls)# mac security drop
```

49.13 mac filtering

Description

This command is used to configure blackhole MAC addresses for a VSI instance. Packets with source MAC addresses matching the blackhole addresses will be filtered (dropped). The no version removes the blackhole MAC address configuration.

Syntax

mac filtering *mac-addr*
no mac filtering [*mac-addr*]

Parameter

mac-addr—— The blackhole MAC address, formatted as colon-separated hexadecimal.

Command Mode

VPLS Instance Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VSI instance a1 and configure blackhole MAC address 10:7C:61:B1:2F:6B:

```
Switch(config)# vsi a1 vsi-id 10
Switch(l2vpn-vpls)# mac filtering 10:7C:61:B1:2F:6B
```

49.14 mac static

Description

This command is used to configure the static MAC addresses for a VSI instance. Static MAC addresses are categorized into two types:

This command is used to configure static MAC addresses for a VSI instance. Static MAC addresses are divided into two types:

- Static AC MAC: Bound to an AC interface.
- Static PW MAC: Bound to a remote PEER.

When a static MAC address conflicts with a dynamically learned one, the static entry overrides the dynamic one. The no version deletes the static MAC address entry.

Syntax

mac address-table static *mac-addr* **vsi** *vsi-id* **interface** *interface-type* *interface-num* [**vlan** *vlan-id*]

mac address-table static *mac-addr* **vsi** *vsi-id* **peer** *peer-ip*

no mac address-table static *mac-addr* **vsi** *vsi-id* **interface** *interface-type* *interface-num* [**vlan** *vlan-id*]

no mac address-table static *mac-addr* **vsi** *vsi-id* **peer** *peer-ip*

Parameter

mac-addr — The MAC address, formatted as colon-separated hexadecimal.

vsi-id — The index of the VSI instance, an integer ranging from <1-4294967295>.

interface-type—— The type of the interface.

interface-num—— The index of the interface.

vlan-id—— The VLAN ID, required if the interface is a vlanIf interface.

peer-ip—— The IP address of the VPLS peer, in dotted-decimal format.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure static MAC address 10:7C:61:B1:2F:6B, binding it to vlanIf 20 of VSI instance a1 and remote peer 3.3.3.3 of VSI instance a2:

```
Switch(config)# vsi a1 vsi-id 10
Switch(l2vpn-vpls)# exit
Switch(config)# vsi a2 vsi-id 20
Switch(l2vpn-vpls)# exit
Switch(config)# mac address-table static 10:7C:61:B1:2F:6B vsi 10
interface gigabitEthernet 1/0/11 vlan 20
Switch(config)# mac address-table static 10:7C:61:B1:2F:6B vsi 20 peer
3.3.3.3
```

Chapter 50 IS-IS Configuration Commands (Only for Certain Devices)

Intermediate System to Intermediate System (IS-IS) is a dynamic routing protocol proposed by ISO. Currently, IS-IS is also supported in TCP/IP environments. It is a widely used protocol in Interior Gateway Protocols (IGP).

IS-IS is a link-state protocol, and the core concept of its routing calculation is the Shortest Path First (SPF) algorithm.

50.1 router isis

Description

The **router isis** command is used to create an IS-IS instance and enter the Router configuration mode. When the command includes a VRF name, it means that the IS-IS instance belongs to the VRF instance. When the VRF parameter is not specified, the IS-IS instance belongs to the public network. To delete the IS-IS instance, please use the **no router isis** command. When the VRF parameter is not specified, the corresponding instance will be deleted according to the area-tag.

Syntax

```
router isis area-tag [vrf vrf-name]  
no router isis area-tag [vrf vrf-name]
```

Parameter

area-tag—— IS-IS instance name, used to identify an IS-IS instance on this switch.

vrf-name—— VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an ISIS instance aaa and add it to vrf1.

```
Switch(config)# router isis aaa vrf vrf1
```


50.2 area-password

Description

This command is used to enable the IS-IS Level-1 area authentication function. After the function is enabled, IS-IS will carry authentication information in the message exchange in the area and verify the authentication information. To disable this function, please use the **no area-password** command.

Syntax

area-password { **clear** | **md5** } { **0** | **7** } *text*
no area-password

Parameter

clear: Encrypt in plain text.

md5: Encrypt using md5 algorithm.

0: Enter plain text.

7: Enter in cipher text.

text: Password text

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure MD5 encrypted authentication for the IS-IS Level-1 area:

```
Switch(config-router)#area-password md5 0 tp-link
```

50.3 domain-password

Description

This command is used to enable the authentication function of the IS-IS Level-2 area. After enabling this function, IS-IS will carry authentication information in the message exchange in this area and verify the authentication information. To disable this function, please use the **no domain-password** command.

Syntax

domain-password { clear | md5 } { 0 | 7 } *text*
no domain-password

Parameter

clear: Encrypt in plain text.

md5: Encrypt using md5 algorithm.

0: Enter plain text.

7: Enter in cipher text.

text: Password text

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure MD5 encrypted authentication for the IS-IS Level-2 area:

```
Switch(config-router)#domain-password md5 0 tp-link
```

50.4 graceful-restart

Description

This command is used to enable the IS-IS Graceful Restart function. When enabled, IS-IS will send restart notification messages to neighboring routers before initiating a restart. During the restart process, IS-IS strives to preserve routing information to minimize impact on other devices in the network. To disable this function, please use the **no graceful-restart** command.

Syntax

graceful-restart
no graceful-restart
graceful-restart suppress-sa
no graceful-restart suppress-sa
graceful-restart t2-interval *t2-interval*
no graceful-restart t2-interval
graceful-restart t3-interval *t3-interval*
no graceful-restart t3-interval

Parameter

suppress-sa: Suppress partial advertisement information during the IS-IS graceful restart process.

t2-interval: The duration in IS-IS graceful restart during which the restarting router waits for neighboring routers to send CSNP (Complete Sequence Number PDU) to facilitate rapid database synchronization. The range is 30 to 1800 seconds, and the default value is 60 seconds.

T3-interval: The duration in IS-IS graceful restart during which the restarting router waits for neighboring routers to acknowledge its graceful restart. The range is 30 to 1800 seconds, and the default value is 300 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure graceful restart for IS-IS routes:

```
Switch(config-router)#graceful-restart
Switch(config-router)#graceful-restart suppress-sa
```

50.5 hostname

Description

This command is used to enable the dynamic host name function of IS-IS. After enabling this function, IS-IS will configure a dynamic host name for the IS-IS system on the local switch and notify the neighbor device through the LSP message. To disable this function, please use the **no hostname** command.

Syntax

```
hostname { name | dynamic }
no hostname
```

Parameter

name: Specified host name, in text form.

dynamic: Use dynamic host name, in this mode, the system configured host name will be obtained.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the dynamic host name function of IS-IS:

```
Switch(config-router)# hostname dynamic
```

50.6 is-type

Description

This command is used to set the IS area type, which is Level-1-2 by default. To restore the default configuration, please use the **no is-type** command.

Syntax

```
is-type { level-1 | level-1-2 | level-2-only }  
no is-type
```

Parameter

level-1: Set the IS-IS area type to Level-1

level-1-2: Set the IS-IS area types to Level-1 and Level-2
level-2-only: Set the IS-IS area type to Level-2

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS area type to Level-1:

```
Switch(config-router)# is-type level-1
```

50.7 log-adjacency-changes

Description

This command is used to enable S-IS to record events of adjacency state changes. To disable this function, please use the **no log-adjacency-changes** command.

Syntax

log-adjacency-changes
no log-adjacency-changes

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS area type to Level-1:

```
Switch(config-router)# log-adjacency-changes
```

50.8 lsp-gen-interval

Description

This command is used to configure the interval for generating LSPs. When the local network flaps, the IS-IS local LSP may be frequently refreshed, causing frequent IS-IS flapping. To restore the default configuration, please use the **no lsp-gen-interval** command.

Syntax

lsp-gen-interval *interval*
no lsp-gen-interval

Parameter

interval: The interval for generating LSPs, ranging from 1 to 120s. It is 30s by default.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the LSP generating interval to 10s:

```
Switch(config-router)# lsp-gen-interval 10
```

50.9 lsp-mtu

Description

This command is used to configure the maximum length of a self-generated LSP. To restore the default configuration, please use the **no lsp-mtu** command.

Syntax

lsp-mtu *size*
no lsp-mtu

Parameter

size: The maximum length of LSP, ranging from 512 to 4352 bytes. It is 1497 bytes by default.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the maximum length of LSP to 1024 bytes:

```
Switch(config-router)# lsp-mtu 1024
```

50.10 lsp-refresh-interval

Description

This command is used to configure the interval for refreshing the IS-IS LSP. To restore the default configuration, please use the **no lsp-refresh-interval** command.

Syntax

lsp-refresh-interval *interval* [level-1 | level-2]
no lsp-refresh-interval

Parameter

interval: The interval for refreshing the IS-IS LSP, ranging from 1 to 65535s. It is 900s by default.

level-1: LSP level-1 refresh interval

level-2: LSP level-2 refresh interval

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the LSP refresh interval to 100s:

```
Switch(config-router)# lsp-refresh-interval 100
```

50.11 max-lsp-lifetime

Description

This command is used to configure the maximum lifetime of an IS-IS LSP packet. To restore the default configuration, please use the **no max-lsp-lifetime** command.

Syntax

max-lsp-lifetime *time* [level-1 | level-2]
no max-lsp-lifetime

Parameter

time: The max lifetime of LSP, ranging from 350 to 65535s. It is 1200s by default.

level-1: LSP level-1 refresh interval

level-2: LSP level-2 refresh interval

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the maximum lifetime of an LSP to 1000s:

```
Switch(config-router)# max-lsp-lifetime 1000
```

50.12 metric-style

Description

This command is used to configure IS-IS metric style. To restore the default configuration, please use the **no metric-style** command.

Syntax

metric-style { narrow | transition | wide }

no metric-style

Parameter

narrow: Narrow mode. It is the default mode.

transition: Compatible mode, supporting both narrow and wide modes.

wide: Wide mode, mainly used for TE scenarios.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set IS-IS metric style to wide:

```
Switch(config-router)# metric-style wide
```

50.13 net

Description

This command is used to configure NET of IS-IS. To delete NET, please use the **no net** command.

Syntax

net *net-name*

no net *net-name*

Parameter

net-name: Network Entity Title, in the format of X..X.XXXX.XXXX.XXXX.00.

The first "X..X" is the IS-IS area address, the 12 "X"s in the middle are the switch's System ID, and the last "00" is the SEL.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure IS-IS NET as 10.0000.0000.0000.1111.00:

```
Switch(config-router)#net 10.0000.0000.0000.1111.00
```

50.14 purge-originator

Description

This command is used to enable the purge originator of IS-IS. To disable this function, please use the **no purge-originator** command.

Syntax

purge-originator

no purge-originator

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the purge originator of IS-IS:

```
Switch(config-router)#purge-originator
```

50.15 set-attached-bit

Description

This command is used to set the ATT bit of IS-IS LSP. By default, Level-1-2 devices will set the ATT bit according to the rules of IS-IS protocol. After this command is configured, the ATT bit will always be set in Level-1 LSP. To cancel the setting of ATT bit, please use the **no set-attached-bit** command.

Syntax

set-attached-bit

no set-attached-bit

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the ATT bit of IS-IS LSP:

```
Switch(config-router)#set-attached-bit
```

50.16 set-overload-bit

Description

This command is used to set the overload bit in IS-IS LSP. To cancel the overload bit setting, please use the **no set-overload-bit** command.

Syntax

set-overload-bit
no set-overload-bit

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the overload bit in IS-IS LSP:

```
Switch(config-router)#set-overload-bit
```

50.17 spf interval

Description

This command is used to configure the frequency of SPF calculations in IS-IS to balance network convergence speed and CPU load. To restore the default settings, please use the **no spf-interval** command.

Syntax

spf-interval *time*
no spf-interval

Parameter

time: The interval for SPF calculation. The range is 1 to 120 seconds, and the default value is 2 seconds

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the interval for SPF calculation to 5 seconds:

```
Switch(config-router)# spf-interval 5
```

50.18 topology

Description

This command is used to enable global IS-IS network multi-topology, allowing independent logical topologies to be created for different protocols or services. To disable this configuration, please use the **no topology** command.

Syntax

```
topology { ipv6-unicast } [ overload ]  
no topology { ipv6-unicast }
```

Parameter

ipv6-unicast: IS-IS enables IPv6 unicast topology.

overload: IS-IS enables topology to set overload bit.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure IS-IS multi-topology:

```
Switch(config-router)#topology ipv6-unicast overload
```

50.19 clear isis neighbor

Description

This command is used to clear the neighbor relationship established by IS-IS and re-establish the relationship with neighbor device.

Syntax

clear isis neighbor [*system-id*]

Parameter

system-id: System ID of the specified neighbor.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear all IS-IS neighbors:

```
Switch(config-router)#clear isis neighbor
```

50.20 redistribute

Description

This command is used to redistribute routes. In a multi-protocol deployment scenario, routes of other protocols or other IS-IS instances can be redistributed to IS-IS, which will then flood the routes throughout the entire area.

Syntax

redistribute { ipv4 { bgp | connected | rip | static | ospf *process-id* | isis *area-name* } | ipv6 { bgp | connected | ospf6 | ripng | static } } { level-1 | level-2 }

Parameter

ipv4: Redistribute IPv4 routing.

ipv6: Redistribute IPv6 routing.

bgp: Redistribute BGP routing.

connected: Redistribute direct routing.

ospf: redirect OSPF routing.

process-id: redirect OSPF routing instance number

isis: redirect IS-IS routing

area-name: redirect IS-IS routing area name

rip: redirect RIP routing
static: Redistribute static routes.
ospf6: Redistribute OSPFv3 routes.
ripng: Redistribute RIPng routes.
level-1: Redirect to level-1 area.
level-2: Redirect to level-2 area.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Redistribute IPv4 BGP routes to the level-1 area of IS-IS:

```
Switch(config-router)# redistribute ipv4 bgp level-1
```

50.21 distance

Description

This command is used to configure the distance of IS-IS protocol routes, that is, the route priority of IS-IS protocol. This function can change the priority strategy of different protocol routes in multi-protocol scenarios.

Syntax

distance *value*

Parameter

value: Distance value, ranging from 1 to 255, and the default value is 110.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the distance of the IS-IS protocol to 100:

```
Switch(config-router)#distance 100
```

50.22 ip router isis

Description

This command is used to enable IPv4 IS-IS on an interface, while its no form disables the IPv4 IS-IS functionality under the interface. Configuration of IS-IS settings under an interface is only permitted when either IPv4 or IPv6 IS-IS has been enabled. If both IPv4 and IPv6 IS-IS are disabled simultaneously, all IS-IS configurations under the interface will be cleared.

Syntax

```
ip router isis area-name  
no ip router isis
```

Parameter

area-name: Specify the area name of the IS-IS instance.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable interface VLAN 1 on IS-IS instance 1:

```
Switch(config)#interface vlan 1  
Switch(config-if)#ip router isis 1
```

50.23 ipv6 router isis

Description

This command is used to enable IPv6 IS-IS on an interface. Its "no" form disables IPv6 IS-IS functionality on the interface. Interface-specific IS-IS configurations can only be performed when either IPv4 or IPv6 IS-IS is enabled. When both IPv4 and IPv6 IS-IS functionalities are disabled, all IS-IS configurations under the interface will be cleared.

Syntax

```
Ipv6 router isis area-name
```

no ipv6 router isis

Parameter

area-name: Specify the area name of the IS-IS instance.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable interface VLAN 1 on IS-IS IPV6 instance 1:

```
Switch(config)#interface vlan 1
Switch(config-if)#ipv6 router isis 1
```

50.24 isis bfd

Description

This command is used to enable BFD on an interface and notify IS-IS. IS-IS can quickly detect changes in interface status. To disable this function, please use the no isis bfd command.

Syntax

```
isis bfd [ bfd-template ]
no isis bfd
```

Parameter

bfd-template: BFD template name, depending on the global BFD template configuration

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable BFD on interface VLAN 1 and notify IS-IS:


```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#isis bfd
```

50.25 isis circuit-type

Description

This command is used to configure the IS-IS area type of the interface. By default, the area type of the IS-IS interface is the area type configured globally for IS-IS. To restore the default configuration, please use the **no isis circuit-type** command.

Syntax

```
isis circuit-type { level-1 | level-1-2 | level-2-only }
```

```
no isis circuit-type
```

Parameter

level-1: Set the IS-IS area type to Level-1

level-1-2: Set the IS-IS area types to Level-1 and Level-2

level-2-only: Set the IS-IS area type to Level-2

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS area type of interface VLAN 1 to Level-1:

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#isis circuit-type level-1
```

50.26 isis csnp-interval

Description

This command is used to configure the interval for sending CSNP packets of IS-IS on the interface. To restore the default configuration, please use the **no isis csnp-interval** command.

Syntax

isis csnp-interval *interval*
no isis csnp-interval

Parameter

interval: The interval for sending CSNP packets, ranging from 1 to 600s, and the default value is 10.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the CSNP message sending interval of IS-IS on interface VLAN 1 to 20s:

```
Switch(config)#interface vlan 1
Switch(config-if)#isis csnp-interval 20
```

50.27 isis hello-interval

Description

This command is used to configure the interval for sending Hello packets of IS-IS on the interface. To restore the default configuration, please use the **no isis csnp-interval** command.

Syntax

isis hello-interval *interval*
no isis hello-interval

Parameter

interval: The interval for sending Hello packets, ranging from 1 to 600s, and the default value is 3.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the Hello message sending interval of IS-IS on interface VLAN 1 to 10s:

```
Switch(config)#interface vlan 1
Switch(config-if)#isis hello-interval 10
```

50.28 isis hello-multiplier

Description

This command is used to configure the multiplier of the IS-IS Hello message on the interface. Hello-interval * Hello-multiplier is the neighbor's Hold timer. To restore the default configuration, please use the **no isis hello-multiplier** command.

Syntax

```
isis hello-multiplier value
no isis hello-multiplier
```

Parameter

value: Hello multiplier, ranging from 2 to 100. It is 10 by default.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS Hello multiplier on interface VLAN 1 to 20:

```
Switch(config)#interface vlan 1
Switch(config-if)# isis hello-multiplier 20
```

50.29 isis metric

Description

This command is used to configure the IS-IS metric on the interface. To restore the default configuration, please use the **no isis metric** command.

Syntax

isis metric *value*
no isis metric

Parameter

value: IS-IS metric, ranging from 0 to 16777215. It is 10 by default.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS metric on interface VLAN 1 to 20:

```
Switch(config)#interface vlan 1
Switch(config-if)#isis metric 20
```

50.30 isis network point-to-point

Description

This command is used to configure the IS-IS network type of the interface. To restore the default configuration, please use the **no isis network point-to-point** command.

Syntax

isis network point-to-point
no isis network point-to-point

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS network type of interface VLAN 1 to P2P:

```
Switch(config)#interface vlan 1
Switch(config-if)# isis network point-to-point
```

50.31 isis passive

Description

This command is used to configure the IS-IS silent function on the interface. After it is enabled, the interface will not be able to perform IS-IS message exchange and route calculation. To disable this function, please use the **no isis passive** command.

Syntax

isis passive
no isis passive

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Make the IS-IS on VLAN 1 silent:

```
Switch(config)#interface vlan 1
Switch(config-if)#isis passive
```

50.32 isis password-key

Description

This command is used to enable the IS-IS authentication function. After the function is enabled, IS-IS will carry authentication information in the message exchange in the area and verify the authentication information. To disable this function, please use the **no area-password** command.

Syntax

isis password-key { **clear** | **md5** } { **0** | **7** } *text*
no isis password-key

Parameter

clear: Encrypt in plain text.

md5: Encrypt using md5 algorithm.

0: Enter plain text.

7: Enter in cipher text.

text: Password text

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure MD5 encrypted authentication for the IS-IS on VLAN 1:

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#isis password-key md5 0 tp-link
```

50.33 isis priority

Description

This command is used to enable the IS-IS authentication function. After the function is enabled, IS-IS will carry authentication information in the message exchange in the area and verify the authentication information. To disable this function, please use the **no area-password** command.

Syntax

isis priority *value*
no isis priority

Parameter

Value: The DIS election priority of the interface, ranging from 0 to 127, and the default value is 64.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS priority of interface VLAN 1 to 100:

```
Switch(config)#interface vlan 1
Switch(config-if)# isis priority 100
```

50.34 topology

Description

This command is used to enable IS-IS multi-topology under the interface, allowing the creation of independent logical topologies for different protocols or services. To disable this configuration, please use the **no topology** command.

Syntax

```
topology { ipv6-unicast }
no topology { ipv6-unicast }
```

Parameter

ipv6-unicast: IS-IS enabled for IPv6 unicast topology.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure IS-IS multi-topology:

```
Switch(config)#interface vlan 1
Switch(config-if)#topology ipv6-unicast
```

50.35 isis three-way-handshake

Description

This command is used to configure the three-way handshake mechanism of the IS-IS neighbor on the interface. By default, IS-IS neighbor establishment is a two-way handshake mechanism. Two-way handshakes have the problem of one-way neighbor establishment. It is recommended to use the three-way handshake mechanism. To restore the default configuration, please use the **no isis three-way-handshake** command.

Syntax

isis three-way-handshake
no isis three-way-handshake

Parameter

None

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the IS-IS three-way handshake neighbor establishment mechanism on interface VLAN 1:

```
Switch(config)#interface vlan 1
Switch(config-if)#isis three-way-handshake
```

50.36 show isis database

Description

This command is used to view the IS-IS database information.

Syntax

show isis [tag { *area-name* }] database [*lsp-id* | detail]

Parameter

area-name: Specify the IS-IS area name for the query.

lsp-id: Specify the LSP ID for the query.

detail: View detailed information **Command Mode**

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the brief information of IS-IS database:

```
Switch#show isis database
```

50.37 show isis graceful-restart

Description

This command is used to view the Graceful Restart information for IS-IS.

Syntax

```
show isis [ tag { area-name } ] graceful-restart status
```

Parameter

area-name: Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS Graceful Restart information:

```
Switch#show isis database
```

50.38 show isis hostname

Description

This command is used to view the IS-IS host name mapping information.

Syntax

show isis [tag { *area-name* }] hostname **Parameter**

area-name: Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS host name mapping information:

```
Switch# show isis hostname
```

50.39 show isis neighbor

Description

This command is used to view the IS-IS neighbor information.

Syntax

show isis [tag { *area-name* }] neighbor [*system-id* | detail]

Parameter

area-name: Specify the IS-IS area name for the query.

system-id: Specify the neighbor's system ID for the query.

detail: View detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the brief information of IS-IS neighbor:

```
Switch# show isis neighbor
```

50.40 show isis route

Description

This command is used to view the IS-IS routing information.

Syntax

show isis [tag { *area-name* }] route

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None**Example**

View the IS-IS routing information:

```
Switch# show isis route
```

50.41 show isis summary

Description

This command is used to view the IS-IS summary.

Syntax

show isis [tag { *area-name* }] summary

Parameter

area-name: Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None**Example**

View the IS-IS summary:

```
Switch# show isis summary
```

50.42 show isis interface

Description

This command is used to view the IS-IS interface information.

Syntax

```
show isis [ tag { area-name } ] interface [ fastEthernet | gigabitEthernet |  
hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet |  
twentyFive-gigabitEthernet | two-gigabitEthernet | vlan ] [ detail ]
```

Parameter

area-name: Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS interface information:

```
Switch# show isis interface
```

50.43 show isis topology

Description

This command is used to view the IS-IS topology information.

Syntax

```
show isis [ tag { area-name } ] topology [ level-1 | level-2 ]
```

Parameter

area-name: Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS topology information:

```
Switch# show isis topology
```

Chapter 51 URPF Configuration Commands (Only for Certain Devices)

Unicast Reverse Path Forwarding (URPF) aims to prevent network attacks based on source IP address spoofing. To safeguard against forged IP packet attacks on the network, at the network ingress point, the origin of IP packets is verified. If the source is suspicious, the packet is dropped directly; if it passes the URPF check, the IP packet is allowed to enter.

51.1 urpf

Description

This command is used to enable or disable the URPF feature. When enabled, it retrieves the previously configured filtering mode for security checks. If no mode was previously configured, it performs security checks based on the default strict-vlan filtering mode. Disabling the URPF feature will not modify the set filtering mode for when URPF was disabled.

Syntax

```
urpf { enable| disable }
```

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the URPF feature on the switch:

```
Switch(config)# urpf enable
```

51.2 urpf mode

Description

This command is used to configure the URPF filter mode.

Syntax

urpf mode { strict-vlan | strict-port | loose }

Parameter

strict-vlan: Filter the packets whose IP or VLAN do not meet the requirements

strict-port: Filter the packets whose IP or port do not meet the requirements

loose: Filter the packets whose IP does not meet the requirements

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the URPF feature on the switch:

```
Switch(config)# urpf mode strict-vlan
```

Chapter 52 Tunnel Configuration Commands (Only for Certain Devices)

Tunnel is an encapsulation technique that uses one network protocol to transport another network protocol. It encapsulates data packets generated by another protocol within its own packets, enabling the transmission of IPv6 packets over an IPv4 network and facilitating interconnection between IPv6 networks. A tunnel represents a virtual point-to-point connection where it provides a channel for the transmission of encapsulated data packets, allowing for encapsulation and decapsulation of data packets at both ends of the tunnel.

EoGRE (Ethernet over GRE) is a tunneling technology used to encapsulate Ethernet frames for transmission over an IP network. By carrying Ethernet traffic from multiple VLANs over an EoGRE tunnel, it enables Layer 2 network interconnection across different geographical locations.

52.1 interface tunnel

Description

This command is used to create a Tunnel entry and enters Tunnel Interface Configuration Mode. Its `no` command deletes the configuration information and removes the tunnel.

Syntax

interface tunnel *tunnel-number*
no interface tunnel *tunnel-number*

Parameter

tunnel-number: Tunnel entry index value, range 1–1000. Only one value can be entered per command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a tunnel with an index value of 10 and enter Tunnel Interface Configuration Mode:


```
Switch(config)# interface tunnel 10
```

52.2 tunnel mode

Description

This command is used to specify the tunnel mode. The tunnel will encapsulate different protocol headers for passenger messages according to different tunnel types. To delete the type of the tunnel interface, please use the **no tunnel mode** command.

Syntax

tunnel mode { gre { eth-ipv4 | ipv4-ipv4 | ipv6-ipv4 } | ipv6ip }
no tunnel mode

Parameter

gre eth-ipv4 — Specifies Ethernet over IPv4 tunnel mode, transmitting Ethernet frames over IPv4.

gre ipv4-ipv4 — Specifies GRE IPv4 over IPv4 tunnel mode, transmitting IPv4 packets over IPv4.

gre ipv6-ipv4 — Specifies GRE IPv6 over IPv4 tunnel mode, transmitting IPv6 packets over IPv4.

ipv6ip — Specifies IPv6 over IPv4 tunnel mode, transmitting IPv6 packets over IPv4.

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure Tunnel 10 to use EoGRE mode:

```
Switch(config)# interface tunnel 10
```

```
Switch(config-tunnel)# tunnel mode gre eth-ipv4
```

52.3 tunnel ttl

Description

This command is used to configure the TTL parameter for the tunnel. TTL (Time to Live) is a field in network protocols used to control the lifetime of a packet within a network. In an EoGRE tunnel, the TTL value determines the maximum number of hops the encapsulated outer IP packet is allowed to traverse in the network. This helps prevent packets from looping indefinitely and limits the propagation distance of packets across wide area networks.

Syntax

tunnel ttl *ttl-value*
no tunnel ttl

Parameter

ttl-value — The Time to Live value, range 1–255. Default is 255.

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the TTL for Tunnel 10 to 254:

```
Switch(config)# interface tunnel 10
Switch(config-tunnel)# tunnel ttl 254
```

52.4 tunnel ip address

Description

This command is used to specify the interface IP address of the tunnel. GRE IPv4-IPv4 tunnels need to be configured with an IPv4 address, and IPv6IP and GRE IPV6-IPv4 tunnels need to be configured with an IPv6 address. To delete the IP address of the tunnel, please use the no ip address command.

Syntax

ip address *ipv4-address* / **ipv6 address** *ipv6-address*
no ip address / **no ipv6 address**

Parameter

ipv4-address: IPv4 address of the tunnel interface.

ipv6-address: IPv6 address of the tunnel interface.

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the interface IP address of the GRE IPv4-IPv4 tunnel as 10.1.1.1:

```
Switch(config)#interface tunnel 1
```

```
Switch(config-tunnel) ip address 10.1.1.1
```

52.5 tunnel source

Description

This command is used to configure the source IP address for the tunnel. The tunnel source can be specified in three modes: IP address, Layer 3 interface, or VLANif.

Syntax

```
tunnel source {ip address ip-address | interface {gigabitEthernet |  
hundred-gigabitEthernet | port-channel | ten-gigabitEthernet |  
twentyFive-gigabitEthernet | two-gigabitEthernet} port-number | vlan-if  
vlanId}  
no tunnel source
```

Parameter

ip-address — Source IP address.

port-number — Port number, e.g., gigabitEthernet 1/0/1.

vlanId — Index value of the Layer 3 VLAN interface.

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the source IP for Tunnel 10 as 192.168.10.1:

```
Switch(config)# interface tunnel 10
Switch(config-tunnel)# tunnel source ip address 192.168.10.1
```

52.6 tunnel destination

Description

This command is used to configure the destination IP address for the tunnel.

Syntax

tunnel destination ip address *ipv4-address*
no tunnel destination ip address

Parameter

ipv4-address — *Destination IP address.*

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the destination IP for Tunnel 10 as 192.168.10.2:

```
Switch(config)# interface tunnel 10
Switch(config-tunnel)# tunnel destination ip address 192.168.10.2
```

52.7 keepalive period retry-times

Description

This command is used to configure the keepalive parameters for the tunnel, which is a mechanism used to detect and maintain the tunnel connection state.

Syntax

keepalive period *period* **retry-times** *times*

Parameter

period — Keepalive packet transmission interval, in seconds. Range 1–6000. Default is 5 seconds.

times — Retry count. Range 1–255. Default is 3.

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure keepalive for Tunnel 10: send a probe every 10 seconds; consider the tunnel down after 5 consecutive timeouts:

```
Switch(config)# interface tunnel 10
```

```
Switch(config-tunnel)# keepalive period 10 retry-times 5
```

52.8 tunnel vlan

Description

This command is used to configure the access-side VLAN(s) for the EoGRE tunnel. A single EoGRE tunnel can correspond to one VLAN or multiple VLANs. The VLAN(s) must already exist before configuration.

Syntax

tunnel vlan { *vlanId* | *vlan-range* }

no tunnel vlan

Parameter

vlanId — A single VLAN index value, range 1–4094.

vlan-range — A VLAN range, supporting the following formats:

- Continuous range: 1-100
- Multiple ranges: 1-10,50-100

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure VLAN 100 as the access-side VLAN for EoGRE Tunnel 10:

```
Switch(config)# interface tunnel 10
Switch(config-tunnel)# tunnel vlan 100
```

52.9 shutdown

Description

This command is used to disable the tunnel interface (enabled by default), but does not delete the configuration.

Syntax

shutdown
no shutdown

Parameter

None

Command Mode

Tunnel Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the functionality of Tunnel 10:

```
Switch(config)# interface tunnel 10
```

```
Switch(config-tunnel)# shutdown
```

52.10 ip route tunnel

Description

This command is used to configure a static route for IPv4 packets to point to a tunnel, so that IPv4 packets can enter the tunnel (including only GRE IPv4-IPv4 type tunnels). To delete the static route configuration, please use the no command.

Syntax

ip route *ip-address mask* **tunnel** *tunnel-number*

no ip route *ip-address mask* **tunnel** *tunnel-number*

Parameter

ip-address: IP address of the static route.

mask: Mask of the static route.

tunnel-number: Tunnel interface to which the static route points

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the IPv4 static route to point to tunnel interface 1:

```
Switch(config)#ip route 192.168.2.0 255.255.255.0 tunnel 1
```

52.11 ipv6 route tunnel

Description

This command is used to configure a static route for IPv6 packets to point to a tunnel, so that IPv6 packets can enter the tunnel (including only IPv6IP and GRE IPv6-IPv4 type tunnels). To delete the static route configuration, please use the no command.

Syntax

ipv6 route *ipv6-dest-address* **tunnel** *tunnel-number*
no ipv6 route *ipv6-dest-address* **tunnel** *tunnel-number*

Parameter

ipv6-dest-address: Specify the destination IPv6 address of the packets, in the format of X:X:X:X::X/<0-128>.

tunnel-number: Tunnel interface to which the static route points

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the IPv6 static route to point to tunnel interface 1:

```
Switch(config)# ipv6 route fc00:2::/64 tunnel 1
```

52.12 show interface tunnel

Description

This command is used to view the tunnel interface information, including configuration details and current status.

Syntax

show interface tunnel {*tunnel-number* | **all**}

Parameter

tunnel-number — Tunnel entry index value, range 1–1000.

all — All tunnels.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display information for Tunnel 10:


```
Switch(config)# show interface tunnel 10
```

Chapter 53 IPv6 Address Configuration Commands

The IPv6 address configuration commands are provided in the Interface Configuration Mode, which includes the routed port, the port-channel interface and the VLAN interface. Enter the configuration mode of these Layer 3 interfaces and configure their IPv6 parameters.

53.1 ipv6 enable

Description

This command is used to enable the IPv6 function on the specified Layer 3 interface. IPv6 function should be enabled before the IPv6 address configuration management. By default it is enabled on VLAN interface 1. IPv6 function can only be enabled on one Layer 3 interface at a time.

If the IPv6 function is disabled, the corresponding IPv6-based modules will be invalid, for example SSHv6, SSLv6, TFTPv6 and more. To disable the IPv6 function, please use **no ipv6 enable** command.

Syntax

ipv6 enable
no ipv6 enable

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IPv6 function on the VLAN interface 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 enable
```

53.2 ipv6 address autoconfig

Description

This command is used to enable the automatic configuration of the ipv6 link-local address. The switch has only one ipv6 link-local address, which can be configured automatically or manually. The general ipv6 link-local address

has the prefix as fe80::/10. IPv6 routers cannot forward packets that have link-local source or destination addresses to other links. The auto-configured ipv6 link-local address is in EUI-64 format. To verify the uniqueness of the link-local address, the manually configured ipv6 link-local address will be deleted when the auto-configured ipv6 link-local address takes effect.

Syntax

ipv6 address autoconfig

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the automatic configuration of the ipv6 link-local address on VLAN interface 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 address autoconfig
```

53.3 ipv6 address autoglobal

Description

The **ipv6 address autoglobal** command is used to enable IPv6 autoglobal address configuration on the interface. When enabled, the interface processes received RA messages to automatically configure a global IPv6 address. To disable this function, use the **no ipv6 address autoglobal** command.

Syntax

ipv6 address autoglobal

no ipv6 address autoglobal

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IPv6 autoglobal on the interface:

```
Switch(config-if)# ipv6 address autoglobal
```

53.4 ipv6 address link-local

Description

The **ipv6 address link-local** command is used to configure the ipv6 link-local address manually on a specified interface. To delete the configured link-local address, please use **no ipv6 address link-local** command.

Syntax

```
ipv6 address ipv6-addr link-local
```

```
no ipv6 address ipv6-addr link-local
```

Parameter

ipv6-addr — The link-local address of the interface. It should be a standardized IPv6 address with the prefix fe80::/10, otherwise this command will be invalid.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the link-local address as fe80::1234 on the VLAN interface 1:

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# ipv6 address fe80::1234 link-local
```

53.5 ipv6 address dhcp

Description

The **ipv6 address dhcp** command is used to enable the DHCPv6 Client function. When this function is enabled, the Layer 3 interface will try to obtain IP from DHCPv6 server. To delete the allocated IP from DHCPv6 server and disable the DHCPv6 Client function, please use **no ipv6 address dhcp** command.

Syntax

ipv6 address dhcp

no ipv6 address dhcp

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Client function on VLAN interface 1:

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# ipv6 address dhcp
```

53.6 ipv6 address ra

Description

This command is used to configure the interface's global IPv6 address according to the address prefix and other configuration parameters from its received RA(Router Advertisement) message. To disable this function, please use **no ipv6 address ra** command.

Syntax

ipv6 address ra

no ipv6 address ra

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the automatic ipv6 address configuration function to obtain IPv6 address through the RA message on VLAN interface 1:

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# ipv6 address ra
```

53.7 ipv6 address eui-64

Description

This command is used to manually configure a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits on the interface. Specify only the network prefix. The last 64 bits are automatically computed from the switch MAC address. To remove a EUI-64 IPv6 address from the interface, please use the **no ipv6 address eui-64** command.

Syntax

```
ipv6 address ipv6-addr eui-64
```

```
no ipv6 address ipv6-addr eui-64
```

Parameter

ipv6-addr—— Global IPv6 address with 64 bits network prefix, for example 3ffe::/64.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure an EUI-64 global address on the interface with the network prefix 3ffe::/64:

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# ipv6 address 3ffe::/64 eui-64
```

53.8 ipv6 address

Description

This command is used to manually configure a global IPv6 address on the interface. To remove a global IPv6 address from the interface, please use **no ipv6 address** command.

Syntax

ipv6 address *ipv6-addr*

no ipv6 address *ipv6-addr*

Parameter

ipv6-addr — Global IPv6 address with network prefix, for example 3ffe::1/64.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the global address 3001::1/64 on VLAN interface 1:

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# ipv6 address 3001::1/64
```

53.9 ipv6 gateway

Description

The **ipv6 gateway** command is used to manually configure the IPv6 gateway address on an interface. To disable this function, use the **no ipv6 gateway** command.

Syntax

ipv6 gateway *gateway-address*

no ipv6 gateway

Parameter

gateway-address — IPv6 gateway address.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the interface gateway to 2000::1:

```
Switch(config-if)# ipv6 gateway 2000::1
```

53.10 ipv6 dnsDynamic

Description

The **ipv6 dnsDynamic** command is used to enable dynamic IPv6 DNS acquisition on an interface. When enabled, the interface can learn IPv6 DNS server information from RA messages or DHCPv6. To disable this function, use the **no ipv6 dnsDynamic** command.

Syntax

ipv6 dnsDynamic

no ipv6 dnsDynamic

Parameter

None.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable dynamic IPv6 DNS acquisition on the interface:

```
Switch(config-if)# ipv6 dnsDynamic
```

53.11 show ipv6 interface

Description

This command is used to display the configured ipv6 information of the management interface, including ipv6 function status, link-local address and global address, ipv6 multicast groups etc.

Syntax

show ipv6 interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ipv6 information of the management interface:

```
Switch(config)# show ipv6 interface
```

Chapter 54 ARP Commands

Address Resolution Protocol (ARP) is used to resolve an IP address into an Ethernet MAC address. The switch maintains an ARP mapping table to record the IP-to-MAC mapping relations, which is used for forwarding packets. An ARP mapping table contains two types of ARP entries: dynamic and static. An ARP dynamic entry is automatically created and maintained by ARP. A static ARP entry is manually configured and maintained.

54.1 arp

Description

This **arp** command is used to add a static ARP entry. To delete the specified ARP entry, please use the **no arp** command. If the command contains vrf, the arp belongs to the vrf instance.

Syntax

arp *ip mac type* [**vrf** *vrf-name*]

no arp *ip type* [**vrf** *vrf-name*]

Parameter

ip — The IP address of the static ARP entry.

mac — The MAC address of the static ARP entry.

type — The ARP type. Configure it as "arpa".

vrf-name — Specify the vrf name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a static ARP entry with the IP as 192.168.0.1 and the MAC as 00:11:22:33:44:55:

```
Switch(config)# arp 192.168.0.1 00:11:22:33:44:55 arpa vrf v1
```

54.2 clear arp-cache

Description

This **clear arp-cache** command is used to clear all the dynamic ARP entries. If the command contains VRF, the ARP entries of the VRF instance are clear.

Syntax

clear arp-cache [**vrf** *vrf-name*]

Parameter

vrf-name——Specify the vrf name.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear ARP entries in VRF v1:

```
Switch(config)# clear arp-cache vrf v1
```

54.3 arp dynamicrenew

Description

This **arp dynamicrenew** command is used to automatically renew dynamic ARP entries. To disable the switch to automatically renew dynamic ARP entries, please use the **no arp dynamicrenew** command. By default, it is enabled.

Syntax

arp dynamicrenew

no arp dynamicrenew

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the switch to automatically renew the dynamic ARP entries:

```
Switch(config)# arp dynamicrenew
```

54.4 arp timeout

Description

This **arp timeout** command is used to configure the ARP aging time of the interface.

Syntax

arp timeout *timeout*

no arp timeout

Parameter

timeout—— Specify the aging time, ranging from 10 to 3000 seconds. The default value is 1200 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ARP aging time as 60 seconds:

```
Switch(config)# arp timeout 60
```

54.5 gratuitous-arp intf-status-up enable

Description

This **gratuitous-arp intf-status-up enable** command is used to enable the Layer 3 interface to send a gratuitous ARP packet when the interface's status becomes up.

Syntax

gratuitous-arp intf-status-up enable

no gratuitous-arp intf-status-up enable

Command Mode

Global Configuration Mode

Privilege Requirement

None.

Example

Enable the switch's Layer 3 interfaces to send gratuitous ARP packets when their status becomes up:

```
Switch(config)# gratuitous-arp intf-status-up enable
```

54.6 gratuitous-arp dup-ip-detected enable

Description

This **gratuitous-arp dup-ip-detected enable** command is used to enable the Layer 3 interface to send a gratuitous ARP packet when receiving a gratuitous packets of which the IP address is the same as its own.

Syntax

gratuitous-arp dup-ip-detected enable

no gratuitous-arp dup-ip-detected enable

Command Mode

Global Configuration Mode

Privilege Requirement

None.

Example

Enable the switch's Layer 3 interface to send gratuitous ARP packets when receiving a gratuitous packets of which the IP address is the same as its own:

```
Switch(config)# gratuitous-arp dup-ip-detected enable
```

54.7 gratuitous-arp learning enable

Description

This **gratuitous-arp learning enable** command is used to enable the Layer 3 interface to learn MAC addresses from the gratuitous ARP packets.

Syntax

gratuitous-arp learning enable

no gratuitous-arp learning enable

Command Mode

Global Configuration Mode

Privilege Requirement

None.

Example

Enable the Layer 3 interface to learn MAC addresses from the gratuitous ARP packets:

```
Switch(config)# gratuitous-arp learning enable
```

54.8 gratuitous-arp send-interval

Description

This **gratuitous-arp send-interval** command is used to configure the interval at which the interface periodically send the gratuitous ARP packets.

Syntax

gratuitous-arp send-interval *interval*

Parameter

Interval—— Specify the interval at which the interface periodically send the gratuitous ARP packets. Value 0 means the interface will not send gratuitous ARP packets.

Command Mode

Interface Configuration Mode (interface vlan / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

None.

Example

Specify the interface VLAN 1 to send gratuitous ARP packets every 1 second:

```
Switch(config)# interface vlan 1
Switch(config-if)# gratuitous-arp send-interval 1
```

54.9 ip proxy-arp

Description

The **ip proxy-arp** command is used to enable Proxy ARP function on the specified VLAN interface or routed port. To disable Proxy ARP on this interface, please use **no ip proxy-arp** command.

Syntax

ip proxy-arp
no ip proxy-arp

Command Mode

Interface Configuration Mode (interface vlan / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

None

Example

Enable the Proxy ARP function on VLAN Interface 2:

```
Switch(config)# interface vlan 2
```

```
Switch(config-if)# ip proxy-arp
```

Enable the Proxy ARP function on routed port 1/0/2:

```
Switch(config)# interface gigabitEthernet 2
```

```
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip proxy-arp
```

54.10 ip local-proxy-arp

Description

The **ip local-proxy-arp** command is used to enable Local Proxy ARP function on the specified VLAN interface or routed port. To disable Local Proxy ARP function on this interface, please use **no ip local-proxy-arp** command.

Syntax

ip local-proxy-arp

no ip local-proxy-arp

Command Mode

Interface Configuration Mode (interface vlan / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

None

Example

Enable the Proxy ARP function on VLAN Interface 2:

```
Switch(config)# interface vlan 2
```

```
Switch(config-if)# ip local-proxy-arp
```

Enable the Proxy ARP function on routed port 1/0/2:

```
Switch(config)# interface gigabitEthernet 2
```



```
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip local-proxy-arp
```

54.11 show arp

Description

This **show arp** command is used to display the active ARP entries. If no parameter is specified, all the active ARP entries will be displayed. If the VRF is specified, the arp entries of the VRF instance are displayed.

Syntax

```
show arp [ ip ] [ mac ] [vrf vrf-name]
```

Parameter

ip — Specify the IP address of your desired ARP entry.

mac — Specify the MAC address of your desired ARP entry.

vrf-name — Specify the VRF name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP entry with the IP as 192.168.0.2 in vrf v1:

```
Switch(config)# show arp 192.168.0.2 vrf v1
```

54.12 show ip arp (interface)

Description

This **show ip arp (interface)** command is used to display the active ARP entries associated with a specified Layer 3 interface.

Syntax

```
show ip arp { gigabitEthernet port | port-channel port-channel-id | vlan id }
```

Parameter

port — Specify the number of the routed port.

port-channel-id—— Specify the ID of the port channel.

id—— Specify the VLAN interface ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP entry associated with VLAN interface 2:

```
Switch(config)# show ip arp vlan 2
```

54.13 show ip arp summary

Description

This **show ip arp summary** command is used to display the number of the active ARP entries.

Syntax

```
show ip arp summary
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the number of the ARP entries:

```
Switch(config)# show ip arp summary
```

54.14 show gratuitous-arp

Description

This **show gratuitous arp** command is used to display the configuration of gratuitous ARP.

Syntax

show gratuitous-arp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of gratuitous ARP:

```
Switch(config)# show gratuitous-arp
```

54.15 show ip proxy-arp

Description

The **show ip proxy-arp** command is used to display the Proxy ARP status.

Syntax

show ip proxy-arp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Display the Proxy ARP status:

```
Switch(config)# show ip proxy-arp
```

Chapter 55 VRRP Commands (Only for Certain Devices)

VRRP (Virtual Routing Redundancy Protocol) is a function on the switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts.

55.1 ip vrrp vrid

Description

The **ip vrrp vrid** command is used to enable the VRRP-V2 protocol on the interface and specify the virtual router ID for it. To disable the protocol on the interface, please use the **no ip vrrp vrid** command.

Syntax

ip vrrp vrid *vrid-index*
no ip vrrp vrid *vrid-index*

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the VRRP-V2 protocol on VLAN 2 and specify the virtual router ID as 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5
```

55.2 ipv6 vrrp vrid

Description

The **ipv6 vrrp vrid** command is used to enable the VRRP-V3 protocol on the interface and specify the virtual router ID for it. To disable the protocol on the interface, please use the **no ipv6 vrrp vrid** command.

Syntax

```
ipv6 vrrp vrid vrid-index  
no ipv6 vrrp vrid vrid-index
```

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the VRRP-V3 protocol on VLAN 2 and specify the virtual router ID as 5:

```
Switch(config)#interface vlan 2  
Switch(config-if)#ipv6 vrrp vrid 5
```

55.3 ip vrrp vrid authentication-mode

Description

The **ip vrrp vrid authentication-mode** command is used to configure the authentication mode of the virtual router on the specified interface. To restore to the default authentication mode, please use the **no ip vrrp vrid authentication-mode** command.

Syntax

```
ip vrrp vrid vrid-index authentication-mode {simple | md5} [0 | 7] password  
no ip vrrp vrid vrid-index authentication-mode
```

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

simple | md5—— Authentication mode, by default it is None and no authentication will be performed. "simple" refers to using a text password for authentication, and "md5" refers to using a text password to perform the authentication of MD5, which has a higher security than Simple mode.

0 | 7 —— Key form, 0 represents plaintext, 7 represents ciphertext.

password—— Password, a string of 1 to 8 alphabets, numbers or symbols. Passwords are casesensitive, spaces allowed but leading spaces ignored, and cannot contain question marks. It is empty by default.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the md5 authentication mode on the VLAN 2, specify the password as 123 and the virtual router ID as 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 authentication-mode md5 123
Switch(config-if)#ip vrrp vrid 5 authentication-mode md5 0 123
```

55.4 ip vrrp vrid description

Description

The **ip vrrp vrid description** command is used to configure and modify the description for the virtual router. To delete the description, please use the **no ip vrrp vrid description** command.

Syntax

ip vrrp vrid *vrid-index* **description** *description*

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

description—— A string describing the virtual router, containing up to 256 characters, consisting only of numbers, English letters, and dashes.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the virtual router description as vr5 and the virtual router ID as 5 on the VLAN 2:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 description vr5
```

55.5 ip vrrp vrid preempt-mode

Description

The **ip vrrp vrid preempt-mode** command is used to configure the preemption mode and delay time of the specified virtual router on the interface. To set the specified virtual router on the interface to non-preempt mode, please use the **no ip vrrp vrid preempt-mode** command. By default, the virtual router is in preempt mode.

Syntax

```
ip vrrp vrid vrid-index preempt-mode [ timer-delay delay-value ]
no ip vrrp vrid vrid-index preempt-mode
```

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

delay-value—— When the current primary router is deemed unavailable, the backup router waits before switching to the primary router. The value ranges from 0 to 255 seconds, and the default is 0.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the virtual router preemption time to 12 seconds and the virtual router ID to 5 on VLAN 2:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 preempt-mode timer-delay 12
```

55.6 ip vrrp vrid priority

Description

The **ip vrrp vrid priority** command is used to configure the priority of the specified virtual router on the interface. To restore the default priority, please use the **no ip vrrp vrid priority** command.

Syntax

```
ip vrrp vrid vrid-index priority priority
no ip vrrp vrid vrid-index priority
```

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

priority—— Priority, value ranges from 1 to 254. The default priority is 100.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the virtual router priority to 1110 and the virtual router ID to 5 on VLAN 2:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 priority 1110
```


55.7 ip vrrp vrid timer-advertise

Description

The **ip vrrp vrid timer-advertise** command is used to configure the frequency at which the specified virtual router sends advertisements on the interface. To restore the default advertisement interval, please use the **no ip vrrp vrid timer-advertise** command.

Syntax

ip vrrp vrid *vrid-index* **timer-advertise** *adver-interval*

no ip vrrp vrid *vrid-index* **timer-advertise**

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

adver-interval—— Advertisement interval, for VRRP-V2, the value range is 1~255, the unit is seconds, the default is 1 second; for VRRP-V3, the value range is 100~4095, the unit is centiseconds, the default is 100 centiseconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the virtual router advertisement interval to 12 seconds and the virtual router ID to 5 on VLAN 2:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 timer-advertise 12
```

55.8 ip vrrp vrid track

Description

The **ip vrrp vrid track** command is used to configure the specified virtual router on the interface to add a tracking interface. To delete the tracking interface, please use the **no ip vrrp vrid track** command.

Syntax

ip vrrp vrid *vrid-index* **track interface** {{fastEthernet | gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet} *port* / **port-channel** *portchannel-id* / **vlan** *vlan-id*}
[**reduce-priority** *priority*]

no ip vrrp vrid *vrid-index* **track interface** {{fastEthernet | gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet} *port* / **port-channel** *portchannel-id* / **vlan** *vlan-id*}

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

fastEthernet | gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet —— Port type, which must be a layer 3 interface.

port—— Port number.

portchannel-id—— LAG group number.

vlan-id—— Decreasing priority of the tracked interface, ranging from 1 to 254, and the default is 10.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the virtual router to track VLAN 3 on the VLAN 2 with a decreasing priority of 20 and a virtual router ID of 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 track interface vlan 3 reduce-priority 20
```

55.9 ip vrrp vrid version

Description

The **ip vrrp vrid version** command is used to configure or switch the VRRP version of the specified virtual router on the interface. The default is VRRP-V2.

Syntax

ip vrrp vrid *vrid-index* **version** *vrrp-version*

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

vrrp-version—— VRRP protocol version, the value is 2 or 3. Due to the differences between VRRP-V2 and VRRP-V3, version switching is only allowed when authentication is not configured, ipv6 virtual address is not configured, and the default notification time is used.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Switch the virtual router on the VALN 2 to VRRP-V3, and the virtual router ID to 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 version 3
```

55.10 ip vrrp vrid virtual-ip

Description

The **ip vrrp vrid virtual-ip** command is used to add a primary virtual IPv4 address to a virtual router. Each virtual router has only one primary virtual IP that cannot be deleted. If the virtual router does not exist, a VRRP-V2 version of the virtual router will be automatically created.

Syntax

ip vrrp vrid *vrid-index* **virtual-ip** *virtual-ip*

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

virtual-ip—— The virtual IP address of the virtual router, which must be in the same network segment as the interface.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add virtual IP address 192.168.0.10 on VLAN 2 with the virtual router ID 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 virtual-ip 192.168.0.10
```

55.11 ip vrrp vrid virtual-ip secondary

Description

The **ip vrrp vrid virtual-ip secondary** command is used to add a secondary virtual IPv4 address to a virtual router. Each virtual router can be configured with up to 32 IP addresses. To delete the corresponding secondary virtual IP address, use the **no ip vrrp vrid virtual-ip secondary** command.

Syntax

```
ip vrrp vrid vrid-index virtual-ip virtual-ip secondary
no ip vrrp vrid vrid-index virtual-ip virtual-ip secondary
```

Parameter

vrid-index — Virtual router ID, ranging from 1 to 255.

virtual-ip — The virtual IP address of the virtual router, which must be in the same network segment as the interface.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add secondary virtual IP address 192.168.0.11 on VALN 2 with the virtual router ID 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ip vrrp vrid 5 virtual-ip 192.168.0.10 secondary
```

55.12 ipv6 vrrp vrid address link-local

Description

The **ipv6 vrrp vrid address link-local** command is used to add a virtual ipv6 local link address to a virtual router. Each virtual router has only one virtual link-local address. If the virtual router does not exist, a VRRP-V3 version of the virtual router will be automatically created. To delete the virtual link-local address, use the **no ipv6 vrrp vrid address link-local** command.

Syntax

```
ipv6 vrrp vrid vrid-index address virtual-linklocal/link-local
no ipv6 vrrp vrid vrid-index address virtual-linklocal/link-local
```

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

virtual-linklocal—— The virtual link-local address of the virtual router. The address prefix should be the fe80::/10 standard ipv6 address.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add virtual ipv6 link-local address fe80::10 on VALN 2 with the virtual router ID 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 vrrp vrid 5 address fe80::10 link-local
```

55.13 ipv6 vrrp vrid address

Description

The **ipv6 vrrp vrid address** command is used to add a virtual ipv6 address to a virtual router. Each virtual router can be configured with up to 32 ipv6 addresses. To delete the virtual address, use the **no ipv6 vrrp vrid address** command.

Syntax

ipv6 vrrp vrid *vrid-index* **address** *virtual-ipv6*
no ipv6 vrrp vrid *vrid-index* **address** *virtual-ipv6*

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

virtual-ipv6—— The global ipv6 address of the virtual router, which must be in the same network segment as the interface ipv6 address.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add virtual ipv6 global address 3001::1 on VALN 2 with the virtual router ID 5:

```
Switch(config)#interface vlan 2
Switch(config-if)#ipv6 vrrp vrid 5 address 3001::1
```

55.14 show ip vrrp

Description

The **show ip vrrp** command is used to display basic configuration information of all virtual routers or a specified virtual router.

Syntax

show ip vrrp [**vrid** *vrid-index*] [**interface** {{fastEthernet | gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet } *port* | **port-channel** *portchannel-id* | **vlan** *vlan-id*}]

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

fastEthernet | gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet —— Port type, which must be a layer 3 interface.

port—— Port number.

portchannel-id—— LAG group number.

vlan-id—— VLAN value.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Display the configuration information of the virtual router ID 5 on VLAN 2:

```
Switch(config)#show ip vrrp vrid 5 interface vlan 2
```

55.15 show ip vrrp statistics

Description

The **show ip vrrp statistics** command is used to display statistics for all virtual routers or a specified virtual router.

Syntax

```
show ip vrrp statistics [vrid vrid-index] [interface {{fastEthernet |  
gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet |  
twentyFive-gigabitEthernet | two-gigabitEthernet } port / port-channel  
portchannel-id / vlan vlan-id}]
```

Parameter

vrid-index—— Virtual router ID, ranging from 1 to 255.

fastEthernet | gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet —— Port type, which must be a layer 3 interface.

port—— Port number.

portchannel-id—— LAG group number.

vlan-id—— VLAN value.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Display statistics of the virtual router ID 5 on VLAN 2:

```
Switch(config)#show ip vrrp statistics vrid 5 interface vlan 2
```

55.16 clear ip vrrp statistics

Description

The **clear ip vrrp statistics** command is used to clear the statistics of all virtual routers on the switch.

Syntax

```
clear ip vrrp statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Clear the statistics of all virtual routers on the switch:

```
Switch(config)#clear ip vrrp statistics
```


Chapter 56 DHCP Server Commands

DHCP (Dynamic Host Configuration Protocol) is a network configuration protocol for hosts on TCP/IP networks, and it provides a framework for distributing configuration information to hosts. DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them.

56.1 service dhcp server

Description

The **service dhcp server** command is used to enable DHCP service globally. To disable DHCP server service, please use **no service dhcp server** command.

Syntax

service dhcp server
no service dhcp server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP server service globally:

```
Switch(config)# service dhcp server
```

56.2 ip dhcp server extend-option capwap-ac-ip

Description

The **ip dhcp server extend-option capwap-ac-ip** command is used to specify the Option 138, which should be configured as the management IP address of an AC (Access Control) device. If the APs in the local network request this option, the server will inform the APs of the AC's IP address by

sending a packet containing this option. To delete the Option 138, please use **no ip dhcp server extend-option capwap-ac-ip** command.

Syntax

ip dhcp server extend-option capwap-ac-ip *ip-address*
no ip dhcp server extend-option capwap-ac-ip

Parameter

ip-address—— Specify the management IP address of an AC (Access Control) device.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the remote DHCP server's IP address as 192.168.3.1:

```
Switch(config)# ip dhcp server extend-option capwap-ac-ip 192.168.3.1
```

56.3 ip dhcp server extend-option vendor-class-id

Description

The **ip dhcp server extend-option vendor-class-id** command is used to configure the class ID of the packets from DHCP server in a different network segment. To delete the class ID settings, please use **no ip dhcp server extend-option vendor-class-id** command.

Syntax

ip dhcp server extend-option vendor-class-id *class-id*
no ip dhcp server extend-option vendor-class-id

Parameter

class-id—— Specify the class ID of the DHCP packets from another network segment.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the class ID of the DHCP packets from another network segment as 34:

```
Switch(config)# ip dhcp server extend-option vendor-class-id 34
```

56.4 ip dhcp server excluded-address

Description

The **ip dhcp server excluded-address** command is used to specify the reserved IP addresses which are forbidden to allocate, such as the gateway address, the network segment broadcast address, the server address etc. To delete the reserved IP addresses, please use **no ip dhcp server excluded-address** command.

Syntax

```
ip dhcp server excluded-address start-ip-address end-ip-address  
no ip dhcp server excluded-address start-ip- address end-ip-address
```

Parameter

start-ip-address —— Specify the start IP address of the reserved IP pool.

end-ip-address —— Specify the end IP address of the reserved IP pool. Only one IP address will be reserved if the end IP address and the start IP address are the same.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the reserved IP addresses from 192.168.1.1 to 192.168.1.9:

```
Switch(config)# ip dhcp server excluded-address 192.168.1.1 192.168.1.9
```

56.5 ip dhcp server pool

Description

The **ip dhcp server pool** command is used to create the address pool of DHCP Server and enter the dhcp configuration mode. To delete the address pool, please use **no ip dhcp server pool** command.

Syntax

ip dhcp server pool *pool-name*
no ip dhcp server pool *pool-name*

Parameter

pool-name—— Specify the address pool name, ranging from 1 to 32 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the address pool of name POOL1:

```
Switch(config)# ip dhcp server pool POOL1
```

56.6 ip dhcp server ping timeout

Description

The **ip dhcp server ping timeout** command is used to specify the timeout of PING process. To resume the default value, please use **no ip dhcp server ping timeout** command.

Syntax

ip dhcp server ping timeout *value*
no ip dhcp server ping timeout

Parameter

value—— Specify the timeout value, ranging from 100 to 10000ms. The default value is 100ms.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the timeout of PING as 200ms:

```
Switch(config)# ip dhcp server ping timeout 200
```

56.7 ip dhcp server ping packets

Description

The **ip dhcp server ping packets** command is used to specify the number of PING packets sent. If this value is set to 0, the PING process will be disabled. To resume the default value, please use **no ip dhcp server ping packets** command.

Syntax

ip dhcp server ping packets *num*
no ip dhcp server ping packets

Parameter

num — Specify the PING packets' number, ranging from 0 to 10. By default it's 1.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the PING packets' number as 2:

```
Switch(config)# ip dhcp server ping packets 2
```

56.8 ip dhcp client gateway-detect

Description

The **ip dhcp client gateway-detect** command is used to enable the gateway-detect function. When enabled, the device will initiate gateway probing tasks on all VLANs configured with DHCP client mode. To disable this function, please use **no ip dhcp client gateway-detect** command. By default, this function is disabled. Note that the gateway mentioned in this function description is not limited to gateway devices, but refers to the routing gateway obtained by DHCP.

Syntax

ip dhcp client gateway-detect
no ip dhcp client gateway-detect

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the gateway-detect function:

```
Switch(config)# ip dhcp client gateway-detect
```

56.9 network

Description

The **network** command is used to specify the address and subnet of the network pool.

Syntax

network { *network-address subnet-mask* } [*vrf-name*]

Parameter

network-address—— Specify the network address of the pool, with the format A.B.C.D. All the IP addresses in the same subnet are allocatable except the reserved addresses and specific addresses.

subnet-mask—— Specify the subnet mask of the pool, with the format A.B.C.D.

vrf-name—— VRF instance name

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool "product" as 192.168.1.0 255.255.255.0:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# network 192.168.1.0 255.255.255.0 vrf1
```

56.10 range

Description

The **range** command is used to define an allocatable IP address sub-range within the network configured under the DHCP address pool. It further limits the addresses that can be assigned from the pool.

Syntax

range *range-id sip dip*

Parameter

range-id—— Specify the range ID. Valid values are 1 to 8.

sip—— Specify the start IP address of the range, in the format A.B.C.D..

dip—— Specify the end IP address of the range, in the format A.B.C.D.

Command Mode

DHCP Pool Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

After configuring network 192.168.0.0 255.255.255.0, define range 1 to limit address allocation to 192.168.0.10 through 192.168.0.20:

```
Switch(config)# ip dhcp server pool product
Switch(dhcp-config)# network 192.168.1.0 255.255.255.0 vrf1
Switch(dhcp-config)# range 1 192.168.0.10 192.168.0.20
```

56.11 vrf

Description

The **vrf** command is used to modify the vrf instance to which the network segment of a specific address pool belongs.

Syntax

vrf [*vrf-name*]

Parameter

vrf-name—— VRF instance name

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

```
Switch(config)# ip dhcp server pool p1
Switch(dhcp-config)# vrf vrf1
```

56.12 lease

Description

The **lease** command is used to specify the lease time of the address pool.

Syntax

lease *lease-time*

Parameter

lease-time — Specify the lease time of the pool, ranging from 1 to 2880 minutes. The default value is 120 minutes.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the lease time of address pool "product" as 10 minutes:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# lease 10
```

56.13 address hardware-address

Description

The **address hardware-address** command is used to reserve the static address bound with hardware address in the address pool. To delete the binding, please use **no address hardware-address**.

Syntax

address *ip-address* **hardware-address** *hardware-address* **hardware-type**
{ ethernet | ieee802 }

no address *ip-address*

Parameter

ip-address — Specify the static binding IP address.

hardware-address — Specify the hardware address, in the format XX:XX:XX:XX:XX:XX.

ethernet | ieee802 — Specify the hardware type.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Reserve the IP address 192.168.0.10 in the address pool "product" for the device with the MAC address as 5e:4c:a6:31:24:01 and the hardware type as ethernet:

```
Switch(config)# ip dhcp server pool product
Switch(dhcp-config)# address 192.168.0.10 hardware-address
5e:4c:a6:31:24:01 hardware-type ethernet
```

56.14 address client-identifier

Description

The **address client-identifier** command is used to specify the static address bound with client ID in the address pool. To delete the binding, please use **no address** command.

Syntax

```
address ip-address client-identifier client-id[ascii]
no address ip-address
```

Parameter

ip-address — Specify the static binding IP address.
client-id — Specify the client ID, in the format of hex value.
ascii — The client ID is entered with ASCII characters.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Reserve the IP address 192.168.0.10 in the address pool "product" for the device with the client ID as abc in ASCII:

```
Switch(config)# ip dhcp pool product
Switch(dhcp-config)# address 192.168.0.10 client-identifier abc ascii
```

56.15 default-gateway

Description

The **default-gateway** command is used to specify the default gateway of the address pool. To delete the configuration, please use **no default-gateway**.

Syntax

default-gateway *gateway-list*
no default-gateway

Parameter

gateway-list—— Specify the gateway list, with the format of A.B.C.D,E.F.G.H. At most 8 gateways can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool product's default gateways as 192.168.0.1 and 192.168.1.1:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# default-gateway 192.168.0.1,192.168.1.1
```

56.16 dns-server

Description

The **dns-server** command is used to specify the DNS server of the address pool. To delete this configuration, please use **no dns-server** command.

Syntax

dns-server *dns-list*
no dns-server

Parameter

dns-list—— Specify the DNS server list, with the format of A.B.C.D,E.F.G.H. At most 8 DNS servers can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool's DNS servers as 192.168.0.1 and 192.168.1.1:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# dns-server 192.168.0.1,192.168.1.1
```

56.17 ip dns-address

Description

The **ip dns-address** command is used to configure the IPv4 DNS address.

Syntax

ip dns-address primary *primary-dns*

ip dns-address secondary *secondary-dns*

ip dns-address primary secondary *secondary-dns*

no ip dns-address primary

no ip dns-address secondary

no ip dns-address

Parameter

primary-dns——IPv4 address of primary DNS.

secondary-dns——IPv4 address of secondary DNS.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify DNS as 8.8.8.8 and 8.8.4.4:

```
Switch(config)# ip dns-address primary 8.8.8.8 secondary 8.8.4.4
```

56.18 ipv6 dns-address

Description

The **ipv6 dns-address** command is used to configure the IPv6 DNS address.

Syntax

```
ipv6 dns-address primary primary-dns
ipv6 dns-address secondary secondary-dns
ipv6 dns-address primary secondary secondary-dns
no ipv6 dns-address primary
no ipv6 dns-address secondary
no ipv6 dns-address
```

Parameter

primary-dns——IPv6 address of primary DNS.

secondary-dns——IPv6 address of secondary DNS.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify DNS as 2001:4860:4860::8888 and 2001:4860:4860::8844.

```
Switch (config)# ipv6 dns-address primary 2001:4860:4860::8888
```

```
Switch (config)# ipv6 dns-address secondary 2001:4860:4860::8844
```

56.19 netbios-name-server

Description

The **netbios-name-server** command is used to specify the Netbios server's IP address. To delete the Netbios servers, please use **no netbios-name-server** command.

Syntax

```
netbios-name-server NBNS-list
no netbios-name-server
```

Parameter

NBNS-list—— Specify the Netbios server list, with the format of A.B.C.D,E.F.G.H. At most 8 Netbios servers can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool's Netbios servers as 192.168.0.1 and 192.168.1.1:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# netbios-name-server 192.168.0.1,192.168.1.1
```

56.20 netbios-node-type

Description

The **netbios-node-type** command is used to specify the Netbios server's node type. To delete the node type settings, please use **no netbios-node-type** command.

Syntax

netbios-node-type *type*

no netbios-node-type

Parameter

type—— Specify the node type as b-node, h-node, m-node or p-node.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool's Netbios server type as b-node:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# netbios-node-type b-node
```

56.21 next-server

Description

The **next-server** command is used to specify the next DHCP server's address during the DHCP boot process. To delete the next server, please use **no next-server** command.

Syntax

```
next-server ip-address  
next-server
```

Parameter

ip-address—— Specify the IP address of the next server.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the next server's IP address as 192.168.2.1:

```
Switch(config)# ip dhcp server pool product  
Switch(dhcp-config)# next-server 192.168.2.1
```

56.22 domain-name

Description

The **domain-name** command is used to specify the domain name for the DHCP client. To delete the domain name, please use **no domain-name** command.

Syntax

```
domain-name domainname  
no domain-name
```

Parameter

domainname—— Specify the domain name for the DHCP client.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the DHCP client's domain name as edu:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# domain-name edu
```

56.23 bootfile

Description

The **bootfile** command is used to specify the name of the DHCP client's bootfile. To delete the bootfile, please use **no bootfile** command.

Syntax

bootfile *file-name*

no bootfile

Parameter

file-name — Specify the name of the DHCP client's bootfile.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the name of the DHCP client's bootfile as boot1:

```
Switch(config)# ip dhcp server pool product
```

```
Switch(dhcp-config)# bootfile boot1
```


56.24 option

Description

The **option** command is used to specify an option for the DHCP client. To delete the option, please use **no option** command.

Syntax

option code [HEX | IP | STRING] *value*
no option

Parameter

value—— Option value, ranging from 1 to 254.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the option for the DHCP client as IP 1:

```
Switch(config)# ip dhcp server pool product
Switch(dhcp-config)# option code 1
```

56.25 show ip dhcp server status

Description

The **show ip dhcp server status** command is used to display the status of the DHCP service.

Syntax

show ip dhcp server status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the status of DHCP service:

```
Switch(config)# show ip dhcp server status
```

56.26 show ip dhcp server statistics

Description

The **show ip dhcp server statistics** command is used to display the DHCP packets received and sent by DHCP server.

Syntax

```
show ip dhcp server statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics of DHCP packets received and sent by the DHCP server:

```
Switch(config)# show ip dhcp server statistics
```

56.27 show ip dhcp server extend-option

Description

The **show ip dhcp server extend-option** command is used to display the configuration of the remote DHCP servers.

Syntax

```
show ip dhcp server extend-option
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of the remote DHCP servers:

```
Switch(config)# show ip dhcp server extend-option
```

56.28 show ip dhcp server pool

Description

The **show ip dhcp server pool** command is used to display the configuration of the address pool.

Syntax

```
show ip dhcp server pool
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured address pool:

```
Switch(config)# show ip dhcp server pool
```

56.29 show ip dhcp server excluded-address

Description

The **show ip dhcp server excluded-address** command is used to display the configuration of reserved addresses.

Syntax

```
show ip dhcp server excluded-address
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured reserved addresses:

```
Switch(config)# show ip dhcp server excluded-address
```

56.30 show ip dhcp server manual-binding

Description

The **show ip dhcp server manual-binding** command is used to display the configuration of static binding address.

Syntax

```
show ip dhcp server manual-binding
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured static binding address:

```
Switch(config)# show ip dhcp server manual-binding
```

56.31 show ip dhcp server binding

Description

The **show ip dhcp server binding** command is used to display the binding entries.

Syntax

```
show ip dhcp server binding [ ip ip-address ]
```

Parameter

ip-address—— Specify the binding IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the address binding entries:

```
Switch(config)# show ip dhcp server binding
```

56.32 clear ip dhcp server statistics

Description

The **clear ip dhcp server statistics** command is used to clear the statistics information of DHCP packets.

Syntax

```
clear ip dhcp server statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the packet statistics:

```
Switch(config)# clear ip dhcp server statistics
```

56.33 clear ip dhcp server binding

Description

The **clear ip dhcp server binding** command is used to clear the binding information.

Syntax

```
clear ip dhcp server binding [ ip-address ]
```

Parameter

ip-address — Specify the binding IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear all the binding addresses:

```
Switch(config)# clear ip dhcp server binding
```

Chapter 57 DHCPv6 Server Commands

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) is a network configuration protocol for hosts on TCP/IP networks, and it provides a framework for distributing configuration information to hosts. DHCPv6 server assigns IPv6 addresses from specified address pools on a switch or router to DHCPv6 clients and manages them.

57.1 ipv6 dhcp server

Description

The **ipv6 dhcp server** command is used to enable DHCPv6 server globally. After DHCPv6 server is enabled globally, you must also enable DHCPv6 server on the interface and configure an address pool for DHCPv6 server to take effect. Disabling DHCPv6 server globally also disables DHCPv6 server on all interfaces. To disable this function, please use **no ipv6 dhcp server** command.

Syntax

ipv6 dhcp server
no ipv6 dhcp server

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable DHCPv6 server globally:

```
Switch(config)# ipv6 dhcp server
```

57.2 ipv6 dhcp server allow-hint

Description

The **ipv6 dhcp server allow-hint** command is used to specify that the DHCPv6 server supports allocating addresses/prefixes based on the address, prefix, and prefix length requested in the DHCPv6 client hint option. The server attempts to allocate the requested values with priority. If the requested values are out of the pool range or already assigned to another client, the server ignores the hint option and allocates other available prefixes. To restore to the default setting, please use **no ipv6 dhcp server allow-hint** command.

Syntax

```
ipv6 dhcp server allow-hint
no ipv6 dhcp server allow-hint
```

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable DHCPv6 server allow-hint globally:

```
Switch(config)# ipv6 dhcp server allow-hint
```

57.3 ipv6 dhcp server preference

Description

The **ipv6 dhcp server preference** command is used to configure the server preference value carried in DHCPv6 Advertise messages. DHCPv6 clients select the server with the highest preference value for IPv6 address or prefix allocation. To restore to the default setting, please use **no ipv6 dhcp server preference** command.

Syntax

ipv6 dhcp server preference *preference*

no ipv6 dhcp server preference

Parameter

preference—— Server preference value in Advertise messages. Valid values are 0 to 255. Default is 0.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the global DHCPv6 server Advertise preference to 255:

```
Switch(config)# ipv6 dhcp server preference 255
```

57.4 ipv6 dhcp server rapid-commit

Description

The **ipv6 dhcp server rapid-commit** command is used to enable Rapid Commit on DHCPv6 server to speed up the address/prefix allocation process. This function takes effect only if the DHCPv6 client also supports Rapid Commit. To disable this function, please use **no ipv6 dhcp server rapid-commit** command.

Syntax

ipv6 dhcp server rapid-commit

no ipv6 dhcp server rapid-commit

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable DHCPv6 server rapid-commit globally:

```
Switch(config)# ipv6 dhcp server rapid-commit
```

57.5 ipv6 dhcp server unicast

Description

The **ipv6 dhcp server unicast** command is used to enable unicast communication between the DHCPv6 server and clients during the renew process. To disable this function, please use **no ipv6 dhcp server unicast** command.

Syntax

ipv6 dhcp server unicast
no ipv6 dhcp server unicast

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable DHCPv6 server unicast globally:

```
Switch(config)# ipv6 dhcp server unicast
```

57.6 ipv6 dhcp server pool

Description

The **ipv6 dhcp server pool** command is used to create a DHCPv6 address pool. A maximum of 64 pools are supported. To remove this configuration, please use **no ipv6 dhcp server pool** command.

Syntax

```
ipv6 dhcp server pool pool-name  
no ipv6 dhcp server pool pool-name
```

Parameter

pool-name — Pool name. The maximum length is 32 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a DHCPv6 pool named office:

```
Switch(config)# ipv6 dhcp server pool office
```

57.7 network

Description

The **network** command is used to configure the address range for address allocation in a DHCPv6 pool. You can configure the range by specifying a prefix/prefix-length, or by specifying a start address and an end address. Multiple networks can be configured in a single pool. A maximum of 64 networks are supported per pool, and networks must not overlap or contain each other. If a network is removed by using the **no network** command, the pool automatically clears the binding information for addresses that were allocated from that network.

Syntax

```
network {prefix} [end]  
no network {prefix} [end]
```

Parameter

prefix — IPv6 prefix/prefix-length, or the start IPv6 address.
end — End IPv6 address.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the pool address range by start address and end address:

```
Switch(dhcp6-config)# network 2001::100 2001::abc
```

Configure the pool address range by prefix and prefix length:

```
Switch(dhcp6-config)# network 2001::/64
```

57.8 prefix-delegation

Description

The **prefix-delegation** command is used to configure the prefix delegation range in a DHCPv6 pool. After this attribute is configured, the pool can provide Prefix Delegation. As long as the pool is applied to an interface, Prefix Delegation can work without configuring an address from the same prefix on the interface. A maximum of 64 delegated prefixes are supported per pool, and prefixes must not overlap or contain each other. To remove this configuration, please use the **no prefix-delegation** command.

Syntax

prefix-delegation *prefix* [*assignLen*] [*description*]

no prefix-delegation *prefix* [*assignLen*] [*description*]

Parameter

prefix—— IPv6 prefix/prefix-length. The prefix address can be entered without being masked.

assignLen—— Delegated prefix length. It cannot be smaller than the prefix length. Default is 64.

description—— Description for the delegated prefix.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure prefix delegation for the pool:

```
Switch(dhcp6-config)# prefix-delegation 2005::/53 64
```

57.9 address

Description

The **address** command is used to configure a static binding entry so that the DHCPv6 server assigns a specified IPv6 address to a specified client (DUID). The reserved address is not assigned to clients with a different DUID. If the server has reached the maximum number of allocated addresses, the server will not assign the address even if the client DUID matches. A maximum of 1000 reserved addresses are supported per pool. To remove this configuration, please use the **no address** command.

Syntax

address *address duid*

no address *address duid*

Parameter

address — Reserved IPv6 address.

duid — DHCPv6 client DUID. It must match the DUID carried in the client Solicit message.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Assign a reserved address to a DHCPv6 client:

```
Switch(dhcp6-config)# address 2002::100:a 00030001000c29c45e01
```

57.10 description

Description

The **description** command is used to configure a description for the DHCPv6 address pool. To remove the description, use the **no description** command.

Syntax

description *description*
no description

Parameter

description—— Pool description. The maximum length is 128 characters.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a description for the pool:

```
Switch(dhcp6-config)# description "This pool is used for reception room"
```

57.11 dns-domain-name

Description

The **dns-domain-name** command is used to configure a DNS domain suffix for the DHCPv6 pool. A maximum of 64 domain suffixes are supported per pool. To remove a configured domain suffix, use the **no dns-domain-name** command.

Syntax

dns-domain-name *domain*
no dns-domain-name *domain*

Parameter

domain—— DNS domain suffix. The maximum length is 64 characters. It must not start or end with ".", must not contain consecutive ".", and must not start with "-". Special characters other than "." and "-" are not allowed.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a DNS domain suffix:

```
Switch(dhcp6-config)# dns-domain-name PC1
```

57.12 dns-server

Description

The **dns-server** command is used to configure DNS server IPv6 addresses for DHCPv6 clients. A maximum of 64 DNS server addresses are supported per pool. To remove a configured DNS server address, use the **no dns-server** command.

Syntax

dns-server *address*

no dns-server *address*

Parameter

address — DNS server IPv6 address.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Notify DHCPv6 clients of the DNS server address:

```
Switch(dhcp6-config)# dns-server 2001:4860:4860::8888
```

57.13 excluded-address

Description

The **excluded-address** command is used to configure IPv6 addresses or address ranges that are excluded from automatic allocation. A maximum of 100 excluded address ranges are supported per pool. To remove an excluded range, use the **no excluded-address** command.

Syntax

excluded-address *start end*
no excluded-address *start end*

Parameter

start—— Start IPv6 address to be excluded from allocation.
end—— End IPv6 address to be excluded from allocation.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Exclude a specific address range from allocation:

```
Switch(dhcp6-config)# excluded-address 2001::100 2001::abc
```

57.14 link

Description

The **link** command is used to configure a pool link prefix, which is used as a criterion for selecting a DHCPv6 pool when an interface is not explicitly bound to a pool. The matching priority of link is lower than network. If the interface cannot match a suitable pool by network, the switch matches a pool by link. To remove the link prefix, use the **no link** command.

Syntax

link *prefix*
no link *prefix*

Parameter

prefix—— IPv6 prefix/prefix-length.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a pool link prefix:

```
Switch(dhcp6-config)# link 2005::/64
```

57.15 nis-domain-name

Description

The **nis-domain-name** command is used to configure a NIS domain suffix for DHCPv6 clients. A maximum of 64 NIS domain suffixes are supported per pool. To remove a configured NIS domain suffix, use the **no nis-domain-name** command.

Syntax

nis-domain-name *domain*

no nis-domain-name *domain*

Parameter

domain—— NIS domain suffix. The maximum length is 64 characters. It must not start or end with ".", must not contain consecutive ".", and must not start with "-". Special characters other than "." and "-" are not allowed.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the NIS domain suffix as "PC1":

```
Switch(dhcp6-config)# nis-domain-name PC1
```

57.16 nis-server

Description

The **nis-server** command is used to configure NIS server IPv6 addresses for DHCPv6 clients. A maximum of 64 NIS server addresses are supported per pool. To remove a configured NIS server address, use the **no nis-server** command.

Syntax

nis-server *address*

no nis-server *address*

Parameter

address — NIS server IPv6 address.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a NIS server address:

```
Switch(dhcp6-config)# nis-server 2001::100
```

57.17 nisp-domain-name

Description

The **nisp-domain-name** command is used to configure a NISP domain suffix for DHCPv6 clients. A maximum of 64 NISP domain suffixes are supported per pool. To remove a configured NISP domain suffix, use the **no nisp-domain-name** command.

Syntax

nisp-domain-name *domain*

no nisp-domain-name *domain*

Parameter

domain—— NISP domain suffix. The maximum length is 64 characters. It must not start or end with ".", must not contain consecutive ".", and must not start with "-". Special characters other than "." and "-" are not allowed.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the NISP domain suffix as "PC1":

```
Switch(dhcp6-config)# nisp-domain-name PC1
```

57.18 nisp-server

Description

The **nisp-server** command is used to configure NISP server IPv6 addresses for DHCPv6 clients. A maximum of 64 NISP server addresses are supported per pool. To remove a configured NISP server address, use the **no nisp-server** command.

Syntax

nisp-server *address*
no nisp-server *address*

Parameter

address—— NISP server IPv6 address.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a NISP server address:

```
Switch(dhcp6-config)# nisp-server 2001::100
```

57.19 preferred-lifetime

Description

The **preferred-lifetime** command is used to configure the preferred lifetime of the delegated prefix. To remove the configuration, use the **no preferred-lifetime** command.

Syntax

preferred-lifetime *lifetime*

no preferred-lifetime *lifetime*

Parameter

lifetime — Preferred lifetime value. Valid values are 60 to 172799999. Default is 86400.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the preferred lifetime to 2000:

```
Switch(dhcp6-config)# preferred-lifetime 2000
```

57.20 valid-lifetime

Description

The **valid-lifetime** command is used to configure the valid lifetime of the delegated prefix. To remove the configuration, use the **no valid-lifetime** command.

Syntax

valid-lifetime *lifetime*

no valid-lifetime *lifetime*

Parameter

lifetime — Valid lifetime value. Valid values are 60 to 172799999. Default is 172800.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the valid lifetime to 2000:

```
Switch(dhcp6-config)# valid-lifetime 2000
```

57.21 sip-domain-name

Description

The **sip-domain-name** command is used to configure a SIP domain suffix for DHCPv6 clients. A maximum of 64 SIP domain suffixes are supported per pool. To remove a configured SIP domain suffix, use the **no sip-domain-name** command.

Syntax

sip-domain-name *domain*

no sip-domain-name *domain*

Parameter

domain—— SIP domain suffix. The maximum length is 64 characters. It must not start or end with ".", must not contain consecutive ".", and must not start with "-". Special characters other than "." and "-" are not allowed.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a SIP domain suffix as PC1:

```
Switch(dhcp6-config)# sip-domain-name PC1
```

57.22 sip-server

Description

The **sip-server** command is used to configure SIP server IPv6 addresses for DHCPv6 clients. A maximum of 64 SIP server addresses are supported per pool. To remove a configured SIP server address, use the **no sip-server** command.

Syntax

sip-server *address*
no sip-server *address*

Parameter

address — SIP server IPv6 address.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a SIP server address:

```
Switch(dhcp6-config)# sip-server 2001::100
```

57.23 sntp-server

Description

The **sntp-server** command is used to configure SNTP server IPv6 addresses for DHCPv6 clients. A maximum of 64 SNTP server addresses are supported per pool. To remove a configured SNTP server address, use the **no sntp-server** command.

Syntax

sntp-server *address*
no sntp-server *address*

Parameter

address — SNTP server IPv6 address.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a SIP server address:

```
Switch(dhcp6-config)# sntp-server 2001::100
```

57.24 vrf

Description

The **vrf** command is used to bind the DHCPv6 pool to a VRF instance. When the VRF is changed, the pool automatically clears all binding entries. To remove the VRF binding, use the **no vrf** command.

Syntax

vrf *vrfName*

no vrf

Parameter

vrfName — VRF instance name.

Command Mode

DHCPv6 Pool Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Bind the pool to VRF office:

```
Switch(dhcp6-config)# vrf office
```

57.25 ipv6 dhcp server

Description

The **ipv6 dhcp server** command is used to enable DHCPv6 server on an interface. If no pool is bound to the interface, the switch automatically searches for and uses a DHCPv6 pool that matches the interface IPv6 address for address allocation. To disable this function, use the **no ipv6 dhcp server** command.

Syntax

ipv6 dhcp server
no ipv6 dhcp server

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable DHCPv6 server on interface VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp server
```

57.26 ipv6 dhcp server allow-hint

Description

The **ipv6 dhcp server allow-hint** command specifies that the DHCPv6 server supports allocating addresses/prefixes based on the address, prefix, and prefix length requested in the DHCPv6 client hint option. The server attempts to allocate the requested values with priority. If the requested values are out of the pool range or already assigned to another client, the server ignores the hint option and allocates other available prefixes. To disable this function, use the **no ipv6 dhcp server allow-hint** command.

Syntax

ipv6 dhcp server allow-hint
no ipv6 dhcp server allow-hint

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable allow-hint on interface VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp server allow-hint
```

57.27 ipv6 dhcp server preference

Description

The **ipv6 dhcp server preference** command is used to configure the server preference value carried in DHCPv6 Advertise messages on an interface. DHCPv6 clients select the server with the highest preference value for IPv6 address or prefix allocation. The default value is 0. To disable this function, use the **no ipv6 dhcp server preference** command.

Syntax

ipv6 dhcp server preference *preference*
no ipv6 dhcp server preference

Parameter

preference — Server preference value in Advertise messages. Valid values are 0 to 255. Default is 0.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the DHCPv6 server preference to 255 on interface VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp server preference 255
```

57.28 ipv6 dhcp server rapid-commit

Description

The **ipv6 dhcp server rapid-commit** command is used to enable Rapid Commit on DHCPv6 server on an interface to speed up the address/prefix allocation process. This function takes effect only if the DHCPv6 client also supports Rapid Commit. To disable this function, use the **no ipv6 dhcp server rapid-commit** command.

Syntax

```
ipv6 dhcp server rapid-commit
no ipv6 dhcp server rapid-commit
```

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable Rapid Commit on interface VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp server rapid-commit
```

57.29 ipv6 dhcp server unicast

Description

The **ipv6 dhcp server unicast** command is used to enable unicast communication between the DHCPv6 server and clients during the renew process on an interface. To disable this function, use the **no ipv6 dhcp server unicast** command.

Syntax

ipv6 dhcp server unicast
no ipv6 dhcp server unicast

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable unicast communication during renew on interface VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp server unicast
```

57.30 ipv6 dhcp server pool

Description

The **ipv6 dhcp server pool** command is used to bind a DHCPv6 pool to an interface. If no pool is bound, the interface automatically matches a suitable pool from all configured pools for address allocation. After a pool is bound, the interface uses the specified pool for address allocation. To disable this function, use the **no ipv6 dhcp server pool** command.

Syntax

ipv6 dhcp server pool *pool-name*
no ipv6 dhcp server pool

Parameter

pool-name — DHCPv6 pool name to be bound to the interface.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Bind DHCPv6 pool pool_1 to interface VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp server pool pool_1
```

57.31 show ipv6 dhcp server binding

Description

The **show ipv6 dhcp server binding** command is used to display all addresses/prefixes allocated by the DHCPv6 server and the corresponding client binding information, including the address/prefix, client DUID, pool name, VRF, binding type, and remaining lease time.

Syntax

```
show ipv6 dhcp server binding
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all binding entries in the database:

```
Switch(config)# show ipv6 dhcp server binding
```

57.32 show ipv6 dhcp server binding summary

Description

The **show ipv6 dhcp server binding summary** command is used to display the number of allocated addresses for all DHCPv6 pools.

Syntax

show ipv6 dhcp server binding summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display allocation statistics for all DHCPv6 pools in the database:

```
Switch(config)# show ipv6 dhcp server binding summary
```

57.33 show ipv6 dhcp server pool

Description

The **show ipv6 dhcp server pool** command is used to display the configuration of all created DHCPv6 pools.

Syntax

show ipv6 dhcp server pool

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all created DHCPv6 pools in the database:

```
Switch(config)# show ipv6 dhcp server pool
```

57.34 show ipv6 dhcp server statistics

Description

The **show ipv6 dhcp server statistics** command is used to display DHCPv6 server packet statistics.

Syntax

show ipv6 dhcp server statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display DHCPv6 server packet statistics:

```
Switch(config)# show ipv6 dhcp server statistics
```

57.35 show ipv6 dhcp server status

Description

The **show ipv6 dhcp server status** command is used to display global DHCPv6 server status and DHCPv6 server information for all interfaces.

Syntax

show ipv6 dhcp server status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display global and per-interface DHCPv6 server status:

```
Switch(config)# show ipv6 dhcp server status
```

57.36 clear ipv6 dhcp server binding

Description

The **clear ipv6 dhcp server binding** command is used to clear DHCPv6 server binding information for a specified IPv6 address or for all addresses. If *vrfName* is specified, only bindings in the specified VRF are cleared.

Syntax

```
clear ipv6 dhcp server binding [ipv6][vrfName]
```

Parameter

ipv6—— IPv6 address of the binding entry to be cleared. If not specified, all binding entries are cleared.

vrfName—— VRF name of the binding entry to be cleared.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear all binding entries:

```
Switch# clear ipv6 dhcp server binding
```

Clear the binding entry for a specific IPv6 address:

```
Switch# clear ipv6 dhcp server binding 2001::1
```

Clear the binding entry for a specific IPv6 address in VRF vrf1:

```
Switch# clear ipv6 dhcp server binding 2001::1 vrf1
```

57.37 clear ipv6 dhcp server statistics

Description

The **clear ipv6 dhcp server statistics** command is used to clear DHCPv6 server packet statistics.

Syntax

clear ipv6 dhcp server statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear DHCPv6 server packet statistics:

```
Switch# clear ipv6 dhcp server statistics
```


Chapter 58 RA Server Commands

RA (Router Advertisement) Server enables an interface to periodically send IPv6 Router Advertisement messages to hosts on the local link. These RA messages provide key IPv6 network parameters, such as the default gateway, on-link prefixes, and host configuration flags (for example, SLAAC vs. DHCPv6). With RA Server enabled, hosts can automatically learn IPv6 routing and addressing information without manual configuration. Administrators can also tune RA behavior by configuring options such as advertisement interval, router lifetime, hop limit, reachable time, retransmit timer, advertised prefixes, and DNS information (RDNSS/DNSSL) to match the network's deployment and policy requirements.

58.1 ipv6 nd ra suppress

Description

The **ipv6 nd ra suppress** command is used to enable or disable RA (Router Advertisement) sending on the interface. RA sending is disabled by default after an interface is created. To disable this function, use the **no ipv6 nd ra suppress** command.

Syntax

ipv6 nd ra suppress
no ipv6 nd ra suppress

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable RA on interface VLAN 1:

```
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 nd ra suppress
```

58.2 ipv6 nd ra dns-server

Description

The **ipv6 nd ra dns-server** command is used to advertise recursive DNS server addresses to clients through RA messages. A maximum of two DNS servers are supported, and they share the same lifetime. To disable this function, use the **no ipv6 nd ra dns-server** command.

Syntax

ipv6 nd ra dns-server *address* **lifetime** *lifetime*

no ipv6 nd ra dns-server [*address* | *lifetime*]

Parameter

address — DNS server IPv6 address.

lifetime — DNS server lifetime.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a recursive DNS server address and lifetime:

```
Switch(config-if)# ipv6 nd ra dns-server 2001:4860:4860::8888 lifetime  
2000
```

Reset the DNS server lifetime to the default value:

```
Switch(config-if)# no ipv6 nd ra dns-server lifetime
```

Stop advertising the specified DNS server:

```
Switch(config-if)# no ipv6 nd ra dns-server 2001:4860:4860::8888
```

58.3 ipv6 nd ra dns-suffix

Description

The **ipv6 nd ra dns-suffix** command is used to advertise a DNS search list (domain suffix list) to clients through RA messages. To disable this function, use the **no ipv6 nd ra dns-suffix** command.

Syntax

ipv6 nd ra dns-suffix *domain* **lifetime** *lifetime*

no ipv6 nd ra dns-suffix [*lifetime*]

Parameter

domain—— DNS domain suffix.

lifetime—— DNS domain suffix lifetime.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure a DNS suffix and lifetime:

```
Switch(config-if)# ipv6 nd ra dns-suffix Google lifetime 2000
```

Reset the DNS suffix lifetime to the default value:

```
Switch(config-if)# no ipv6 nd ra dns-suffix lifetime
```

Stop advertising the DNS suffix:

```
Switch(config-if)# no ipv6 nd ra dns-suffix
```

58.4 ipv6 nd ra hop-limit

Description

The **ipv6 nd ra hop-limit** command is used to configure the maximum Hop Limit value in RA messages. To disable this function, use the **no ipv6 nd ra hop-limit** command.

Syntax

ipv6 nd ra hop-limit *limit*

no ipv6 nd ra hop-limit

Parameter

limit—— Maximum hop limit value in RA messages. Valid values are 0 to 255. Default is 64.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the RA hop limit to 10:

```
Switch(config-if)# ipv6 nd ra hop-limit 10
```

58.5 ipv6 nd ra interval

Description

The **ipv6 nd ra interval** command is used to configure the maximum and minimum advertisement intervals for RA messages. To disable this function, use the **no ipv6 nd ra interval** command.

Syntax

ipv6 nd ra interval *max-interval min-interval*

no ipv6 nd ra interval

Parameter

max-interval—— Maximum RA advertisement interval. Valid values are 4 to 1800 seconds. Default is 600.

min-interval—— Minimum RA advertisement interval. Valid values are 3 to 1350 seconds. Default is 200.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the RA advertisement intervals:

```
Switch(config-if)# ipv6 nd ra interval 4 3
```

58.6 ipv6 nd ra lifetime

Description

The **ipv6 nd ra lifetime** command is used to configure the router lifetime value in RA messages. RA clients must refresh router information after the lifetime expires. To disable this function, use the **no ipv6 nd ra lifetime** command.

Syntax

ipv6 nd ra lifetime *lifetime*
no ipv6 nd ra lifetime

Parameter

lifetime — RA lifetime value. Valid values are 600 to 9000 seconds. The default value is three times the maximum advertisement interval.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the RA lifetime to 2000 seconds:

```
Switch(config-if)# ipv6 nd ra lifetime 2000
```

58.7 ipv6 nd ra managed-config-flag

Description

The **ipv6 nd ra managed-config-flag** command is used to set the M (Managed) flag in RA messages. When enabled, hosts are informed to use stateful address configuration (for example, DHCPv6) to obtain addresses. When disabled, hosts use Stateless Address Autoconfiguration (SLAAC). To disable this function, use the **no ipv6 nd ra managed-config-flag** command.

Syntax

ipv6 nd ra managed-config-flag

no ipv6 nd ra managed-config-flag

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the M flag to indicate that hosts should use DHCPv6 to obtain addresses:

```
Switch(config-if)# ipv6 nd ra managed-config-flag
```

58.8 ipv6 nd ra other-config-flag

Description

The **ipv6 nd ra other-config-flag** command is used to set the O (Other Configuration) flag in RA messages. When enabled, hosts are informed to use stateful configuration (for example, DHCPv6) to obtain information other than IPv6 addresses. When disabled, hosts use stateless configuration to obtain information other than IPv6 addresses. To disable this function, use the **no ipv6 nd ra other-config-flag** command.

Syntax

ipv6 nd ra other-config-flag

no ipv6 nd ra other-config-flag

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the O flag in RA messages:

```
Switch(config-if)# ipv6 nd ra other-config-flag
```

58.9 ipv6 nd ra mtu

Description

The **ipv6 nd ra mtu** command is used to configure the MTU option in RA messages. If this option is not configured, the interface MTU is used by default. If the interface MTU is out of the allowed range, the default value of this command is used. To disable this function, use the **no ipv6 nd ra mtu** command.

Syntax

ipv6 nd ra mtu *mtu*

no ipv6 nd ra mtu

Parameter

mtu—— MTU value advertised in RA messages. Valid values are 1280 to 1500. Default is 1500.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the RA MTU option to 1400:

```
Switch(config-if)# ipv6 nd ra mtu 1400
```

58.10 ipv6 nd ra preference

Description

The **ipv6 nd ra preference** command is used to configure the default router preference in RA messages. A higher preference makes the router more likely to be selected as the default router.

Syntax

ipv6 nd ra preference { high | medium | low }

Parameter

high — Set the router preference to high.

medium — Set the router preference to medium. This is the default.

low — Set the router preference to low.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Set the default router preference in RA messages to high:

```
Switch(config-if)# ipv6 nd ra preference high
```

58.11 ipv6 nd ra reachable-time

Description

The **ipv6 nd ra reachable-time** command is used to configure the reachable time value in RA messages. Hosts use this value as the time (in milliseconds) that a neighbor is considered reachable after receiving a reachability confirmation. To disable this function, use the **no ipv6 nd ra reachable-time** command.

Syntax

ipv6 nd ra reachable-time *time*

no ipv6 nd ra reachable-time

Parameter

time — Reachable time value advertised in RA messages. Valid values are 0 to 3600000. Default is 0.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Set the reachable time to 2000:

```
Switch(config-if)# ipv6 nd ra reachable-time 2000
```

58.12 ipv6 nd ra retrans-timer

Description

The **ipv6 nd ra retrans-timer** command is used to configure the retransmission timer value in RA messages. Hosts use this value as the time interval (in milliseconds) between retransmitted Neighbor Solicitation messages, such as for address resolution or DAD. To disable this function, use the **no ipv6 nd ra retrans-timer** command.

Syntax

ipv6 nd ra retrans-timer *time*

no ipv6 nd ra retrans-timer

Parameter

time — Retransmission timer value advertised in RA messages. Valid values are 0 to 4294967295. Default is 0.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Set the retransmission timer to 2000:

```
Switch(config-if)# ipv6 nd ra retrans-timer 2000
```

58.13 ipv6 nd ra prefix

Description

The **ipv6 nd ra prefix** command is used to configure prefixes advertised in RA messages. By default, after RA sending is enabled on an interface, the switch automatically advertises the prefix of the interface IPv6 address. If a configured prefix overlaps with the interface prefix, the configured prefix takes precedence. To disable this function, use the **no ipv6 nd ra prefix** command.

Syntax

```
ipv6 nd ra prefix {default | prefix} [valid-time] [preferred-time]  
[no-autoconfig | autoconfig] [off-link | on-link]  
no ipv6 nd ra prefix {default | prefix}
```

Parameter

default — Specify the default router address.

prefix — Specify the IPv6 prefix/prefix-length to be advertised.

valid-time — Prefix valid lifetime. Valid values are 0 to 172799999. Default is 2592000.

preferred-time — Prefix preferred lifetime. Valid values are 0 to 172799999. Default is 604800. The value must not exceed valid-time.

no-autoconfig — Clear the A (Autonomous) flag to disable host address autoconfiguration. The A flag is enabled by default.

autoconfig — Set the A (Autonomous) flag to enable host address autoconfiguration.

off-link — Clear the O (Other Configuration) flag to indicate the prefix is not on-link. The O flag is enabled by default.

on-link — Set the O (Other Configuration) flag to indicate the prefix is on-link.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Advertise default router information and set the preferred lifetime to 2000:

```
Switch(config-if)# ipv6 nd ra prefix default 2592000 2000
```

Advertise a custom prefix, set the preferred lifetime to 2000, and disable autoconfiguration (clear A flag):

```
Switch(config-if)# ipv6 nd ra prefix 2001::/64 2592000 2000 no-autoconfig
```

Stop advertising default router information:

```
Switch(config-if)# no ipv6 nd ra prefix default
```

Stop advertising the custom prefix:

```
Switch(config-if)# no ipv6 nd ra prefix 2001::/64
```

58.14 show ipv6 nd ra

Description

The **show ipv6 nd ra** command is used to display RA server configuration for all interfaces.

Syntax

```
show ipv6 nd ra
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display RA server configuration for all interfaces:

```
Switch# show ipv6 nd ra
```

Chapter 59 DHCP Relay Commands

A DHCP Relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. DHCP Relay forward requests and replies between clients and servers when they are not on the same physical subnet.

59.1 service dhcp relay

Description

The **service dhcp relay** command is used to enable DHCP Relay function globally. To disable DHCP Relay function, please use **no service dhcp relay** command.

Syntax

service dhcp relay
no service dhcp relay

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP Relay function globally:

```
Switch(config)# service dhcp relay
```

59.2 ip dhcp relay hops

Description

The **ip dhcp relay hops** command is used to specify the maximum hops (DHCP Relay agent) that the DHCP packets can be relayed. To restore the default value, please use **no service dhcp relay hops** command.

Syntax

ip dhcp relay hops *hops*
no ip dhcp relay hops

Parameter

hops——Specify the maximum hops (DHCP Relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped. The valid value ranges from the 1 to 16, and the default value is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of relay hops as 6:

```
Switch(config)# ip dhcp relay hops 6
```

59.3 ip dhcp relay time

Description

The **ip dhcp relay time** command is used to specify the DHCP relay time threshold. DHCP relay time is the time elapsed since client began address acquisition or renewal process. When the elapsed time of the DHCP packet is greater than the value set here, the DHCP packet will be dropped by the switch. To restore the default value, please use **no service dhcp relay time** command.

Syntax

ip dhcp relay time *time*

no ip dhcp relay time

Parameter

time——Specify the DHCP relay time threshold. The valid value ranges from 1 to 65535. The default value is 0, which means the switch will not examine this field of the DHCP packets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DHCP Relay time as 30 seconds:

```
Switch(config)# ip dhcp relay time 30
```

59.4 ip helper-address

Description

The **ip helper-address** command is used to add DHCP Server address to the Layer 3 interface. To delete the server address, please use **no ip helper-address** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

```
ip helper-address {ip-address} [vrf-name]  
no ip helper-address [ip-address] [vrf-name]
```

Parameter

vrf-name — vrf-name.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add DHCP Server address 192.168.2.1 to interface VLAN 1:

```
Switch(config)# interface vlan 1  
Switch(config-if)# ip helper-address 192.168.2.1 vrf1
```

59.5 ip dhcp relay information option

Description

The **ip dhcp relay information option** command is used to enable option 82 support in DHCP Relay. To disable this function, please use **no ip dhcp relay information option** command.

Syntax

ip dhcp relay information option
no ip dhcp relay information option

Command Mode

Interface Configuration Mode (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option 82 support in DHCP Relay for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#ip dhcp relay information option
```

59.6 ip dhcp relay information strategy

Description

The **ip dhcp relay information strategy** command is used to specify the operation for the Option 82 field of the DHCP request packets from the Host. To restore to the default option, please use **no ip dhcp relay information strategy** command.

Syntax

ip dhcp relay information strategy { drop | keep | replace }
no ip dhcp relay information strategy

Parameter

drop | keep | replace — The operations for Option 82 field of the DHCP request packets from the Host. The default operation is keep.

drop: Discard the packet with the Option 82 field.

keep: Keep the Option 82 field in the packet.

replace: Replace the option 82 field with the system option defined by the switch.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the option 82 strategy as replace to replace the Option 82 field with the local parameter on receiving the DHCP request packet for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# ip dhcp relay information strategy replace
```

59.7 ip dhcp relay information format

Description

The **ip dhcp relay information format** command is used to select the format of option 82 sub-option value field. To restore to the default option, please use **no ip dhcp relay information format** command.

Syntax

ip dhcp relay information format { normal | private }

no ip dhcp relay information format

Parameter

normal | private — The format type of option 82 sub-option value field.

normal: Indicates that the format of sub-option value field is TLV (type-length-value).

private: Indicates that the format of sub-option value field is the value you configure for the related sub-option.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Select the format of option 82 sub-option value field as TLV (type-length-value) for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#ip dhcp relay information format normal
```

59.8 ip dhcp relay information circuit-id

Description

The **ip dhcp relay information circuit-id** command is used to specify the custom circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp relay information circuit-id** command.

Syntax

```
ip dhcp relay information circuit-id circuitID
no ip dhcp relay information circuit-id
```

Parameter

circuitID—— Specify the circuit ID, ranging from 1 to 128 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the circuit ID as "TP-Link" for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)# ip dhcp relay information circuit-id TP-Link
```

59.9 ip dhcp relay information remote-id

Description

The **ip dhcp relay information remote-id** command is used to specify the custom remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp relay information remote-id** command.

Syntax

ip dhcp relay information remote-id *remoteID*
no ip dhcp relay information remote-id

Parameter

remoteID—— Specify the remote ID, ranging from 1 to 128 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the remote ID as "TP-Link" for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)# ip dhcp relay information remote-id TP-Link
```

59.10 ip dhcp relay default-interface

Description

The **ip dhcp relay default-interface** command is used to configure default relay agent interface. When the switch works at DHCP VLAN Relay mode and there is no IP interface in the VLAN, the switch uses the IP of default relay agent interface to fill in the relay agent IP address field of DHCP packets. To delete the default relay agent interface use **no ip dhcp relay default-interface**.

Syntax

ip dhcp relay default-interface
no ip dhcp relay default-interface

Command mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure interface VLAN 1 as the default relay agent interface:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip dhcp relay default-interface
```

59.11 ip dhcp relay vlan

Description

The **ip dhcp relay vlan** command is used to add DHCP server address to specified VLAN. If there is an IP interface in the VLAN and it has configured a DHCP server address at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets. To delete the DHCP server address use **no ip dhcp relay vlan**. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

ip dhcp relay vlan *{vid}* **helper-address** *{ip-address}* [*vrf-name*]
no ip dhcp relay vlan *{vid}* **helper-address** [*ip-address*] [*vrf-name*]

Parameter

vid—— VLAN ID.
ip-address—— DHCP Server address.
vrf-name—— VRF instance name.

Command mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add DHCP server address 192.168.2.1 to VLAN 1:

```
Switch(config)# ip dhcp relay vlan 1 helper-address 192.168.2.1 vrf1
```

59.12 show ip dhcp relay

Description

The **show ip dhcp relay** command is used to display the global status and Option 82 configuration of DHCP Relay.

Syntax

```
show ip dhcp relay
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

```
Switch(config)# show ip dhcp relay
```

Chapter 60 DHCPV6 Relay Commands

A DHCPV6 Relay agent is a Layer 3 device that forwards DHCPV6 packets between clients and servers. DHCPV6 Relay forward requests and replies between clients and servers when they are not on the same physical subnet.

60.1 ipv6 dhcp relay

Description

The **ipv6 dhcp relay** command is used to enable DHCPV6 Relay function globally. To disable DHCPV6 Relay function, please use **no ipv6 dhcp relay** command.

Syntax

ipv6 dhcp relay
no ipv6 dhcp relay

Command Mode

Global Configuration Mode
Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCPV6 Relay function globally:

```
Switch(config)# ipv6 dhcp relay
```

60.2 ipv6 dhcp relay vlan 1 helper-address

Description

The **ipv6 dhcp relay vlan 1 helper-address** command is used to add DHCPV6 Server address to the Layer 3 interface. To delete the server address, please use **no ipv6 dhcp relay vlan 1 helper-address** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

ipv6 dhcp relay vlan {*vlan-id*} helper-address {*ip-address*} [*vrf-name*]
no ipv6 dhcp relay vlan {*vlan-id*} helper-address [*ip-address*]

Parameter

vlan-id—— VLAN ID.

ip-address—— DHCPv6 Server address.

vrf-name—— VRF instance name.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add DHCPV6 Server address 2019:2020::21D:FFF:FE61:2005 to interface VLAN 1:

```
Switch(config)# ipv6 dhcp relay vlan 1 helper-address  
2019:2020::21D:FFF:FE61:2005 vrf1
```

60.3 ipv6 dhcp relay information option 18

Description

The **ipv6 dhcp relay information option18** command is used to enable option 18 support of a specified port in DHCPV6 Relay. To disable this function, please use **no ipv6 dhcp relay information option18** command.

Syntax

ipv6 dhcp relay information option18
no ipv6 dhcp relay information option18

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option18 support in DHCPV6 Relay for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)# ipv6 dhcp relay information option18
```

60.4 ipv6 dhcp relay information option37

Description

The **ipv6 dhcp relay information option37** command is used to enable option37 support of a specified port in DHCPV6 Relay. To disable this function, please use **no ipv6 dhcp relay information option37** command.

Syntax

```
ipv6 dhcp relay information option37
no ipv6 dhcp relay information option37
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option37 support in DHCPV6 Relay for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)# ipv6 dhcp relay information option37
```

60.5 ipv6 dhcp relay information remote-id

Description

The **ipv6 dhcp relay information remote-id** command is used to specify the custom remote ID when option37 customization is enabled. To clear the remote ID, please use **no ipv6 dhcp relay information remote-id** command.

Syntax

ipv6 dhcp relay information remote-id *remoteID*
no ipv6 dhcp relay information remote-id

Parameter

remoteID—— Specify the remote ID, ranging from 1 to 128 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the remote ID as "tplink192.168.0.3" for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)# ipv6 dhcp relay information remote-id tplink 192.168.0.
```

60.6 show ipv6 dhcp relay

Description

The **show ipv6 dhcp relay** command is used to display the global status of DHCPV6 Relay.

Syntax

show ipv6 dhcp relay

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global status of DHCPv6 Relay:

```
Switch(config)# show ipv6 dhcp relay
```

60.7 show ipv6 dhcp relay information

Description

The **show ipv6 dhcp relay information** command is used to display the interface status of DHCPv6 Relay.

Syntax

```
show ipv6 dhcp relay information
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the interface status of DHCPv6 Relay:

```
Switch(config)# show ipv6 dhcp relay information
```

60.8 show ipv6 dhcp relay counters

Description

The **show ipv6 dhcp relay counters** command is used to display the packet counter of the DHCPV6 relay.

Syntax

```
show ipv6 dhcp relay counters
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the packet counter of the DHCPV6 relay:

```
Switch# show ipv6 dhcp relay counters
```

Chapter 61 DHCP L2 Relay Commands

61.1 ip dhcp l2relay

Description

The **ip dhcp l2relay** command is used to enable DHCP L2 Relay function globally. To disable DHCP L2 Relay function, please use **no ip dhcp l2relay** command.

Syntax

ip dhcp l2relay
no ip dhcp l2relay

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP L2 Relay function globally:

```
Switch(config)# ip dhcp l2relay
```

61.2 ip dhcp l2relay vlan

Description

The **ip dhcp l2relay vlan** command is used to enable DHCP L2 relay in the specified VLAN. To disable DHCP L2 Relay in the specific vlan, please use **no ip dhcp l2relay vlan** command.

Syntax

ip dhcp l2relay vlan *vlan-range*
no ip dhcp l2relay vlan *vlan-range*

Parameter

vlan-range — Specify the vlan to be enabled with DHCP L2 relay.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP L2 Relay for VLAN 2:

```
Switch(config)# ip dhcp l2relay vlan 2
```

61.3 ip dhcp l2relay information option

Description

The **ip dhcp l2relay information option** command is used to enable option82 support in DHCP Relay. To disable this function, please use **no ip dhcp l2relay information option** command.

Syntax

ip dhcp l2relay information option
no ip dhcp l2relay information option

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option82 support in DHCP Relay for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# ip dhcp l2relay information option
```

61.4 ip dhcp l2relay information strategy

Description

The **ip dhcp l2relay information strategy** command is used to specify the operation for the Option 82 field of the DHCP request packets from the Host. To restore to the default option, please use **no ip dhcp l2relay information strategy** command.

Syntax

```
ip dhcp l2relay information strategy { drop | keep | replace }  
no ip dhcp l2relay information strategy
```

Parameter

drop | keep | replace — The operations for Option 82 field of the DHCP request packets from the Host. The default operation is keep.

drop: Discard the packet with the Option 82 field.

keep: Keep the Option 82 field in the packet.

replace: Replace the option 82 field with the system option defined by the switch.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the option 82 strategy as replace to replace the Option 82 field with the local parameter on receiving the DHCP request packet for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# ip dhcp l2relay information strategy replace
```

61.5 ip dhcp l2relay information format

Description

The **ip dhcp l2relay information format** command is used to select the format of option 82 sub-option value field. To restore to the default option, please use **no ip dhcp l2relay information format** command.

Syntax

```
ip dhcp l2relay information format { normal | private }  
no ip dhcp l2relay information format
```

Parameter

normal | private — The format type of option 82 sub-option value field.

normal: Indicates that the format of sub-option value field is TLV (type-length-value).

private: Indicates that the format of sub-option value field is the value you configure for the related sub-option.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Select the format of option 82 sub-option value field as TLV (type-length-value) for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2  
Switch(config-if)#ip dhcp l2relay information format normal
```

61.6 ip dhcp l2relay information circuit-id

Description

The **ip dhcp l2relay information circuit-id** command is used to specify the custom circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp l2relay information circuit-id** command.

Syntax

ip dhcp l2relay information circuit-id *circuitID*
no ip dhcp l2relay information circuit-id

Parameter

circuitID—— Specify the circuit ID, ranging from 1 to 128 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the circuit ID as "TP-Link" for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)# ip dhcp l2relay information circuit-id TP-Link
```

61.7 ip dhcp l2relay information remote-id

Description

The **ip dhcp l2relay information remote-id** command is used to specify the custom remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp l2relay information remote-id** command.

Syntax

ip dhcp l2relay information remote-id *remoteID*
no ip dhcp l2relay information remote-id

Parameter

remoteID—— Specify the remote ID, ranging from 1 to 128 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the remote ID as "TP-Link" for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# ip dhcp l2relay information remote-id TP-Link
```

61.8 show ip dhcp l2relay

Description

The **show ip dhcp l2relay** command is used to display the global status and Option 82 configuration of DHCP Relay.

Syntax

```
show ip dhcp l2relay
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

```
Switch(config)# show ip dhcp l2relay
```


61.9 show ip dhcp l2relay interface

Description

The **show ip dhcp l2relay interface** command is used to display the DHCP L2 Relay status for the ports.

Syntax

show ip dhcp l2relay interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP L2 Relay configuration of port 1/0/2:

```
Switch(config)# show ip dhcp l2relay interface gigabitEthernet 1/0/2
```

Chapter 62 DHCPV6 L2 Relay Commands

62.1 ipv6 dhcp l2relay

Description

The **ipv6 dhcp l2relay** command is used to enable DHCPV6 L2 Relay function globally. To disable DHCPV6 L2 Relay function, please use **no ipv6 dhcp l2relay** command.

Syntax

ipv6 dhcp l2relay
no ipv6 dhcp l2relay

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCPV6 L2 Relay function globally:

```
Switch(config)# ipv6 dhcp l2relay
```

62.2 ipv6 dhcp l2relay vlan

Description

The **ipv6 dhcp l2relay vlan** command is used to enable DHCPV6 L2 relay in the specified VLAN. To disable DHCPV6 L2 Relay in the specific vlan, please use **no ipv6 dhcp l2relay vlan** command.

Syntax

ipv6 dhcp l2relay vlan *vlan-id*
no ipv6 dhcp l2relay vlan *vlan-id*

Parameter

vlan-id—— Specify the vlan to be enabled with DHCPV6 L2 relay.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP L2 Relay for VLAN 1:

```
Switch(config)# ipv6 dhcp l2relay vlan 1
```

62.3 ipv6 dhcp l2relay forwarding-mode

Description

The **ipv6 dhcp l2relay forwarding-mode** command is used to enable the relay mode of DHCPv6 L2Relay. By default, it is not enabled. After enabling, the device will encapsulate the original DHCPv6 packet within the Relay Message option (option 9) of a Relay-Forward type packet in the RFC 6221 LDRA format, and then insert other relay agent options (such as interface-id, remote-id). It will also receive Relay-Reply type packets from the server, decapsulate them, and forward them to the client. To disable this function, please use **no ipv6 dhcp l2relay forwarding-mode** command.

Syntax

ipv6 dhcp l2relay forwarding-mode
no ipv6 dhcp l2relay forwarding-mode

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCPv6 L2Relay to perform relay forwarding in LDRA format.:

```
Switch(config)# ipv6 dhcp l2relay forwarding-mode
```

62.4 ipv6 dhcp l2relay information interface-id

Description

The **ipv6 dhcp l2relay information interface-id** command is used to configure a custom interface-id (option 18) field. After enabling option 18, DHCPv6 L2Relay relay packets will carry the user-defined interface-id field. To remove this configuration, please use **no ipv6 dhcp l2relay information interface-id** command.

Syntax

ipv6 dhcp l2relay information interface-id *interfaceld*
no ipv6 dhcp l2relay information interface-id

Parameter

interfaceld—— Custom interface-id, with a length not exceeding 64 bytes. Printable characters except double quotes and question marks are allowed. The default value is the unprefix port number of the local port.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a custom interface-id as "tplink.1" under port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# ipv6 dhcp l2relay information interface-id "tplink.1"
```

62.5 ipv6 dhcp l2relay information option18

Description

The **ipv6 dhcp l2relay information** command is used to enable option18 support of a specified port in DHCPV6 L2Relay. To disable this function, please use **no ipv6 dhcp l2relay information** command.

Syntax

ipv6 dhcp l2relay information option18
no ipv6 dhcp l2relay information option18

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option18 support in DHCPV6 L2Relay for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)# ipv6 dhcp l2relay information option18
```

62.6 ipv6 dhcp l2relay information option37

Description

The **ipv6 dhcp l2relay information option37** command is used to enable option37 support of a specified port in DHCPV6 L2Relay. To disable this function, please use **no ipv6 dhcp l2relay information option37** command.

Syntax

ipv6 dhcp l2relay information option37
no ipv6 dhcp l2relay information option37

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option37 support in DHCPV6 L2Relay for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# ipv6 dhcp l2relay information option37
```

62.7 ipv6 dhcp l2relay information remote-id

Description

The **ipv6 dhcp l2relay information remote-id** command is used to specify the custom remote ID when option 37 customization is enabled. To clear the remote ID, please use **no ipv6 dhcp l2relay information remote-id** command.

Syntax

```
ipv6 dhcp l2relay information remote-id remoteID  
no ipv6 dhcp l2relay information remote-id
```

Parameter

remoteID—— Specify the remote ID, ranging from 1 to 128 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the remote ID as "tplink192.168.0.3" for port 2:

```
Switch(config)#interface gigabitEthernet 1/0/2  
Switch(config-if)# ipv6 dhcp l2relay information remote-id tplink  
192.168.0.3
```

62.8 show ipv6 dhcp l2relay

Description

The **show ipv6 dhcp l2relay** command is used to display the global status of DHCPV6 L2Relay.

Syntax

show ipv6 dhcp l2relay

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global status of DHCPV6 L2Relay:

```
Switch(config)# show ipv6 dhcp l2relay
```

62.9 show ipv6 dhcp l2relay information

Description

The **show ipv6 dhcp l2relay information** command is used to display the interface status of DHCPv6 L2Relay.

Syntax

show ipv6 dhcp relay information

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the interface status of DHCPv6 L2Relay:

```
Switch(config)# show ipv6 dhcp l2relay information
```

Chapter 63 QoS Commands

QoS (Quality of Service) function is used to optimize the network performance. It provides you with network service experience of a better quality. The switch implements three priority modes based on port, on 802.1p and on DSCP.



Note: When data packets simultaneously meet the matching conditions of both the Switch QoS Rule and the OUI based VLAN, due to the priority of TCAM, only one of them will take effect.

63.1 qos trust mode

Description

The **qos trust mode** command is used to configure the trust mode of CoS (Class of Service) function for the ports. The default trust mode is trust port priority.

Syntax

qos trust mode { dot1p | dscp | untrust }

Parameter

dot1p—— Trust 802.1p mode. In this mode, data will be classified into different services based on the 802.1p priority.

dscp—— Trust dscp mode. In this mode, data will be classified into different services based on the dscp priority.

untrust—— Trust port mode. In this mode, data will be classified into different services based on the based on the port priority.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the trust mode of port 1/0/3 as dscp:

```
Switch(config)# interface gigabitEthernet 1/0/3
```

```
Switch(config-if)# qos trust mode dscp
```


63.2 qos port-priority

Description

The **qos port-priority** command is used to configure the port to 802.1p priority mapping for the desired port. To return to the default configuration, please use **no qos port-priority** command. When Port Priority is enabled, the packets will be mapped to different priority queues based on the ingress ports.

Syntax

qos port-priority { *dot1p-priority* }
no qos port-priority

Parameter

dot1p-priority—— The 802.1p priority that the packets will be mapped to from the desired port. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively. By default, the priority is 0.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the priority of port 5 as 3:

```
Switch(config)# interface gigabitEthernet 1/0/5  
Switch(config-if)# qos port-priority 3
```

63.3 qos cos-map

Description

The **qos cos-map** command is used to configure 802.1p to queue mapping globally. To return to the default configuration, please use **no qos cos-map** command. When 802.1P Priority is enabled, the packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority.

Syntax

qos cos-map { *dot1p-priority* } { *tc-queue* }

no qos cos-map

Parameter

dot1p-priority—— The value of 802.1p priority. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively.

tc-queue—— The number of TC queue that the 80.1p priority will be mapped to. It ranges from 0 to 7.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Map the 802.1p priority 5 to TC-2:

```
Switch (config)# qos cos-map 5 2
```

63.4 qos dot1p-remap

Description

The **qos dot1p-remap** command is used to configure the 802.1p to 802.1p mappings. To return to the default configuration, please use **no qos dot1p-remap** command. When 802.1p remap is configured, the packets with the specific 802.1p priority will tagged with the desired new 802.1p priority.

Syntax

qos dot1p-remap { *dot1p-priority* } { *new-dot1p-priority* }

no qos dot1p-remap

Parameter

dot1p-priority—— The original 802.1p priority. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively.

new-dot1p-priority—— The new 802.1p priority. It ranges from 0 to 7.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Remap 802.1p priority 5 to 802.1p priority 6:

```
Switch(config)#qos dot1p-remap 5 6
```

For other devices:

Remap 802.1p priority 5 to 802.1p priority 6 for port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#qos dot1p-remap 5 6
```

63.5 qos dscp-map

Description

The **qos dscp-map** command is used to configure the DSCP to 802.1p mapping. To return to the default configuration, please use **no qos dscp-map** command. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP Priority is enabled, IP datagram are mapped to different priority levels based on DSCP priority.

Syntax

```
qos dscp-map { dscp-value-list } { dot1p-priority }
```

```
no qos dscp-map
```

Parameter

dscp-value-list—— The DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63.

dot1p-priority——The 802.1p priority to which the DSCP priority will be mapped. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively. By default, the priority is 0.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Map DSCP Priority 5 to 802.1p priority 2:

```
Switch(config)#qos dscp-map 5 2
```

For other devices:

Map DSCP Priority 5 to 802.1p priority 2 for port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#qos dscp-map 5 2
```

63.6 qos dscp-remap

Description

The **qos dscp-remap** command is used to configure the DSCP to DSCP mappings. To return to the default configuration, please use **no qos dscp-remap** command. When DSCP remap is configured, the packets with the specific DSCP priority will be changed to the desired new DSCP priority.

Syntax

```
qos queue dscp-map { dscp-value-list } { dscp-remap-value }
```

```
no qos queue dscp-map
```

Parameter

Dscp-value-list——The original DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63.

Dscp-remap-value—— The new DSCP value, which ranges from 0 to 63.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Map DSCP values 10-12 to DSCP value 2:

```
Switch(config)# qos dscp-remap 10-12 2
```

For other devices:

Map DSCP values 10-12 to DSCP value 2 for port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
```

```
Switch(config-if)# qos dscp-remap 10-12 2
```

63.7 qos queue bandwidth



Note: This command is only available on certain devices

Description

The **qos queue bandwidth** command is used to configure the minimum guaranteed bandwidth allocated to the specified queue. A value of 0 means there is no guaranteed minimum bandwidth in effect (best-effort service). The default value is 0. The sum of all bandwidth values for the queues must not exceed 100%. To return to the default configuration, please use **no qos bandwidth** command.

Syntax

```
qos queue { tc-queue } bandwidth { rate }
```

```
no qos queue { tc-queue } bandwidth
```

Parameter

tc-queue—— The egress queue ID. It ranges from 0 to 7, which represents TC queue from TC0 to TC7 respectively.

rate——The minimum bandwidth percentage for queue, ranging from 1 to 100 in increments of 1. By default, it is 0.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the minimum bandwidth of TC5 as 10% for port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
```

```
Switch(config-if)# qos queue 5 bandwidth 10
```

63.8 qos queue mode

Description

The **qos queue mode** command is used to configure the Scheduler Mode. When the network is congested, the program that many packets complete for resources must be solved, usually in the way of queue scheduling. The switch will control the forwarding sequence of the packets according to the priority queues and scheduling algorithms you set. On this switch, the priority levels are labeled as TC0, TC1, TC2 ... TC7.

Syntax

```
qos queue { tc-queue } mode { sp | wrr } [ weight weight ]
```

Parameter

tc-queue—— The egress queue ID. It ranges from 0 to 7, which represents TC queue from TC0 to TC7 respectively.

sp —— Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr — Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. If you select this mode, you need to specify the queue weight at the same time.

weight — Configure the weight value of the specified TC queue. When the scheduler mode is specified as WRR, the weight value ranges from 1 to 127. The 8 queues will take up the bandwidth according to their ratio.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Specify the Scheduler Mode of TC1 as WRR and set the queue weight as 10:

```
Switch(config)# qos queue 1 mode wrr weight 10
```

For other devices:

Specify the Scheduler Mode of TC1 as WRR and set the queue weight as 10 for port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
Switch(config-if)# qos queue 1 mode wrr weight 10
```

63.9 qos localPri

Description

The **qos localPri** command is used to configure the egress queue of packets. After configuration, the packets of the corresponding VLAN will be assigned to the specified egress queue.

Syntax

qos localPri queue

Parameter

queue: The egress queue of the packets.

Command Mode

VLAN Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the egress queue for VLAN 2:

```
Switch(config)#vlan 2
Switch(config-vlan)#qos localPri 3
```

63.10 qos cosPri

Description

The **qos cosPri** command is used to configure the 802.1P priority carried by packets when they leave. After configuration, the packets of the corresponding VLAN will be assigned to the specified egress queue.

Syntax

qos cosPri priority

Parameter

priority: 802.1P priority specified for the packets.

Command Mode

VLAN Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the 802.1P priority for VLAN 2:

```
Switch(config)#vlan 2
Switch(config-vlan)#qos cosPri 4
```


63.11 qos dscpPri

Description

The **qos dscpPri** command is used to configure the egress queue of packets. After configuration, the packets of the corresponding VLAN will be assigned to the specified egress queue.

Syntax

qos dscpPri dscp

Parameter

dscp: DSCP priority specified for the packets.

Command Mode

VLAN Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DSCP priority for VLAN 2:

```
Switch(config)#vlan 2
```

```
Switch(config-vlan)#dscp localPri 10
```

63.12 qos wred-profile

Description

The **qos wred-profile** command is used to configure the parameters of the WRED drop profile, including the lower threshold, upper threshold, and maximum drop percentage. To delete the corresponding WRED drop profile, please use the **no qos wred-profile** command.



Note: This command is only available on certain devices.

Syntax

qos wred-profile name low high drop-percentage

no qos wred-profile [name]

Parameter

name: WRED drop profile name.

low: Drop threshold lower limit.

high: Drop threshold upper limit.

drop-percentage: Maximum drop percentage.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a WRED drop profile:

```
Switch(config)#qos wred-profile test 40 80 500
```

63.13 qos wred-bind

Description

The **qos wred-bind** command is used to bind the WRED drop template to the specified port. When traffic exits the port, the WRED policy will be implemented. To unbind the WRED drop profile, please use the **no qos wred-bind** command.



Note: This command is only available on certain devices.

Syntax

qos wred-bind name

no qos wred-bind

Parameter

name: WRED drop profile name.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind the WRED drop profile to ports 1/0/1-4:

```
Switch(config)# interface range gigabitEthernet 1/0/1-4
```

```
Switch(config-if-range)#qos wred-bind test
```

63.14 show qos wred-profile

Description

The **show qos wred-profile** command is used to view the WRED profile info.



Note: This command is only available on certain devices.

Syntax

```
show qos wred-profile [name]
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the WRED profile configuration:

```
Switch#show qos wred-profile
```

63.15 show qos wred-bind interface

Description

The **show qos wred-bind interface** command is used to view the binding information of the WRED template.



Note: This command is only available on certain devices.

Syntax

```
show qos wred-bind interface [{fastEthernet | gigabitEthernet |  
hundred-gigabitEthernet | port-channel | ten-gigabitEthernet |  
twentyFive-gigabitEthernet | two-gigabitEthernet} interface-value]
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the information of the WRED template bound to bound to ports 1/0/1-3:

```
Switch#show qos wred-bind interface gigabitEthernet 1/0/1-3
```

63.16 show qos cos-map

Description

The **show qos cos-map** command is used to display the 802.1p priority to TC queue mappings.

Syntax

```
show qos cos-map
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the 802.1p to queue mappings:

```
Switch# show qos cos-map
```

63.17 show qos dot1p-remap interface



Note: This command is only available on certain devices.

Description

The **show qos dot1p-remap interface** command is used to display the 802.1p priority to 802.1p priority mappings.

Syntax

```
show qos dot1p-remap interface [fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port | port-channel port-channel-id]
```

Parameter

port — The port number.

port-channel-id — The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IEEE 802.1P remap configuration of all the ports:

```
Switch# show qos dot1p-remap interface
```

63.18 show qos dot1p-remap



Note: This command is only available on certain devices.

Description

The **show qos dot1p-remap interface** command is used to display the 802.1p priority to 802.1p priority mappings.

Syntax

```
show qos dot1p-remap
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IEEE 802.1P remap configuration:

```
Switch# show qos dot1p-remap
```

63.19 show qos dscp-map interface



Note: This command is only available on certain devices.

Description

The **show qos dscp-map interface** command is used to display the DSCP priority configuration of the ports.

Syntax

```
show qos dscp-map interface [fastEthernet port] gigabitEthernet port |  
ten-gigabitEthernet port | port-channel port-channel-id]
```

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP priority configuration of all the ports:

```
Switch# show qos dscp-map interface
```

63.20 show qos dscp-map



Note: This command is only available on certain devices.

Description

The **show qos dscp-map** command is used to display the DSCP priority configuration.

Syntax

```
show qos dscp-map
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP priority configuration:

```
Switch# show qos dscp-map
```

63.21 show qos dscp-remap interface



Note: This command is only available on certain devices.

Description

The **show qos dscp-remap interface** command is used to display the DSCP priority to DSCP priority mappings of the ports.

Syntax

show qos dscp-remap interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port — The port number.

port-channel-id — The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP to DSCP mappings for all the ports:

```
Switch# show qos dscp-remap interface
```

63.22 show qos dscp-remap



Note: This command is only available on certain devices.

Description

The **show qos dscp-remap** command is used to display the DSCP priority to DSCP priority mappings.

Syntax

show qos dscp-remap

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP to DSCP mappings:

```
Switch# show qos dscp-remap
```

63.23 show qos port-priority interface

Description

The **show qos port-priority interface** command is used to display the port to 802.1p priority mappings for the ports.

Syntax

show qos port-priority interface [**fastEthernet** *port*] **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port — The port number.

port-channel-id — The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port to 802.1p priority mappings for all the ports:

```
Switch# show qos port-priority interface
```

63.24 show qos trust interface

Description

The **show qos trust interface** command is used to display the trust mode of the ports.

Syntax

show qos trust interface [**fastEthernet** *port*] **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port — The port number.

port-channel-id — The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the trust mode of all the ports:

```
Switch# show qos trust interface
```

63.25 show qos queue interface

Description

The **show qos queue interface** command is used to display the scheduler settings of the ports.

Syntax

```
show qos queue interface [fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port | port-channel port-channel-id]
```

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the scheduler settings of all the ports:

```
Switch# show qos queue interface
```

63.26 show qos rule

Description

The **show qos rule** command is used to display the configuration of applied QoS entries under the Controller mode (QoS rules can only be configured in Controller mode).

Syntax

```
show qos rule
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of applied QoS entries under the Controller mode:

```
Switch# show qos rule
```

Chapter 64 Bandwidth Control Commands

Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Rate limit functions to limit the ingress/egress traffic rate on each port. Storm Control function allows the switch to monitor broadcast packets, multicast packets and Unknown unicast frames in the network.

64.1 storm-control rate-mode

Description

The **storm-control rate-mode** command is used to configure the storm control mode of the interface. To return to the default configuration, please use **no storm-control rate-mode** command.

Syntax

```
storm-control rate-mode { kbps | ratio | pps }  
no storm-control rate-mode
```

Parameter

kbps —— Select the storm control mode of the interface as kbps. The switch will limit the maximum speed of the specific kinds of traffic in kilo-bits per second.

ratio —— Select the storm control mode of the interface as ratio. The switch will limit the percentage of bandwidth utilization for specific kinds of traffic.

pps —— The switch will limit the maximum number of packets per second for specific kinds of traffic.

Note: pps is only available on certain devices.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

This command should be used along with the [storm-control](#) command to enable the storm control function and specify the detailed parameters.

Example

Set the storm control mode as kbps on port 1/0/5:

```
Switch(config)# interface gigabitEthernet 1/0/5
Switch(config-if)# storm-control rate-mode kbps
```

64.2 storm-control

Description

The **storm-control** command is used to enable the broadcast, multicast, or unknown unicast storm control function and to set threshold levels on an interface. To return to the default configuration, please use **no storm-control** command.

Syntax

```
storm-control { broadcast | multicast | unicast } { rate }
no storm-control { broadcast | multicast | unicast }
```

Parameter

broadcast | multicast | unicast — Select the mode of the storm control on the interface.

rate — Specify the bandwidth for receiving packets on the port. The specified type of packet traffic exceeding the bandwidth will be processed according to the configuration of **storm-control exceed** command. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Before you configure the storm-control type as kbps or ratio, please ensure that the port is not in pps mode.

Example

Configure the broadcast storm control rate as 1024 kbps on port 1/0/5:

```
Switch(config)# interface gigabitEthernet 1/0/5
Switch(config-if)# storm-control rate-mode kbps
Switch(config-if)# storm-control broadcast 1024
```

64.3 storm-control exceed

Description

The **storm-control exceed** command is used to configure the action that the switch will perform when the storm exceeds the defined limit on an interface.

Syntax

```
storm-control exceed { drop | shutdown } [ revocer-time time ]
```

Parameter

drop — Set the Action as Drop. The port will drop the subsequent packets when the traffic exceeds the limit.

shutdown — Set the Action as Shutdown. The port will be shutdown when the traffic exceeds the limit.

time — Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 and the default value is 0. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, which means the port will not recover to its normal state automatically and you can recover the port manually using **storm-control recover** command.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the action as drop on port 1/0/5:

```
Switch(config)# interface gigabitEthernet 1/0/5
Switch(config-if)# storm-control exceed drop
```

64.4 storm-control recover

Description

The **storm-control recover** command is used to recover the port manually after the port is shutdown because of the storm. When the recover time is specified as 0, the port will not recover to its normal state automatically. In this condition, you need to use this command to recover the port manually.

Syntax

storm-control recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Recover port 1/0/5 manually:

```
Switch(config)# interface gigabitEthernet 1/0/5
Switch(config-if)# storm-control recover
```

64.5 bandwidth

Description

The **bandwidth** command is used to configure the bandwidth limit for an Ethernet port. To disable the bandwidth limit, please use **no bandwidth** command.

Syntax

bandwidth {[**ingress** *ingress-rate*] [**egress** *egress-rate*]}
no bandwidth { all | ingress | egress }

Parameter

ingress-rate—— Specify the upper rate limit for receiving packets. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64.

egress-rate—— Specify the upper rate limit for sending packets. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ingress-rate as 5120Kbps and egress-rate as 1024Kbps for port 1/0/5:

```
Switch(config)# interface gigabitEthernet 1/0/5
Switch(config-if)# bandwidth ingress 5120 egress 1024
```

64.6 show storm-control

Description

The **show storm-control** command is used to display the storm-control information of Ethernet ports.

Syntax

```
show storm-control interface [ fastEthernet port | gigabitEthernet port-list
ten-gigabitEthernet port | port-channel port-channel-id-list ]
```

Parameter

port-list——The list of Ethernet ports.

port-channel-id-list—— The list of port channels.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the storm-control information of port 4, 5, 6, and 7:

```
Switch(config)# show storm-control interface gigabitEthernet 1/0/4-7
```

64.7 show bandwidth

Description

The **show bandwidth** command is used to display the bandwidth-limit information of Ethernet ports.

Syntax

show bandwidth interface [**fastEthernet** *port* | **gigabitEthernet** *port-list* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id-list*]

Parameter

port-list——The list of Ethernet ports.

port-channel-id-list——The list of port channels.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bandwidth-limit information of port 1/0/4:

```
Switch(config)# show bandwidth interface gigabitEthernet 1/0/4
```


Chapter 65 OUI-Based VLAN Commands (Only for Certain Devices)

OUI-Based VLAN (Organizationally Unique Identifier-Based Virtual Local Area Network) is a functionality that transmits and modifies the 802.p priority of packets within a specified VLAN based on the source MAC address of the packets. Similar to Voice VLAN, OUI-Based VLAN differs in the following ways: (1) OUI-Based VLAN does not provide users with default templates for OUI entries; users can configure them themselves; (2) Voice VLAN can only specify one VLAN as the Voice VLAN, whereas OUI-Based VLAN can assign different VLANs to different OUI entries; (3) The mask length for Voice VLAN is fixed, while OUI-Based VLAN allows for variable-length masks to be set for MAC addresses during configuration; (4) For each OUI entry, OUI-Based VLAN can specify which port the entry applies to.

65.1 voice vlan

Description

This command is used to configure OUI-Based VLAN entries. After the entries are configured, the system will automatically number each entry. Users can add ports when configuring entries, or add ports in port view after configuring entries. To delete the configured entries, please use the **no voice-vlan** command.

Syntax

```
voice-vlan mac-addr mac-address oui-mask oui-mask vlan vlan-id priority priority oui-desc oui-description [interface {fastEthernet | gigabitEthernet | hundred-gigabitEthernet | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet} interface-value]
no voice-vlan index
```

Parameter

mac-address: MAC address, formatted as 00:0a:eb:00:13:86, represents the source MAC address that needs to be matched.

oui-mask: MAC address mask, formatted as ff:ff:ff:00:00:00, where the final match is the result of performing a bitwise AND operation between *mac-address* and *oui-mask*.

vlan-id: 802.1q VLAN ID, ranging from 2 to 4094.

priority: 802.1p priority, ranging from 0 to 7.

oui-description: Description information for the OUI entry, with a string length not exceeding 16 characters.

interface-value: Port number.

index: Automatically generated entry index number by the system.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add OUI-based VLAN entries:

```
Switch(config)#voice-vlan mac-addr 00:01:00:00:00:00 oui-mask  
ff:ff:00:00:00:00 vlan 100 priority 4 oui-desc oui1
```

65.2 voice-vlan(interface)

Description

This command is used to enable the OUI-Based VLAN function on the interface. To disable this function, please use the **no voice-vlan entry** command.

Syntax

voice-vlan entry *index*

no voice-vlan entry *index*

Parameter

index: The entry index number generated by the system is used to specify which OUI entry applies to a port through the index.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable OUI-based VLAN on interfaces 1/0/2-6:

```
Switch(config)#interface range gigabitEthernet 1/0/2-6
Switch(config-if-range)#voice-vlan entry 1
```

65.3 show voice-vlan

Description

This command is used to view the OUI-Based VLAN configuration.

Syntax

show voice-vlan

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the OUI-Based VLAN:

```
Switch# show voice-vlan
```

Chapter 66 Voice VLAN Commands

Voice VLANs are configured specially for voice data stream. By configuring Voice VLANs and adding the ports with voice devices attached to voice VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

66.1 voice vlan

Description

The **voice vlan** command is used to enable Voice VLAN function. To disable Voice VLAN function, please use **no voice vlan** command.

Syntax

voice vlan *vlan-id*

no voice vlan

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 2 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Voice VLAN function for VLAN 10:

```
Switch(config)# voice vlan 10
```

66.2 voice vlan (interface)

Description

The **voice vlan** command is used to enable Voice VLAN function on the desired ports. To disable Voice VLAN function on ports, please use **no voice vlan** command.

Syntax

voice vlan

no voice vlan

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Voice VLAN function for port 1/0/1:

```
Switch(config)# interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#voice vlan
```

66.3 voice vlan priority

Description

The **voice vlan priority** command is used to configure the priority for the Voice VLAN. To restore to the default priority, please use **no voice vlan priority** command.

Syntax

voice vlan priority *pri*

no voice vlan priority

Parameter

pri—— Priority, ranging from 0 to 7, and the default value is 7.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the priority of the Voice VLAN as 5:

```
Switch(config)# voice vlan priority 5
```

66.4 voice vlan oui

Description

The **voice vlan oui** command is used to create Voice VLAN OUI. To delete the specified Voice VLAN OUI, please use **no voice vlan oui** command.

Syntax

voice vlan oui *oui-prefix* **oui-desc** *string*

no voice vlan mac-address *oui-prefix*

Parameter

oui-prefix—— The OUI address of the voice device, in the format of XX:XX:XX.

string—— Give a description to the OUI for identification which contains 16 characters at most.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a Voice VLAN OUI described as TP-Phone with the OUI address 00:11:11:11:11:11 and the mask address FF:FF:FF:00:00:00:

```
Switch(config)#voice vlan oui 00:11:11 oui-desc TP-Phone
```

66.5 show voice vlan

Description

The **show voice vlan** command is used to display the global configuration information of Voice VLAN.

Syntax

show voice vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the configuration information of Voice VLAN globally:

```
Switch(config)# show voice vlan
```

66.6 show voice vlan oui-table

Description

The **show voice vlan oui** command is used to display the configuration information of Voice VLAN OUI.

Syntax

show voice vlan oui

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the configuration information of Voice VLAN OUI:

```
Switch(config)# show voice vlan oui-table
```

66.7 show voice vlan interface

Description

The **show voice vlan interface** command is used to display the Voice VLAN configuration information of all ports.

Syntax

show voice vlan interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the Voice VLAN configuration information of all ports and port channels:

```
Switch(config)# show voice vlan interface
```


Chapter 67 Auto VoIP Commands

The Auto VoIP feature is used to prioritize the transmission of voice traffic. Voice over Internet Protocol (VoIP) enables telephone calls over a data network, and the Auto VoIP feature helps provide a classification mechanism for voice packets. When Auto VoIP is configured on a port that receives both voice and data traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is heavy.

67.1 **auto-voip**

Description

The **auto-voip** command is used to enable the Auto VoIP function globally.

To disable the Auto VoIP function, use **no auto-voip** command.

Syntax

auto-voip

no auto-voip

Command Mode

Global Configuration Mode

Example

Enable the Auto VoIP function globally:

```
Switch(config)# auto-voip
```

67.2 **auto-voip (interface)**

Description

The **auto-voip** command is used to specify the interface mode as VLAN ID for the ports. In this mode, the voice devices will send voice packets with desired VLAN tag.

Syntax

auto-voip *vlan-id*

Parameter

vlan-id——Specify the Auto VoIP VLAN ID. The valid values are from 2 to 4094.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set Auto VoIP VLAN 3 for port 3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# auto-voip 3
```

67.3

auto-voip dot1p

Description

The **auto-voip dot1p** command is used to specify the interface mode as dot1p for the ports. In this mode, the voice devices will send voice packets with desired 802.1p priority.

Syntax

auto-voip dot1p *dot1p*

Parameter

dot1p—Set the 802.1p priority of Auto VoIP on specified ports. It ranges from 0 to 7.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set the 802.1p priority as 5 for the port:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# auto-voip dot1p 5
```

67.4

auto-voip untagged

Description

The **auto-voip untagged** command is used to specify the interface mode as untagged for the ports. In this mode, the voice devices will send untagged voice packets.

Syntax

auto-voip untagged

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set the interface mode as untagged for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# auto-voip untagged
```

67.5

auto-voip none

Description

The **auto-voip none** command is used to specify the interface mode as none for the ports. In this mode, the switch allows the voice devices to use its own configuration to send voice traffic.

Syntax

auto-voip none

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Instruct voice devices that are connected to port 3 to send the packets according to its own configuration:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# auto-voip none
```

67.6

no auto-voip (interface)

Description

The **no auto-voip** command is used to specify the interface mode as disabled for the ports, which means the Auto VoIP function is disabled on the corresponding port.

Syntax

no auto-voip

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Disable the Auto VoIP function on port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# no auto-voip
```

67.7

auto-voip dscp

Description

The **auto-voip dscp** command is used to set the DSCP value of Auto VoIP on specified ports.

Syntax

auto-voip dscp *value*

Parameter

value——Set the DSCP value of Auto VoIP on specified ports. It ranges from 0 to 63. By default, it is 0.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set DSCP value of Auto VoIP on port 3 as 33:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# auto-voip dscp 33
```

67.8

auto-voip data priority

Description

The **auto-voip data priority** command is used to enable or disable the CoS Override Mode on specified ports.

Syntax

```
auto-voip data priority { trust | untrust }
```

Parameter

trust—In this mode, the switch will then put the voice packets in the corresponding TC queue according to the 802.1p priority of the packets.

untrust—In this mode, the switch will ignore the 802.1p priority in the voice packets and put the packets in TC-5 directly.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set the CoS Override Mode as trust for port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# auto-voip data priority trust
```

67.9

show auto-voip

Description

The **show auto-voip** command is used to display the Auto VoIP configuration information.

Syntax

```
show auto-voip [ interface ]
```

Parameter

interface — Displays the Auto VoIP configuration information of ports.
When no parameter is entered, displays the global Auto VoIP configuration information.

Command Mode

Privileged EXEC Mode and any Configuration Mode

Example

Displays the global Auto VoIP configuration information:

```
Switch (config)# show auto-voip
```

Chapter 68 Access Control Commands

68.1 user access-control ip-based enable

Description

The **user access-control ip-based enable** command is used to configure the access control mode IP-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control ip-based enable
no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the access control mode as IP-based:

```
Switch(config)# user access-control ip-based enable
```

68.2 user access-control ip-based

Description

The **user access-control ip-based** command is used to limit the IP-range of the users for login. Only the users within the IP-range you set here are allowed to login. You can add up to 30 IP-based entries. To cancel the user access limit, please use **no user access-control ip-based** command.

Syntax

user access-control ip-based { *ip-addr ip-mask* } [snmp] [telnet] [ssh]
[http] [https] [ping] [all]

no user access-control ip-based index *id*

Parameter

ip-addr—— The source IP address. Only the users within the IP-range you set here are allowed for login. 5 IP-based entries can be configured at most.

ip-mask—— The subnet mask of the IP address.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] —— Specify the access interface. These interfaces are enabled by default.

id—— Delete the specified IP-based entry.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the access-control of the user whose IP address is 192.168.0.148:

```
Switch(config)# user access-control ip-based 192.168.0.148  
255.255.255.255
```

68.3 user access-control mac-based enable

Description

The **user access-control mac-based enable** command is used to configure the access control mode MAC-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control mac-based enable

no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the access control mode as MAC-based:

```
Switch(config)# user access-control mac-based enable
```

68.4 user access-control mac-based

Description

The **user access-control mac-based** command is used to limit the MAC address of the users for login. Only the user with this MAC address you set here is allowed to login. You can add up to 30 mac-based control entries. To delete the mac-based access control entry, please use **no user access-control mac-based** command.

Syntax

```
user access-control mac-based { mac-addr } [ snmp ] [ telnet ] [ ssh ] [ http ]  
[ https ] [ ping ] [ all ]  
no user access-control mac-based index id
```

Parameter

mac-addr — The source MAC address. Only the user with this MAC address is allowed to login.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] — Specify the access interface. These interfaces are enabled by default.

id — Specify the ID of the mac-based entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure that only the user whose MAC address is 00:00:13:0A:00:01 is allowed to login:

```
Switch(config)# user access-control mac-based 00:00:13:0A:00:01
```

68.5 user access-control port-based enable

Description

The **user access-control port-based enable** command is used to configure the access control mode Port-based. To disable the access control feature, please use **no user access-control** command.

Syntax

```
user access-control port-based enable  
no user access-control
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the access control mode as Port-based:

```
Switch(config)# user access-control port-based enable
```

68.6 user access-control port-based

Description

The **user access-control port-based** command is used to limit the ports for login. Only the users connected to these ports you set here are allowed to login. You can add up to 30 port-based control entries. To delete the port-based access control entry, please use **no user access-control port-based** command.

Syntax

user access-control port-based interface { **gigabitEthernet** *port-list* } [snmp]
[telnet] [ssh] [http] [https] [ping] [all]
no user access-control port-based index *id*

Parameter

port-list——The list group of Ethernet ports, in the format of 1/0/1-4. You can appoint 5 ports at most.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] —— Specify the access interface. These interfaces are enabled by default.

id—— Specify the ID of the port-based entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure that only the users connected to ports 2-6 are allowed to login:

```
Switch(config)# user access-control port-based interface gigabitEthernet  
1/0/2-6
```

68.7 user access-control ipv6-based enable

Description

The **user access-control ipv6-based enable** command is used to configure the access control mode IPV6-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control ipv6-based enable
no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the access control mode as IPV6-based:

```
Switch(config)# user access-control ipv6-based enable
```

68.8 user access-control ipv6-based

Description

The **user access-control ipv6-based** command is used to limit the IPV6-range of the users for login. Only the users within the IPV6-range you set here are allowed to login. You can add up to 30 IPV6-based entries. To cancel the user access limit, please use **no user access-control ipv6-based** command.

Syntax

user access-control ipv6-based { *ipv6-addr* } [snmp] [telnet] [ssh] [http]
[https] [ping] [all]

no user access-control ipv6-based index *id*

Parameter

ipv6-addr—— The source IP address. Only the users within the IPV6-range you set here are allowed for login.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] —— Specify the access interface. These interfaces are enabled by default.

id—— Delete the specified IP-based entry that ranges from 1 to 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the access-control of the user whose IP address is fe80::1234:

```
Switch(config)# user access-control ipv6-based fe80::1234
```

68.9 user access-control

ip-based index

Description

The **user access-control ip-based index** command is used to add an IP-based access-control entry at the specified index. If an entry already exists at the specified index, it will be overwritten. Otherwise, a new entry is added. The entry can restrict access to specific management services; the default is all. To delete entries by their order in the list, use **the no user access-control ip-based order** command.

Syntax

```
user access-control ip-based index {index ip-addr ip-mask} [snmp] [telnet]
[ssh] [http] [https] [ping] [all]
no user access-control ip-based order {order / order-order}
```

Parameter

index — Entry index. Valid values are 1 to 30.

ip-addr — Permitted IPv4 address.

ip-mask — IPv4 address mask.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] — Management services allowed by this entry. Default is all.

order — Entry order. Valid values are 1 to 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Add an entry at index 3 for IP 192.168.0.1/32, allowing SNMP and Telnet only:

```
Switch(config)# user access-control ip-based index 3 192.168.0.1
255.255.255.255 snmp telnet
```

Delete entries by order (delete entries 2 to 6):

```
Switch(config)# no user access-control ip-based order 2-6
```

68.10 user access-control

ipv6-based index

Description

The **user access-control ipv6-based index** command is used to add an IPv6-based access-control entry at the specified index. If an entry already exists at the specified index, it will be overwritten. Otherwise, a new entry is added. The entry can restrict access to specific management services; the default is all. To delete entries by their order in the list, use the **no user access-control ipv6-based order** command.

Syntax

```
user access-control ipv6-based index {index ipv6-addr} [snmp] [telnet] [ssh]  
[http] [https] [ping] [all]  
no user access-control ipv6-based order {order / order-order}
```

Parameter

index — Entry index. Valid values are 1 to 30.

ipv6-addr — Permitted IPv6 address.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] — Management services allowed by this entry. Default is all.

order — Entry order. Valid values are 1 to 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Add an entry at index 2 for IPv6 address 3001::1002, allowing all services:

```
Switch(config)# user access-control ipv6-based index 2 3001::1002
```

Delete an entry by order (delete entry 4):

```
Switch(config)# no user access-control ipv6-based order 4
```

68.11 user access-control mac-based index

Description

The **user access-control mac-based index** command is used to add a MAC-based access-control entry at the specified index. If an entry already exists at the specified index, it will be overwritten. Otherwise, a new entry is added. The entry can restrict access to specific management services; the default is all. To delete entries by their order in the list, use the **no user access-control mac-based order** command.

Syntax

```
user access-control mac-based index {index mac-addr} [snmp] [telnet] [ssh]  
[http] [https] [ping] [all]  
no user access-control mac-based order {order / order-order}
```

Parameter

index — Entry index. Valid values are 1 to 30.

mac-addr — Permitted MAC address.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] — Management services allowed by this entry. Default is all.

order — Entry order. Valid values are 1 to 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Add an entry at index 15 for MAC 00:00:00:00:00:01, allowing HTTP only:

```
Switch(config)# user access-control mac-based index 15  
00:00:00:00:00:01 http
```

Delete entries by order (delete entries 5 to 9):

```
Switch(config)# no user access-control mac-based order 5-9
```

68.12 user access-control

port-based index

Description

The **user access-control port-based index** command is used to add a port-based access-control entry at the specified index. If an entry already exists at the specified index, it will be overwritten. Otherwise, a new entry is added. The entry can restrict access to specific management services; the default is all. To delete entries by their order in the list, use the **no user access-control port-based order** command.

Syntax

```
user access-control port-based index {index} interface {fastEthernet |  
gigabitEthernet | hundred-gigabitEthernet | ten-gigabitEthernet |  
twentyFive-gigabitEthernet | two-gigabitEthernet} port [snmp] [telnet] [ssh]  
[http] [https] [ping] [all]  
no user access-control port-based order {order / order-order}
```

Parameter

index — Entry index. Valid values are 1 to 30.

port — Permitted interface port list.

[**snmp**] [**telnet**] [**ssh**] [**http**] [**https**] [**ping**] [**all**] — Management services allowed by this entry. Default is all.

order — Entry order. Valid values are 1 to 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Add an entry at index 3 for ports 1/0/1-2, allowing HTTPS only:

```
Switch(config)# user access-control port-based index 3 interface  
gigabitEthernet 1/0/1-2 https
```

Delete an entry by order (delete entry 6):

```
Switch(config)# no user access-control port-based order 6
```




Chapter 69 HTTP and HTTPS Commands

With the help of HTTP (HyperText Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer), you can manage the switch through a standard browser.

HTTP is the protocol to exchange or transfer hypertext.

SSL (Secure Sockets Layer), a security protocol, is to provide a secure connection for the application layer protocol (e.g. HTTP) based on TCP. Adopting asymmetrical encryption technology, SSL uses key pair to encrypt/decrypt information. A key pair refers to a public key (contained in the certificate) and its corresponding private key. By default the switch has a certificate (self-signed certificate) and a corresponding private key. The Certificate/Key Download function enables the user to replace the default key pair.

69.1 ip http server

Description

The **ip http server** command is used to enable the HTTP server on the switch. If ip http server is disabled while ip http secure-server is enabled, all HTTP access is redirected to the HTTPS server. The HTTP server is disabled by default. The HTTP and HTTPS servers can be disabled at the same time. To disable the HTTP function, please use **no ip http server** command.

Syntax

ip http server

no ip http server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Disable the HTTP function:

```
Switch(config)# no ip http server
```

69.2 ip http port

Description

The **ip http port** command is used to configure the port number of the HTTP server within the switch. To set the number to the default value, please use **no ip http port** command.

Syntax

ip http port *port-num*

no ip http port

Parameter

port-num — Enter the port number. This value ranges from 1 to 65535.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the port number of HTTP server as 1800:

```
Switch(config)# ip http port 1800
```

69.3 ip http max-users

Description

The **ip http max-users** command is used to configure the maximum number of users that are allowed to connect to the HTTP server. To cancel this limitation, please use **no ip http max-users** command.

Syntax

ip http max-users *admin-num operator-num poweruser-num user-num*

no ip http max-users

Parameter

admin-num — The maximum number of the users logging on to the HTTP server as Admin, ranging from 1 to 16. The total number of users should be no more than 16.

operator-num—— The maximum number of the users logging on to the HTTP server as operator, ranging from 0 to 15. The total number of users should be no more than 16.

poweruser-num—— The maximum number of the users logging on to the HTTP server as Power User, ranging from 0 to 15. The total number of users should be no more than 16.

user-num—— The maximum number of the users logging on to the HTTP server as User, ranging from 0 to 15. The total number of users should be no more than 16.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the maximum number of the Admin, Operator, Power User and User as 5, 1, 1, 1 for HTTP:

```
Switch(config)# ip http max-users 5 1 1 1
```

69.4 ip http session timeout

Description

The **ip http session timeout** command is used to configure the connection timeout of the HTTP server. To restore to the default timeout time, please use **no ip http session timeout** command.

Syntax

ip http session timeout *time*

no ip http session timeout

Parameter

time——The timeout time, ranging from 5 to 30 in minutes. By default, the value is 10.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the timeout time of the HTTP connection as 15 minutes:

```
Switch(config)# ip http session timeout 15
```

69.5 ip http secure-server

Description

The **ip http secure-server** command is used to enable the HTTPS server within the switch. To disable the HTTPS function, please use **no ip http secure-server** command. This function is enabled by default. The HTTP and HTTPS server function can be disabled at the same time.

Syntax

ip http secure-server

no ip http secure-server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the HTTP function:

```
Switch(config)# no ip http secure-server
```

69.6 ip http secure-port

Description

The **ip http secure-port** command is used to configure the port number of the HTTPS server within the switch. To set the number to the default value, please use **no ip http secure-port** command.

Syntax

ip http secure-port *port-num*

no ip http secure-port

Parameter

port-num — Enter the port number. This value ranges from 1 to 65535.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the port number of HTTPS server as 2800:

```
Switch(config)# ip http secure-port 2800
```

69.7 ip http secure-protocol

Description

The **ip http secure-protocol** command is used to configure the SSL protocol version. To restore to the default SSL version, please use **no ip http secure-protocol** command. By default, the switch supports all the protocol versions, including SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2.

Syntax

ip http secure-protocol { ssl3 | tls1 | tls11 | tls12 | all }

no ip http secure-protocol

Parameter

ssl3 — Select SSL Version 3.0 as the protocol for HTTPS.

tls1 — Select TLS Version 1.0 as the protocol for HTTPS.

tls11 — Select TLS Version 1.1 as the protocol for HTTPS.

tls12 — Select TLS Version 1.2 as the protocol for HTTPS.

all — Enable all the above protocols for HTTPS. The HTTPS server and client will negotiate the protocol each time.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the protocol of SSL connection as SSL 3.0:

```
Switch(config)# ip http secure-protocol ssl3
```

69.8 ip http secure-ciphersuite

Description

The **ip http secure-ciphersuite** command is used to configure the cipherSuites over the SSL connection supported by the switch. To restore to the default ciphersuite types, please use **no ip http secure-ciphersuite** command.

Syntax

```
ip http secure-ciphersuite { [ rc4-128-md5 ] [ rc4-128-sha ] [ des-cbc-sha ]  
[ 3des-ede-cbc-sha ] [ ecdhe-a128-g-s256 ] [ ecdhe-a256-g-s384 ] }  
no ip http secure-ciphersuite
```

Parameter

[rc4-128-md5] [rc4-128-sha] [des-cbc-sha] [3des-ede-cbc-sha]
[ecdhe-a128-g-s256] [ecdhe-a256-g-s384] — Specify the encryption algorithm and the digest algorithm to use on an SSL connection. By default, the switch supports all these ciphersuites.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ciphersuite to be used for encryption over the SSL connection as 3des-ede-cbc-sha:

```
Switch(config)# ip http secure-ciphersuite 3des-ede-cbc-sha
```

69.9 ip http secure-max-users

Description

The **ip http secure-max-users** command is used to configure the maximum number of users that are allowed to connect to the HTTPs server. To cancel this limitation, please use **no ip http secure-max-users** command.

Syntax

ip http secure-max-users *admin-num operator-num poweruser-num user-num*

no ip secure-max-users

Parameter

admin-num—— The maximum number of the users logging on to the HTTPs server as Admin, ranging from 1 to 16. The total number of users should be less than 16.

Operator-num—— The maximum number of the users logging on to the HTTPs server as operator, ranging from 0 to 15. The total number of users should be less than 16.

poweruser-num—— The maximum number of the users logging on to the HTTP server as Power User, ranging from 0 to 15. The total number of users should be less than 16.

user-num—— The maximum number of the users logging on to the HTTP server as User, ranging from 0 to 15. The total number of users should be less than 16.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of the Admin, Operator, Power User and User as 5, 1, 1, 1 for HTTPs:

```
Switch(config)# ip http secure-max-users 5 1 1 1
```


69.10 ip http secure-subject-alt-name

Description

The **ip http secure-subject-alt-name** command is used to configure the subject-alt-name (SAN) field of the HTTPS self-signed certificate. The default value is empty. To remove the SAN configuration, use the **no ip http secure-subject-alt-name** command.

Syntax

```
ip http secure-subject-alt-name domain  
no ip http secure-subject-alt-name domain
```

Parameter

domain—— IP address or domain name to be used in the SAN field of the HTTPS certificate.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the SAN of the HTTPS certificate as 192.168.0.1:

```
Switch(config)# ip http secure-subject-alt-name 192.168.0.1
```

69.11 ip http secure-certification signature-algorithm

Description

The **ip http secure-certification signature-algorithm** command is used to configure the signature algorithm for the HTTPS self-signed certificate. The default signature algorithm is RSA-PSS-SHA256.

Syntax

```
ip http secure-certification signature-algorithm { rsa-sha256 |  
rsa-pss-sha256 }
```

Parameter

rsa-sha256—— RSA-SHA256 signature algorithm.

rsa-pss-sha256—— RSA-PSS-SHA256 signature algorithm.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the HTTPS certificate signature algorithm to RSA-SHA256:

```
Switch(config)#ip http secure-certification signature-algorithm  
rsa-sha256
```

69.12 ip http secure-session timeout

Description

The **ip http secure-session timeout** command is used to configure the connection timeout of the HTTPS server. To restore to the default timeout time, please use **no ip http secure-session timeout** command.

Syntax

```
ip http secure-session timeout time  
no ip http secure-session timeout
```

Parameter

time—— The timeout time, ranging from 5 to 30 in minutes. By default, the value is 10.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the timeout time of the HTTPs connection as 15 minutes:

```
Switch(config)# ip http secure-session timeout 15
```

69.13 ip http secure-server download certificate

Description

The **ip http secure-server download certificate** command is used to download a certificate to the switch from TFTP server.

Syntax

```
ip http secure-server download certificate ssl-cert ip-address ip-addr
```

Parameter

ssl-cert—— The name of the SSL certificate which is selected to download to the switch. The length of the name ranges from 1 to 25 characters. The Certificate must be BASE64 encoded.

ip-addr—— The IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download an SSL Certificate named ssl-cert from TFTP server with the IP address of 192.168.0.146:

```
Switch(config)# ip http secure-server download certificate ssl-cert  
ip-address 192.168.0.146
```

Download an SSL Certificate named ssl-cert from TFTP server with the IP address of fe80::1234

```
Switch(config)# ip http secure-server download certificate ssl-cert  
ip-address fe80::1234
```

69.14 ip http secure-server download key

Description

The **ip http secure-server download key** command is used to download an SSL key to the switch from TFTP server.

Syntax

ip http secure-server download key *ssl-key* **ip-address** *ip-addr*

Parameter

ssl-key—— The name of the SSL key which is selected to download to the switch. The length of the name ranges from 1 to 25 characters. The Key must be BASE64 encoded.

ip-addr—— The IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download an SSL key named ssl-key from TFTP server with the IP address of 192.168.0.146:

```
Switch(config)# ip http secure-server download key ssl-key ip-address  
192.168.0.146
```

Download an SSL key named ssl-key from TFTP server with the IP address of fe80::1234

```
Switch(config)# ip http secure-server download key ssl-key ip-address  
fe80::1234
```

69.15 show ip http configuration

Description

The **show ip http configuration** command is used to display the configuration information of the HTTP server, including status, session timeout, access-control, max-user number and the idle-timeout, etc.

Syntax

```
show ip http configuration
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of the HTTP server:

```
Switch(config)# show ip http configuration
```

69.16 show ip http secure-server

Description

The **show ip http secure-server** command is used to display the global configuration of SSL.

Syntax

```
show ip http secure-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSL:

```
Switch(config)# show ip http secure-server
```

Chapter 70 SSH Commands

SSH (Security Shell) can provide the unsecured remote management with security and powerful authentication to ensure the security of the management information.

70.1 ip ssh server

Description

The **ip ssh server** command is used to enable SSH function. To disable the SSH function, please use **no ip ssh server** command.

Syntax

ip ssh server
no ip ssh server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the SSH function:

```
Switch(config)# ip ssh server
```

70.2 ip ssh port

Description

The **ip ssh port** command is used to configure the port for SSH service. To set the value to the default, please use **no ip ssh port** command.

Syntax

ip ssh port *port*
no ip ssh port

Parameter

port — Set the port number. It ranges from 1 to 65535. The default value is 22.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the SSH port number as 22:

```
Switch(config)# ip ssh port 22
```

70.3 ip ssh algorithm

Description

The **ip ssh algorithm** command is used to configure the algorithm in SSH function. To disable the specified algorithm, please use **no ip ssh algorithm** command.

Syntax

ip ssh algorithm { AES-CBC | 3DES-CBC | AES-GCM | AES-CTR |
HMAC-SHA1 | HMAC-SHA2 | HMAC-MD5 | UMAC }

no ip ssh algorithm

Parameter

AES-CBC | 3DES-CBC | AES-GCM | AES-CTR | HMAC-SHA1 |
HMAC-SHA2 | HMAC-MD5 | UMAC — Specify the SSH
algorithm.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the SSH algorithm as AES-CBC:

```
Switch(config)# ip ssh algorithm AES-CBC
```


70.4 ip ssh algorithm compatibility

Description

The **ip ssh algorithm compatibility** command is used to configure enable compatibility configuration to allow SSH to use unsafe encryption algorithms.

Syntax

ip ssh algorithm compatibility

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable compatibility configuration to allow SSH to use unsafe encryption algorithms:

```
Switch#ip ssh algorithm compatibility
```

This command will synchronously enable unsafe algorithms such as AES-CBC, 3DES-CBC, HMAC-SHA1, HMAC-MD5, etc. (yes/no)

70.5 ip ssh session-timeout

Description

The **ip ssh session-timeout** command is used to configure the SSH session idle timeout. To restore to the factory defaults, use **no ip ssh session-timeout** command.

Syntax

ip ssh session-timeout *value*

no ip ssh session-timeout

Parameter

value—— SSH session idle timeout in seconds. It ranges from 60 to 36000 in seconds. By default, this value is 360 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the SSH session idle timeout as 360 seconds:

```
Switch(config)# ip ssh session-timeout 360
```

70.6 ip ssh max-client

Description

The **ip ssh max-client** command is used to specify the maximum number of the connections to the SSH server. To return to the default configuration, please use **no ip ssh max-client** command.

Syntax

ip ssh max-client *num*

no ip ssh max-client

Parameter

num — The maximum number of the connections to the SSH server. It ranges from 1 to 5. By default, this value is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the maximum number of the connections to the SSH server as 3:

```
Switch(config)# ip ssh max-client 3
```

70.7 ip ssh download

Description

The **ip ssh download** command is used to download the SSH key file from TFTP server.

Syntax

ip ssh download { v2 } *key-file* **ip-address** *ip-addr* [**vrf** *vrf-name*]

Parameter

v2 — Select the type of SSH public key as SSH-2.

key-file — The name of the key-file which is selected to download. The length of the name ranges from 1 to 25 characters. The key length of the downloaded file must be in the range of 512 to 3072 bits.

ip-addr — The IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

vrf-name — VRF instance name (1-15 characters).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download an SSH-2 type key file named ssh-key from TFTP server with the IP address 192.168.0.148:

```
Switch(config)# ip ssh download v2 ssh-key ip-address 192.168.0.148
```

Download an SSH-2 type key file named ssh-key from TFTP server with the IP address fe80::1234:

```
Switch(config)# ip ssh download v2 ssh-key ip-address fe80::1234
```

70.8 remove public-key

Description

The **remove public-key** command is used to remove the SSH public key from the switch.

Syntax

remove public-key { v2 }

Parameter

v2 — Select the type of SSH public key as SSH-2.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Remove the SSH-2 type public key from the switch:

```
Switch# remove public-key v2
```

70.9 show ip ssh

Description

The **show ip ssh** command is used to display the global configuration of SSH.

Syntax

show ip ssh

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSH:

```
Switch(config)# show ip ssh
```

Chapter 71 Telnet Commands

71.1 telnet

Description

The **telnet** command is used to log in and manage other devices via telnet.

Syntax

telnet *ip-addr*

Parameter

ip-addr—The IP address of the device you want to log in.

Command Mode

Privileged EXEC Mode

Privilege Requirement

None.

User Guidelines

Make sure the switch can access the device, and the device can be logged in via telnet.

Example

Log in to a device with the IP address of 192.168.0.10:

```
Switch# telnet 192.168.0.10
```

71.2 telnet enable

Description

The **telnet enable** command is used to enable the Telnet function. To disable the Telnet function, please use the **telnet disable** command. This function is enabled by default.

Syntax

telnet enable

telnet disable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Disable the Telnet function:

```
Switch(config)# telnet disable
```

71.3 telnet port

Description

The **telnet port** command is used to configure the telnet port number. To restore the setting, please use the **no telnet port** command.

Syntax

telnet port *port*

no telnet port

Parameter

port—The number of telnet port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the telnet port number as 566:

```
Switch(config)# telnet port 566
```

71.4 show telnet-status

Description

The **show telnet-status** command is used to display the configuration information of the Telnet function.

Syntax

show telnet-status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display whether the Telnet function is enabled:

```
Switch(config)# show telnet-status
```

Chapter 72 Serial Port Commands



Note: Serial Port commands are only available on certain devices.

72.1 serial_port baud-rate

Description

The **serial_port baud-rate** command is used to configure the communication baud rate on the console port. To return to the default baud rate, please use **no serial_port** command.

Syntax

serial_port baud-rate { 9600 | 19200 | 38400 | 57600 | 115200 }

no serial_port

Parameter

9600 | 19200 | 38400 | 57600 | 115200 —Specify the communication baud rate on the console port. The default baud rate is 38400 bps.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the communication baud rate on the console port to the default value:

```
Switch(config)# no serial_port
```


Chapter 73 AAA Commands

AAA stands for authentication, authorization and accounting. This feature is used to authenticate users trying to log in to the switch or trying to access the administrative level privilege.

- **Applicable Access Application**

The authentication can be applied on the following access applications: Telnet, SSH and HTTP.

- **Authentication Method List**

A method list describes the authentication methods and their sequence to authenticate a user. The switch supports Login List for users to gain access to the switch, and Enable List for normal users to gain administrative privileges.

- **RADIUS/TACACS+ Server**

User can configure the RADIUS/TACACS+ servers for the connection between the switch and the server.

- **Server Group**

User can define the authentication server group with up to several servers running the same secure protocols, either RADIUS or TACACS+. Users can set these servers in a preferable order, which is called the server group list. When a user tries to access the switch, the switch will ask the first server in the server group list for authentication. If no response is received, the second server will be queried, and so on.

73.1 tacacs-server host

Description

The **tacacs-server host** command is used to configure a new TACACS+ server. To delete the specified TACACS+ server, please use **no tacacs-server host** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

```
tacacs-server host ip-address [ port port-id ] [ timeout time ] [ vrfName vrf-name ] [ key { [ 0 ] string | 6 encrypted-string | 7 encrypted-string } ]  
no tacacs-server host ip-address
```

Parameter

ip-address—— Specify the IP address of the TACACS+ server.

port-id—— Specify the server's port number for AAA. By default it is 49.

time—— Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

vrf-name——Specify the vrf name of the TACACS server. By the default it is default.

[0] *string* | 6 *encryped-string* | 7 *encrypted-string*—— 0, 6 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 6 indicates a symmetric encrypted password with fixed length will follow (AES-128). 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages. "*encrypted-string*" is a symmetric encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The TACACS+ servers you configured are added in the server group "tacacs" by default.

Example

Configure a TACACS+ server with the IP address as 1.1.1.1, TCP port as 1500, timeout as 6 seconds, VRF instance asv1, and the unencrypted key string as 12345.

```
Switch(config)# tacacs-server host 1.1.1.1 port 1500 timeout 6 vrfName  
v1 key 12345
```

73.2 show tacacs-server

Description

This **show tacacs-server** command is used to display the summary information of the TACACS+ servers.

Syntax

show tacacs-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the TACACS+ servers:

```
Switch(config)# show tacacs-server
```

73.3 radius-server host

Description

The **radius-server host** command is used to configure a new RADIUS server. To delete the specified RADIUS server, please use **no radius-server host** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

radius-server host *ip-address* [**alias** *name*] [**auth-port** *port-id*] [**acct-port** *port-id*] [**timeout** *time*] [**retransmit** *number*] [**nas-id** *nas-id*] [**vrfName** *vrf-name*] [**radsec-enable** *radsec-enable*] [**verify-enable** *verify-enable*] [**tls-port** *port*] [**tls-idletimeout** *idletimeout*] [**tls-connectiontimeout** *connectiontimeout*] [**tls-retrys** *retrys*] [**certificate** *certificate*] [**client-profile-id** *client-profile-id*] [**key** {[0] *string* | 6 *encrypted-string* | 7 *encrypted-string*}]

no radius-server host *ip-address*

Parameter

name — Specify the name of this RADIUS server.

ip-address — Specify the IP address of the RADIUS server.

auth-port *port-id* — Specify the UDP destination port for authentication requests. By default it is 1812.

acct-port *port-id* — Specify the UDP destination port for accounting requests. By default it is 1813.

time—— Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

number—— Specify the number of times a RADIUS request is resent to a server if the server is not responding in time. By default it is 2 times.

nas-id——Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

vrf-name——Specify the vrf name of the RADIUS server. By the default it is default.

radsec-enable: RADSEC state (enabled/disabled).

verify-enable: State of validating RADIUS server certificate (enabled/disabled).

port: RADIUS server listening port, ranging from 1 to 65535.

idletimeout: TLS tunnel idle timeout, ranging from 10 to 60.

connectiontimeout: TLS connection timeout, ranging from 1 to 9.

retrys: Number of send attempts, ranging from 1 to 5.

certificate: Certificate template name.

client-profile-id: Client template name and client key

[0] *string* | 6 *encryped-string* | 7 *encrypted-string*—— 0, 6 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 6 indicates a symmetric encrypted password with fixed length will follow (AES-128). 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages. "*encrypted-string*" is a symmetric encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The RADIUS servers you configured are added in the server group "radius" by default.

Example

Configure a RADIUS server with an IP address of 1.1.1.1, an auth-port of 1200, a timeout of 6, a retransmit of 3, a VRF instance of v1, and a key of 12345:

```
Switch(config)# radius-server host 1.1.1.1 auth-port 1200 timeout 6  
retransmit 3 vrfName v1 key 12345
```

73.4 radius-server radsec-profile

Description

The **radius-server radsec-profile** command is used to create a RADSEC template with a specified name and enter its configuration mode. To delete the RADSEC template with the corresponding name, please use the **no radius-server radsec-profile** command.

Syntax

```
radius-server radsec-profile name  
no radius-server radsec-profile name
```

Parameter

name: The name of the radsec-profile.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a RADSEC template named test:

```
Switch(config)#radius-server radsec-profile test
```

73.5 download ca-certificate

Description

The **download ca-certificate** command is used to download the CA certificate.

Syntax

download ca-certificate *filename* **ip** *ipaddress*

Parameter

filename: The name of the certificate file to be imported, which should be a PEM file.

ipaddress: TFTP server IP address.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Import the certificate file named clntcert.pem as the CA certificate, with the TFTP server address as 192.168.0.146:

```
Switch(config)#radius-server radsec-profile test
Switch(radsec-certificate)#download ca-certificate clntcert.pem ip
192.168.0.146
```

73.6 download client-certificate

Description

The **download client-certificate** command is used to download the client certificate provided by the user.

Syntax

download client-certificate *filename* **ip** *ipaddress*

Parameter

filename: The name of the certificate file to be imported, which should be a PEM file.

ipaddress: TFTP server IP address.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Import the certificate file named clntcert.pem as the client certificate, with the TFTP server address set to 192.168.0.146:

```
Switch(config)#radius-server radsec-profile test
Switch(radsec-certificate)#download client-certificate clntcert.pem ip
192.168.0.146
```

73.7 download client-key

Description

The **download client-key** command is used to download the private key file provided by the user.

Syntax

download client-certificate *filename* **ip** *ipaddress* **password** *password*

Parameter

filename: The name of the certificate file to be imported, which should be a PEM file.

ipaddress: TFTP server IP address.

password: Private key file password.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Import the file named clntkey.pem as the private key, the TFTP server address is 192.168.0.146, and the private key file password is key123:

```
Switch(config)#radius-server radsec-profile test  
  
Switch(radsec-certificate)#download client-certificate clntcert.pem ip  
192.168.0.146 password key123
```

73.8 show radius-server

Description

This **show radius-server** command is used to display the summary information of the RADIUS servers.

Syntax

```
show radius-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the RADIUS servers:

```
Switch(config)# show radius-server
```

73.9 show radius-server certificate

Description

This **show radius-server certificate** command is used to display the certificate directory and the corresponding certificate names.

Syntax

```
show radius-server certificate
```


Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the certificate directory and corresponding certificate names:

```
Switch(config)# show radius-server certificate
```

73.10 radius-server load-balance algorithm

Description

The **radius-server load-balance algorithm** command is used to configure the load-balancing algorithm.

Syntax

radius-server load-balance algorithm *method*

Parameter

method: RADIUS server load balancing algorithm (message-based/user-based).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the load balancing algorithm of the RADIUS server group to message-based:

```
Switch(config)#radius-server load-balance algorithm message-based
```

73.11 radius-server load-balance least-outstanding

Description

The **radius-server load-balance least-outstanding** command is used to configure the load balancing batch of the RADIUS server.

Syntax

radius-server load-balance least-outstanding *Batch_size*

Parameter

Batch_size: RADIUS server batch, ranging from 1 to 100, and the default value is 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the RADIUS server load balancing batch size to 50:

```
Switch(config)#radius-server load-balance least-outstanding 50
```

73.12 radius-server dead-count

Description

The **radius-server dead-count** command is used to configure the maximum number of consecutive non-responses during the RADIUS server status detection process.

Syntax

radius-server dead-count *dead-count*

Parameter

dead-count: Maximum number of consecutive non-responses during the RADIUS server status detection process, ranging from 1 to 6, and the default value is 2.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the maximum number of consecutive non-responses during the RADIUS server status detection process to 3:

```
Switch(config)#radius-server dead-count 3
```

73.13 radius-server dead-cycle

Description

The **radius-server dead-cycle** command is used to configure the number of cycles in the detection period during the RADIUS server status detection process.

Syntax

radius-server dead-cycle *dead-cycle*

Parameter

dead-cycle: Maximum number of consecutive non-responses during the RADIUS server status detection process, ranging from 1 to 6, and the default value is 2.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the number of cycles in the detection period during the RADIUS server status detection process to 3:

```
Switch(config)#radius-server dead-cycle 3
```

73.14 radius-server dead-interval

Description

The **radius-server dead-interval** command is used to configure the detection period of the RADIUS server status detection process.

Syntax

radius-server dead-interval *dead-interval*

Parameter

dead-interval: Maximum number of consecutive non-responses during the RADIUS server status detection process, ranging from 1 to 15s, and the default value is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the detection period of the RADIUS server status detection process to 10s:

```
Switch(config)#radius-server dead-interval 10
```

73.15 radius-server dead-time

Description

The **radius-server dead-time** command is used to configure the duration that the RADIUS server remains in the down state.

Syntax

radius-server dead-time *dead-time*

Parameter

dead-time: After the device marks the RADIUS server status as Down, it will set the server status to Force-up within the set dead-time. The range is 1~900s, and the default value is 300.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the duration for the RADIUS server in the down state to 600s:

```
Switch(config)#radius-server dead-time 600
```

73.16 radius-server max-unresponsiveinterval

Description

The **radius-server max-unresponsiveinterval** command is used to configure the maximum unresponsive interval of the RADIUS server.

Syntax

radius-server max-unresponsiveinterval *interval*

Parameter

interval: The maximum unresponsive interval of the RADIUS server. The range is 1~900s, and the default value is 300.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the maximum unresponsive interval of the RADIUS server to 600s:

```
Switch(config)#radius-server max-unresponsiveinterval 600
```

73.17 radius-server testuser

Description

The **radius-server testuser** command is used to configure the user name and password used by the automatic detection function.

Syntax

radius-server testuser *username password*

Parameter

username: Username used by the automatic detection function, 64 characters/numbers at most.

password: Password used by the automatic detection function, 64 characters/numbers at most.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Set the user name used for the automatic detection function to test and the password to key123:

```
Switch(config)#radius-server testuser test key123
```

73.18 radius-server detect-server

Description

The **radius-server detect-server** command is used to configure the interval and timeout used by the automatic detection function. To disable this feature, please use the **no radius-server detect-server** command.

Syntax

```
radius-server detect-server { interval interval | timeout timeout }
```

Parameter

interval: The automatic detection interval of the RADIUS server in the down state, ranging from 1-200s, and the default value is 60.

timeout: The automatic detection timeout, ranging from 1-9s, the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the interval and timeout used by the automatic detection function to 6s:

```
Switch(config)# radius-server detect-server timeout 6
```

73.19 aaa group

Description

This **aaa group** command is used to create AAA server groups to group existing TACACS+/RADIUS servers for authentication. This command puts the switch in the server group subconfiguration mode.

To delete the corresponding AAA group, please use the **no aaa group** command.

Syntax

```
aaa group { radius | tacacs } group-name  
no aaa group { radius | tacacs } group-name
```

Parameter

radius | tacacs — Specify the server group type as RADIUS or TACACS+.

group-name — Specify the server group name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a RADIUS server group with the name radius1:


```
Switch(config)# aaa group radius radius1
```

73.20 server

Description

This **server** command is used to add the existing server in the defined server group. To remove the specified server from the server group, please use the **no server** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

```
server ip-address [ vrfName vrf-name ]  
no server ip-address [ vrfName vrf-name ]
```

Parameter

ip-address—— Specify the server's IP address.

vrf-name——Specify the vrf name of the server. By the default it is default.

Command Mode

Server Group Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create the RADIUS server 1.1.1.1 and VRF address v1 to RADIUS server group "rad copy startup-config tftp command is used to backup the configuration file to TFTP server ius1":

```
Switch(config)# aaa group radius radius1  
Switch(aaa-group)# server 1.1.1.1 vrfName v1
```

73.21 server-alias

Description

The **server-alias** command is used to add the existing server in the defined server group by its alias. To remove the specified server from the server group, please use the **no server-alias** command.

Syntax

server-alias *name*

no server-alias *name*

Parameter

name — Specify the alias of the server

Command Mode

Server Group Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a RADIUS server 1.1.1.1 and assign it an alias "test", then add it to the RADIUS group "rad" via the alias:

```
Switch(config)#radius-server host 1.1.1.1 alias test key 123
```

```
Switch(config)#aaa group radius rad
```

```
Switch(aaa-group)#server-alias test
```

73.22 show aaa group

Description

This **show aaa group** command is used to display the summary information of the AAA groups. All the servers in this group will be listed if you specify the group name.

Syntax

show aaa group [*group-name*]

Parameter

group-name — Specify the server group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the server groups:

```
Switch(config)# show aaa group
```

73.23 aaa authentication login

Description

This **aaa authentication login** command is used to configure a login authentication method list. A method list describes the authentication methods and their sequence to authenticate a user. To delete the specified authentication method list, please use the **no aaa authentication login** command.

Syntax

```
aaa authentication login { method-list } { method1 } [ method2 ] [ method3 ]  
[ method4 ]  
no authentication login method-list
```

Parameter

method-list—— Specify the method list name.

method1, method2, method3, method4—— Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for login.

Users can also define new method with the [aaa group](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the login authentication method list is "default" with "local" as method1.

Example

Configure a login authentication method list "list1" with the priority1 method as radius and priority2 method as local:

```
Switch(config)# aaa authentication login list1 radius local
```

73.24 aaa authentication enable

Description

This **aaa authentication enable** command is used to configure a privilege authentication method list. A method list describes the authentication methods and their sequence to elevate a user's privilege. To delete the specified authentication method list, please use the **no aaa authentication enable** command.

Syntax

```
aaa authentication enable { method-list } { method1 } [ method2 ] [ method3 ]  
[ method4 ]
```

```
no authentication enable method-list
```

Parameter

method-list — Specify the method list name.

method1, method2, method3, method4 — Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for privilege elevation.

Users can also define new method with the [aaa group](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the enable authentication method is "default" with "none" as method1.

Example

Configure a privilege authentication method list "list2" with the priority1 method as radius and priority2 method as local:

```
Switch(config)# aaa authentication enable list2 radius local
```

73.25 aaa authentication dot1x default

Description

This **aaa authentication dot1x default** command is used to configure an 802.1x authentication method list. A method list describes the authentication methods for users' login in 802.1x. To delete the default authentication method list, please use the **no aaa authentication dot1x default** command.

Syntax

aaa authentication dot1x default { *method* }

no aaa authentication dot1x default

Parameter

method—— Specify the method name. Only RADIUS server group is supported, and the default method is server group "radius".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1x authentication method as "radius1":

```
Switch(config)# aaa authentication dot1x default radius1
```

73.26 aaa accounting dot1x default

Description

This **aaa accounting dot1x default** command is used to configure an 802.1x accounting method list. To delete the default accounting method list, please use the **no aaa accounting dot1x default** command.

Syntax

```
aaa accounting dot1x default { method }  
no aaa accounting dot1x default
```

Parameter

method—— Specify the method name. Only RADIUS server group is supported, and the default method is server group "radius".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1x accounting method as "radius1":

```
Switch(config)# aaa accounting dot1x default radius1
```

73.27 show aaa authentication

Description

This **show aaa authentication** command is used to display the summary information of the authentication login, enable and dot1x method list.

Syntax

```
show aaa authentication [ login | enable | dot1x ]
```

Parameter

login | enable | dot1x —— Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the authentication method lists:

```
Switch(config)# show aaa authentication
```

73.28 show aaa accounting

Description

This **show aaa accounting** command is used to display the summary information of the accounting method list.

Syntax

```
show aaa accounting [ dot1x ]
```

Parameter

dot1x — Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the default 802.1x accounting method list:

```
Switch(config)# show aaa accounting
```

73.29 line telnet

Description

The **line telnet** command is used to enter the Line Configuration Mode to configure the telnet terminal line to which you want to apply the authentication list.

Syntax

line telnet

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the telnet terminal line configuration mode:

```
Switch(config)#line telnet
```

73.30 login authentication (telnet)

Description

The **login authentication** command is used to apply the login authentication method list to the telnet terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list—— Specify the login method list on the telnet terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the telnet terminal line as "list1":

```
Switch(config)#line telnet
```



```
Switch(config-line)# login authentication list1
```

73.31 line ssh

Description

The **line ssh** command is used to enter the Line Configuration Mode to configure the ssh terminal line to which you want to apply the authentication list.

Syntax

```
line ssh
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the ssh terminal line configuration mode:

```
Switch(config)#line ssh
```

73.32 login authentication (ssh)

Description

The **login authentication** command is used to apply the login authentication method list to the ssh terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

```
login authentication { method-list }
```

```
no login authentication
```

Parameter

method-list—— Specify the login method list on the ssh terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the ssh terminal line as "list1":

```
Switch(config)# line ssh
Switch(config-line)# login authentication list1
```

73.33 line console



Note: This command is only available on certain devices.

Description

The **line console** command is used to enter the Line Configuration Mode to configure the console terminal line to which you want to apply the authentication list.

Syntax

line console *line-number*

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the console 0 terminal line configuration mode:

```
Switch(config)#line console 0
```

73.34 login authentication (console)



Note: This command is only available on certain devices.

Description

The **login authentication** command is used to apply the login authentication method list to the console terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list—— Specify the login method list on the console terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the console 0 terminal line as "list1":

```
Switch(config)# line console 0
```

```
Switch(config-line)# login authentication list1
```

73.35 enable authentication (telnet)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the telnet terminal line. To restore to the default

authentication method list, please use the **no enable authentication** command.

Syntax

enable authentication { *method-list* }
no enable authentication

Parameter

method-list—— Specify the enable method list on the telnet terminal line. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the telnet terminal line as "list2":

```
Switch(config)#line telnet
Switch(config-line)# enable authentication list2
```

73.36 enable authentication (ssh)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the ssh terminal line. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

enable authentication { *method-list* }
no enable authentication

Parameter

method-list—— Specify the enable method list on the ssh terminal line. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the ssh terminal line as "list2":

```
Switch(config)# line ssh
```

```
Switch(config-line)# enable authentication list2
```

73.37 enable authentication (console)



Note: This command is only available on certain devices.

Description

The **enable authentication** command is used to apply the privilege authentication method list to the console terminal line. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

enable authentication { *method-list* }

no enable authentication

Parameter

method-list—— Specify the enable method list on the console terminal line. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the console 0 terminal line as "list2":

```
Switch(config)# line console 0
Switch(config-line)# enable authentication list2
```

73.38 ip http login authentication

Description

The **ip http login authentication** command is used to apply the login authentication method list to users accessing through HTTP. To restore to the default authentication method list, please use the **no ip http login authentication** command.

Syntax

```
ip http login authentication { method-list }
no ip http login authentication
```

Parameter

method-list—— Specify the login method list on the HTTP access. It is "default" by default, which contains the method "local".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the HTTP access as "list1":

```
Switch(config)# ip http login authentication list1
```

73.39 ip http enable authentication

Description

The **ip http enable authentication** command is used to apply the privilege authentication method list to users accessing through HTTP. To restore to the default authentication method list, please use the **no ip http enable authentication** command.

Syntax

ip http enable authentication { *method-list* }
no ip http enable authentication

Parameter

method-list—— Specify the enable method list on the HTTP access. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the HTTP access as "list2":

```
Switch(config)# ip http enable authentication list2
```

73.40 show aaa global

Description

This **show aaa global** command is used to display global status of AAA function and the login/enable method lists of different application modules: telnet, ssh and HTTP.

Syntax

show aaa global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the AAA function's global status and each application's method list:

```
Switch(config)# show aaa global
```

73.41 enable admin password

Description

The **enable admin password** command is used to set or change the Enable password for users to change the access level to admin. To remove the Enable password, please use **no enable admin** command. This command uses the symmetric encryption.

Syntax

```
enable admin password { [ 0 ] password | 6 encrypted-password | 7  
encrypted-password }  
no enable admin
```

Parameter

0 — Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password — Enable password, a string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are !\$%()'*, -./[]_{}. By default, it is empty. By default, it is empty.

6 — Indicates a symmetric encrypted password with fixed length will follow (AES-128). *encrypted-password* — A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

7 — Indicates a symmetric encrypted password with fixed length will follow. *encrypted-password* — A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the

encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If the password you configured here is unencrypted and the global encryption function is enabled in [service password-encryption](#), the password in the configuration file will be displayed in the symmetric encrypted form.

If both the **enable admin password** and **enable admin secret** are defined, only the latest configured password will take effect.

Example

Set the Enable password as "abc123" and unencrypted for users to change the access level to admin:

```
Switch(config)#enable admin password 0 abc123
```

73.42 enable admin secret

Description

The **enable admin secret** command is used to set or change the Enable password for users to change the access level to admin. To remove the Enable password, please use **no enable admin** command. This command uses the MD5 encryption.

Syntax

```
enable admin secret {[ 0 ] password | 4 encrypted-password | 5  
encrypted-password | 8 encrypted-password | 9 encrypted-password}  
no enable admin
```

Parameter

0 — Specify the encryption type. 0 indicates that an unencrypted password will follow. the password will be encrypted by MD5. By default, the encryption type is 0.

password — A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are !\$%()'*, -./[]_{}. By default, it is empty.

4 — Indicates an SHA256 encrypted password with fixed length will follow.

5 — Indicates an MD5 encrypted password with fixed length will follow.

8 — Indicates a PBKDF2 encrypted password with fixed length will follow.

9 — Indicates a SCRYPT encrypted password with fixed length will follow.

encrypted-password — An/A MD5/SCRYPT/PBKDF2 encrypted password with fixed length, which you can copy from another switch's configuration file.

After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **enable admin password** and **enable admin secret** are defined, only the latest configured password will take effect.

Example

Set the Enable password as "abc123" and unencrypted for users to change the access level to admin. The password will be displayed in the encrypted form.

```
Switch(config)#enable admin secret 0 abc123
```

73.43 enable-admin

Description

The **enable-admin** command is used to get the administrative privileges by a non-admin user.

Syntax

enable-admin

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only User, Power User and Operator level users have access to these commands.

Example

Get the administrative privileges (the Enable password is "123456"):

```
Switch# enable-admin
```

```
Password: 123456
```

Chapter 74 IEEE 802.1x Commands

IEEE 802.1x function is to provide an access control for LAN ports via the authentication. An 802.1x system include three entities: supplicant, authenticator and authentication server.

- Supplicant: the device that requests access to the LAN.
- Authentication server: performs the actual authentication of the supplicant. It validates the identity of the supplicant and notifies the authenticator whether or not the supplicant is authorized to access the LAN.
- Authenticator: controls the physical access to the network based on the authentication status of the supplicant. It is usually an 802.1x-supported network device, such as this TP-Link switch. It acts as an intermediary (proxy) between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant.

This chapter handles with the authentication process between the supplicant and the switch.

To realize the authentication and accounting function, you should also enable the AAA function and configure the RADIUS server. Go to [Chapter 42 AAA Commands](#) for more details.

74.1 dot1x system-auth-control

Description

The **dot1x system-auth-control** command is used to enable the IEEE 802.1x function globally. To disable the IEEE 802.1x function, please use **no dot1x system-auth-control** command.

Syntax

```
dot1x system-auth-control  
no dot1x system-auth-control
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IEEE 802.1x function:

```
Switch(config)#dot1x system-auth-control
```

74.2 dot1x handshake

Description

The **dot1x handshake** command is used enable the handshake feature. The handshake feature is used to detect the connection status between the TP-Link 802.1x supplicant and the switch. Please disable the handshake feature if you are using a non-TP-Link 802.1x-compliant client software. This feature is enabled by default.

Syntax

dot1x handshake

no dot1x handshake

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the 802.1x handshake function:

```
Switch(config)# no dot1x handshake
```

74.3 dot1x auth-protocol

Description

The **dot1x auth-protocol** command is used to configure the authentication protocol of IEEE 802.1x and the default 802.1x authentication method is "eap". To restore to the default 802.1x authentication protocol, please use **no dot1x auth-protocol** command.

Syntax

dot1x auth-protocol { pap | eap }

no dot1x auth-protocol

Parameter

pap | eap —Authentication protocols.

pap: EAP termination mode. IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP packets are terminated at the switch and repackaged in the Password Authentication Protocol (PAP) packets, and then transferred to the RADIUS server.

eap: EAP relay mode. IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP protocol packets with authentication data are encapsulated in the advanced protocol (such as RADIUS) packets and transmitted to the authentication server.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Authentication protocol of IEEE 802.1x as "pap":

```
Switch(config)#dot1x auth-protocol pap
```

74.4 dot1x vlan-assignment

Description

The **dot1x vlan-assignment** command is used to enable the VLAN assignment feature. To disable this feature, please use **no dot1x vlan-assignment** command.

802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated.

If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN.

If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN.

If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.

Syntax

dot1x vlan-assignment
no dot1x vlan-assignment

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the VLAN assignment feature:

```
Switch(config)#dot1x vlan-assignment
```

74.5 dot1x accounting

Description

The **dot1x accounting** command is used to enable the IEEE 802.1x accounting function globally. To disable the IEEE 802.1x accounting function, please use **no dot1x accounting** command.

Syntax

dot1x accounting
no dot1x accounting

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the enable the IEEE 802.1x accounting function globally:

```
Switch(config)#dot1x accounting
```

74.6 dot1x mab

Description

The **dot1x mab** command is used to enable the MAB feature on the port. To disable this feature, please use **no dot1x mab** command.

With MAB (MAC-Based Authentication Bypass) feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1x capability. For example, most printers, IP phones and fax machines do not have 802.1x capability.

Syntax

dot1x mab

no dot1x mab

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MAB feature on the Gigabit Ethernet port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#dot1x mab
```

74.7 dot1x guest-vlan

Description

The **dot1x guest-vlan** command is used to configure the Guest VLAN function on the port. To disable the Guest VLAN function, please use **no dot1x guest-vlan** command.

Syntax

```
dot1x guest-vlan vid  
no dot1x guest-vlan
```

Parameter

vid—— The VLAN ID needed to enable the Guest VLAN function, ranging from 0 to 4094. 0 means that Guest VLAN is disabled. The supplicants in the Guest VLAN can access the specified network source.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Guest VLAN function for VLAN 5 and set the VLAN ID as 20 on the Gigabit Ethernet port 1/0/1::

```
Switch(config)#interface gigabitEthernet 1/0/1  
Switch(config-if)#dot1x guest-vlan 5
```

74.8 dot1x timeout quiet-period

Description

The **dot1x timeout quiet-period** command is used to enable the quiet-period function on the port. To disable the function, please use **no dot1x timeout quiet-period** command.

Syntax

```
dot1x timeout quiet-period [ time ]  
no dot1x timeout quiet-period
```

Parameter

time—— The length of the quiet-period time. If one user's authentication fails, its subsequent IEEE 802.1x authentication requests will not be processed during the quiet-period time. It ranges from 1 to 999 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the quiet-period function and set the quiet-period as 5 seconds on the Gigabit Ethernet port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#dot1x quiet-period 5
```

74.9 dot1x timeout supp-timeout

Description

The **dot1x timeout supp-timeout** command is used to configure the supplicant timeout on the port. To restore to the default, please use **no dot1x timeout supp-timeout** command.

Syntax

```
dot1x timeout supp-timeout time
no dot1x timeout supp-timeout
```

Parameter

time —The maximum time for the switch to wait for the response from supplicant before resending a request to the supplicant, ranging from 1 to 60 in second. By default, it is 30 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the supplicant timeout value as 5 seconds on the Gigabit Ethernet port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#dot1x timeout supp-timeout 5
```

74.10 dot1x max-req

Description

The **dot1x max-req** command is used to configure the maximum transfer times of the repeated authentication request when the server cannot be connected. To restore to the default value, please use **no dot1x max-req** command.

Syntax

```
dot1x max-req times
no dot1x max-req
```

Parameter

times — The maximum transfer times of the repeated authentication request, ranging from 1 to 9 in times. By default, the value is 3.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum transfer times of the repeated authentication request as 5 on the Gigabit Ethernet port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#dot1x max-req 5
```

74.11 dot1x

Description

The **dot1x** command is used to enable the IEEE 802.1x function for a specified port. To disable the IEEE 802.1x function for a specified port, please use **no dot1x** command.

Syntax

dot1x

no dot1x

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IEEE 802.1x function for the Gigabit Ethernet port 1:

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#dot1x
```

74.12 dot1x port-control

Description

The **dot1x port-control** command is used to configure the Control Mode of IEEE 802.1x for the specified port. By default, the control mode is "auto". To restore to the default configuration, please use **no dot1x port-control** command.

Syntax

dot1x port-control {auto | authorized-force | unauthorized-force}

no dot1x port-control

Parameter

auto | authorized-force | unauthorized-force — The Control Mode for the port.

auto: In this mode, the port will normally work only after passing the 802.1x Authentication.

authorized-force: In this mode, the port can work normally without passing the 802.1x Authentication.

unauthorized-force: In this mode, the port is forbidden working for its fixed unauthorized status.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Control Mode for Gigabit Ethernet port 20 as "authorized-force":

```
Switch(config)#interface gigabitEthernet 1/0/20
Switch(config-if)#dot1x port-control authorized-force
```

74.13 dot1x port-method

Description

The **dot1x port-method** command is used to configure the control type of IEEE 802.1x for the specified port. By default, the control type is "mac-based". To restore to the default configuration, please use **no dot1x port-method** command.

Syntax

```
dot1x port-method { mac-based | port-based }
no dot1x port-method
```

Parameter

mac-based | port-based —The control type for the port.

mac-based: Any client connected to the port should pass the 802.1x authentication for access.

port-based: All the clients connected to the port can access the network on the condition that any one of the clients has passed the 802.1x Authentication.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Control Type for Gigabit Ethernet port 20 as "port-based":

```
Switch(config)#interface gigabitEthernet 1/0/20
Switch(config-if)#dot1x port-method port-based
```

74.14 dot1x auth-init

Description

The **dot1x auth-init** command is used to initialize the specific client.

Syntax

```
dot1x auth-init [ mac mac-address ]
```

Parameter

mac-address: Enter the MAC address of the client that will be unauthorized.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Initialize the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

```
Switch(Config)# interface gigabitEthernet 1/0/1
Switch(Config-if)#dot1x auth-init mac 00:02:58:4f:6c:23
```

74.15 dot1x auth-reauth

Description

The **dot1x auth-reauth** command is used to reauthenticate the specific client.

Syntax

```
dot1x auth-reauth [ mac mac-address]
```

Parameter

mac-address: Enter the MAC address of the client that will be reauthenticated.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Reauthenticate the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

```
Switch(Config)# interface gigabitEthernet 1/0/1
Switch(Config-if)#dot1x auth-reauth mac 00:02:58:4f:6c:23
```

74.16 show dot1x global

Description

The **show dot1x global** command is used to display the global configuration of 801.X.

Syntax

```
show dot1x global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of 801.X globally:

```
Switch(config)#show dot1x global
```

74.17 show dot1x interface

Description

The **show dot1x interface** command is used to display all ports or the specified port's configuration information of 801.X.

Syntax

show dot1x interface [**gigabitEthernet** *port*]

Parameter

port—— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of 801.X for Gigabit Ethernet port 20:

```
Switch(config)#show dot1x interface gigabitEthernet 1/0/20
```

Display the configuration information of 801.X for all Ethernet ports:

```
Switch(config)#show dot1x interface
```

74.18 show dot1x auth-state interface

Description

The **show dot1x auth-state interface** command is used to display the authentication status of each port.

Syntax

show dot1x auth-state interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*]

Parameter

port—— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the authentication status of each port:

```
Switch(config)#show dot1x auth-state interface
```

Chapter 75 Port Security Commands (Only for Certain Devices)

You can use the Port Security feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets. In addition, the switch can send a notification if the number of learned MAC addresses on the port exceeds the limit.

75.1 mac address-table max-mac count

Description

The **mac address-table max-mac-count** command is used to enable the port security feature of the port and configure the related parameters. To disable the feature and restore the parameters to defaults on the port, please use **no mac address-table max-mac-count** command.

Syntax

```
mac address-table max-mac-count { [ max-number num ]  
[ exceed-max-learned enable | disable ] [ mode { dynamic | static |  
permanent } ] [ status { forward | drop | disable } ] }  
no mac address-table max-mac-count [ max-number | mode | status ]
```

Parameter

num: The maximum number of MAC addresses that can be learned on a port, ranging from 0 ~ 64. The default value is 64.

status: Select the action to be taken when the number of MAC addresses reaches the maximum number of MAC addresses learned on the port. By default, this function is disabled.

forward: Forward but not learn packets after reaching the upper limit of secure addresses.

drop: Discard packets after reaching the upper limit of secure addresses.

disable: Disable port security.

exceed-max-learned {enable | disable}: When the upper limit is reached, an SNMP message will be generated and sent to the network administrator.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the maximum number of MAC addresses that can be learned on port 1/0/1 as 30, enable exceed-max-learned feature and configure the mode as permanent and the status as drop:

```
Switch (config)#interface gigabitEthernet 1/0/1  
Switch(config-if)#mac address-table max-mac-count max-number 30  
exceed-max-learned enable mode permanent status drop
```

75.2 mac address-table sticky mac

Description

The **mac address-table sticky mac** command is used to configure sticky MAC manually. To delete the specified sticky MAC entry, please use the **no mac address-table sticky mac** command.

Syntax

```
mac address-table sticky mac mac-address vip vlan-id interface  
{ fastEthernet port | gigabitEthernet port | hundred-gigabitEthernet port |  
ten-gigabitEthernet port | twentyFive-gigabitEthernet port |  
two-gigabitEthernet port }  
no mac address-table sticky mac mac-address vip vlan-id
```

Parameter

mac-address: The MAC address of the entry to be added.

vlan-id: The VLAN ID of the entry to be added. The range is 1 to 4094.

port: The port of the entry to be added.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a sticky address 00:02:58:4f:6c:23 and bind it to sticky mode port 1, VLAN 1:

```
Switch(config)#mac address-table sticky mac 00:02:58:4f:6c:23 vid 1
interface gigabitEthernet 1/0/1
```

75.3 mac address-table sticky save-time

Description

The **mac address-table sticky save-time** command is used to configure the interval for saving sticky MAC. To restore the default configuration, please use the **no mac address-table sticky save-time** command.

Syntax

mac address-table sticky save-time *time*
no mac address-table sticky save-time

Parameter

time: The interval for saving sticky MAC, which is 600s by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the save-time to 50S:

```
Switch(config)# mac address-table sticky save-time 50
```

75.4 mac address-table spoofing-defend

Description

The **mac address-table spoofing-defend** command is used to designate the interface as trusted for MAC address learning and assign it a higher priority. The switch prioritizes MAC address entries learned on this trusted port over entries learned on untrusted ports. This helps prevent MAC flapping caused by redundant paths and mitigates MAC spoofing attempts from access ports. To disable this feature, please use the **no mac address-table spoofing-defend** command.

Syntax

```
mac address-table spoofing-defend
no mac address-table spoofing-defend
```

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MAC spoofing-defend on an interface:

```
Switch(config-if)# mac address-table spoofing-defend
```

Chapter 76 MACsec Commands (Only for Certain Devices)

Media Access Control Security (MACsec) defines a method for secure data communication on IEEE 802 local area networks. MACsec provides users with secure MAC layer data transmission and reception services, including user data encryption, data frame integrity verification, and data source authenticity validation.

76.1 macsec mka-policy

Description

This command is used to configure a macsec policy template. When users configure the macsec function of a specific port, they can apply the corresponding template to simplify the configuration process. To delete the template, please use the **no** command.

Syntax

```
macsec mka-policy policy-name [confidentiality-offset offset |  
replay-protection [window-size window-size] | validation-mode mode]  
no macsec mka-policy policy-name [confidentiality-offset |  
replay-protection [window-size] | validation-mode]
```

Parameter

policy-name: MACsec policy template name.

offset: MACsec message encryption position offset. The value range is {0 | 30 | 50}, and the default value is 0.

window-size: The window size of the replay-protection function, ranging from 0 to 4294967295, and the default value is 0

mode: MACsec key matching mode, the value range is {check | strict}, and the default value is check

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a MACsec policy configuration template named test and set the validation-mode of the template to strict mode:

```
Switch(config)#macsec mka-policy test
Switch(config)#macsec mka-policy test validation-mode strict
```

76.2 macsec apply-policy

Description

This command is used to apply the MACsec policy template configuration to the corresponding interface. To delete the policy, please use the **no macsec apply-policy** command.

Syntax

```
macsec apply-policy policyName
no macsec apply-policy
```

Parameter

policy-name: MACsec policy template name.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, and apply the MACsec policy template named test:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec apply-policy test
```

76.3 macsec cipher_suite

Description

This command is used to configure the MACsec packet encryption algorithm. To disable this function, please use the **no macsec cipher_suite** command.

Syntax

```
macsec cipher_suite type
```

no macsec cipher_suite

Parameter

type: The encryption algorithm type used, the value is {gcm-aes-128 | gcm-aes-256}, the default value is gcm-aes-128.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, and set the cipher_suite to the gcm-aes-128 algorithm:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec cipher_suite gcm-aes-128
```

76.4 macsec confidentiality-offset

Description

This command is used to configure the cheap byte count when the macsec function encrypts packets, that is, the number of bytes after which the encryption of the packet data begins. To disable this function, please use the **no macsec confidentiality-offset** command.

Syntax

macsec confidentiality-offset offset

no macsec confidentiality-offset

Parameter

offset: The MACsec message encryption position offset. The value is {0 | 30 | 50}, and the default value is 0

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, and set the encryption offset to 30:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec confidentiality-offset 30
```

76.5 macsec desire

Description

This command is used to enable the packet encryption function. To disable this function, please use the **no macsec desire** command.

Syntax

macsec desire
no macsec desire

Parameter

None

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MACsec packet encryption function on port 1/0/2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec desire
```

76.6 macsec mka

Description

This command is used to enable the MKA negotiation function. To disable this function, please use the **no macsec mka** command.

Syntax

macsec mka
no macsec mka

Parameter

None

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MKA negotiation function on port 1/0/2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec mka
```

76.7 macsec mka priority

Description

This command is used to configure the weight of the local end in the mka negotiation. During the MKA session establishment process, the one with the lower priority value will be elected as the key server. To restore the default value, please use the **no macsec mka priority** command.

Syntax

```
macsec mka priority priority
no macsec mka priority
```

Parameter

priority: The priority of the local end in the MKA negotiation, ranging from 0 to 255. The default value is 255

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, and set the MKA negotiation priority to 20:

```
Switch(config)#interface gigabitEthernet 1/0/2
```

76.8 macsec mka psk

Description

This command is used to configure the local pre-configured security connection associated key information in the MKA negotiation. To disable this function, please use the **no macsec mka psk ckn cak** command.

Syntax

macsec mka psk ckn name **cak** string

no macsec mka psk ckn cak

Parameter

name: The name of the local pre-configured security connection association key used for MKA negotiation.

string: The value of the local pre-configured security connection association key used for MKA negotiation

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, and set the pre-configured security connection association key name to "test" and its value to "abcdefg":

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#macsec mka psk ckn test cak abcdefg
```

76.9 macsec mka timer

Description

This command is used to configure the mka session keepalive time that times out due to failure to receive mka messages from the peer. To disable this function, please use the **no macsec mka timer mka-life** command.

Syntax

macsec mka timer mka-life seconds

no macsec mka timer mka-life

Parameter

seconds: MKA session timeout keepalive time, ranging from 6-60s. The default value is 21s.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, and set the timeout keepalive time to 6s:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec mka timer mka-life 6
```

76.10 macsec replay-protection

Description

This command is used to enable replay-protection and the window range for allowing packets to pass. When replay-protection is disabled, out-of-order packets will not be received; when it is enabled, out-of-order packets within the window range will be received. To disable this function, please use the **no macsec replay-protection [window-size]** command.

Syntax

macsec replay-protection [window-size size-value]

no macsec replay-protection [window-size]

Parameter

size-value: Window size, ranging from 0 to 4294967295. The default value is 0.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, enable replay-protection and

set the window size to 10:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec replay-protection
Switch(config-if)#macsec replay-protection window-size 10
```

76.11 macsec validation-mode

Description

This command is used to set the validation mode of ICK information in the MKA negotiation process. When configured in strict mode, the ICK information will be strictly matched. When the ICK information carried in the received MKA message is inconsistent with that of the local end, the message will be discarded; when configured in check mode, only the ICK information is checked. When the ICK information carried in the received MKA message is inconsistent with that of the local end, it will still be parsed normally, but the MKA session will not be established. To disable this function, please use the **no macsec validation-mode** command.

Syntax

```
macsec validation-mode mode
no macsec validation-mode
```

Parameter

mode: The matching mode of ICK information in the MKA negotiation, the value range is {check | strict}, and the default value is check.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MACsec function on port 1/0/2, and set validation-mode to strict mode:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#macsec validation-mode strict
```

Chapter 77 Port Mirroring Commands

Port Mirroring allows the switch to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic on source ports, LAGs or the CPU. Usually, the monitoring port is connected to data diagnose device, which is used to analyze the monitored packets for monitoring and troubleshooting the network.

77.1 monitor session destination interface

Description

The **monitor session destination interface** command is used to configure the monitoring port. Each monitor session has only one monitoring port. To change the monitoring port, please use the **monitor session destination interface** command by changing the port value. The **no monitor session** command is used to delete the corresponding monitoring port or monitor session.

Syntax

```
monitor session session_num destination interface gigabitEthernet port  
no monitor session session_num destination interface gigabitEthernet port  
no monitor session session_num
```

Parameter

session_num — The monitor session number, can only be specified as 1.
port — The monitoring port number.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create monitor session 1 and configure port 1/0/1 as the monitoring port:

```
Switch(config)# monitor session 1 destination interface gigabitEthernet  
1/0/1
```

Delete the monitoring port 1/0/2 from monitor session 1:

```
Switch(config)# no monitor session 1 destination interface  
gigabitEthernet 1/0/2
```

Delete the monitor session 1:

```
Switch(config)# no monitor session 1
```

77.2 monitor session source

Description

The **monitor session source** command is used to configure the monitored interface. To delete the corresponding monitored interface, please use **no monitor session source** command.

Syntax

```
monitor session session_num source { cpu cpu_number | interface  
gigabitEthernet port-list | interface port-channel port-channel-id } mode  
no monitor session session_num source { cpu cpu_number | interface  
gigabitEthernet port-list | interface port-channel port-channel-id } mode
```

Parameter

session_num—— The monitor session number. It can only be specified as 1.

cpu_number—— The CPU number. It can only be specified as 1.

port-list—— List of the Ethernet port number. It is multi-optional.

lag-list—— List of LAG interfaces. It is multi-optional.

mode—— The monitor mode. There are three options: rx, tx and both. Rx (ingress monitoring mode), means the incoming packets received by the monitored interface will be copied to the monitoring port. Tx (egress monitoring mode), indicates the outgoing packets sent by the monitored interface will be copied to the monitoring port. Both (ingress and egress monitoring), presents the incoming packets received and the outgoing packets sent by the monitored interface will both be copied to the monitoring port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

1. The monitoring port is corresponding to current interface configuration mode.
2. Monitored ports number is not limited, but it can't be the monitoring port at the same time.
3. Whether the monitoring port and monitored ports are in the same VLAN or not is not demanded strictly.
4. The monitoring port and monitored ports cannot be link-aggregation member.

Example

Create monitor session 1, then configure port 4, 5, 7 as monitored port and enable ingress monitoring:

```
Switch(config)# monitor session 1 source interface gigabitEthernet  
1/0/4-5,1/0/7 rx
```

Delete port 4 in monitor session 1 and its configuration:

```
Switch(config)# no monitor session 1 source interface gigabitEthernet  
1/0/4 rx
```

77.3 monitor session 1 destination remote vlan

Description

The **monitor session 1 destination remote vlan** command is used to configure the RSPAN VLAN for remote port monitoring of egress packets. Please set the destination port before using this command. To disable this function, please use the **no monitor session 1 destination remote vlan** command.

Syntax

monitor session 1 destination remote vlan vlanid

no monitor session 1 destination remote vlan vlanid

Parameter

vlanid — Remote port monitoring export message VLAN. The value ranges from 2 to 4094 and is mutually exclusive with voice VLAN and internal VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the RSPAN VLAN for remote port monitoring of egress packets:

```
Switch(config)#monitor session 1 destination remote vlan 4094
```

77.4 monitor session 1 source remote vlan

Description

The **monitor session 1 source remote vlan** command is used to monitor the packets added to the RSPAN VLAN port. To disable this function, use the **no monitor session 1 source remote vlan** command.

Syntax

```
monitor session 1 source remote vlan vlanid  
no monitor session 1 source remote vlan vlanid
```

Parameter

vlanid — Remote port monitoring export message VLAN. The value ranges from 2 to 4094 and is mutually exclusive with voice VLAN and internal VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Monitor the packets added to the RSPAN VLAN port:

```
Switch(config)#monitor session 1 source remote vlan 4094
```

77.5 show monitor session

Description

The **show monitor session** command is used to display the configuration of port monitoring.

Syntax

show monitor session [*session_num*]

Parameter

session_num — The monitor session number, can only be specified as 1. It is optional.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the monitoring configuration of monitor session 1:

```
Switch(config)# show monitor session 1
```

Chapter 78 ACL Commands

ACL (Access Control List) is used to filter data packets by configuring a series of match conditions, operations and time ranges. It provides a flexible and secured access control policy and facilitates you to control the network security.

78.1 access-list create

Description

The **access-list create** command is used to create an ACL.

Syntax

access-list create *acl-id* [**name** *acl-name*]

no access-list create { *acl-id* }

Parameter

acl-id —Enter an ACL ID. The IDs for MAC ACL are from 0 to 499. The IDs for IP ACL are from 500 to 999. The IDs for Combined ACL are from 1000 to 1499. The IDs for IPv6 ACL are from 1500 to 1999. The IDs for Packet Content ACL are from 2000 to 2499.

Note: Packet Content ACL is only available on certain devices.

acl-name — Enter a name to identify the ACL.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an IP ACL whose ID is 523:

```
Switch(config)# access-list create 523
```

78.2 access-list packet-content profile



Note: This command is only available on certain devices.

Description

The **access-list packet-content profile** command is used to specify the offset of each chunk. There are four chunks to be configured. They must be configured before you configure the chunk value&mask.

Syntax

```
access-list packet-content profile chunk-offset0 offset0 chunk-offset1 offset1 chunk-offset2 offset2 chunk-offset3 offset3
```

Parameter

offset0 -offset3: Specify the offset of each chunk. The value ranges from 0 to 31. When the offset is set as 31, it matches the first 127,128, 1, 2 bytes of the packet; when the offset is set as 0, it matches the 3, 4, 5, 6 bytes, and so on, for the rest of the offset value.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a packet content profile with offset 0,1,2,3:

```
Switch(config)# access-list packet-content profile chunk-offset0 0  
chunk-offset1 1 chunk-offset2 2 chunk-offset3 3
```

78.3 access-list resequence

Description

The **access-list resequence** command is used to resequence the rules by providing a Start Rule ID and Step value.

Syntax

```
access-list resequence acl-id-or-name start start-rule-id step rule-id-step-value
```

Parameter

acl-id-or-name—— The ACL ID or name.

start-rule-id—— The start rule ID.

rule-id-step-value—— The step value.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Resequence the rules of ACL 12 with the start ID as 1 and step value as 5:

```
Switch(config)# access-list resequence 12 start 1 step 5
```

78.4 access-list mac

Description

The **access-list mac** command is used to create MAC ACL. To delete the MAC ACL, please use **no access-list mac**.

Syntax

access-list mac *acl-id-or-name* **rule** { auto | *rule-id* } { deny | permit } **logging** { enable | disable } [**smac** *source-mac* **smask** *source-mac-mask*] [**dmac** *destination-mac* **dmask** *destination-mac-mask*] [**type** *ether-type*] [**pri** *dot1p-priority*] [**vid** *vlan-id*] [**tseg** *time-range-name*]
no access-list mac *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name — Enter the ID or name of the ACL that you want to add a rule for.

auto — The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id — Assign an ID to the rule.

deny | permit — Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if "deny" is selected and forwarded if "permit" is selected.

enable | disable — Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac — Enter the source MAC address. The format is FF:FF:FF:FF:FF:FF.

source-mac-mask — Enter the mask of the source MAC address. This is required if a source MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

destination-mac — Enter the destination MAC address. The format is FF:FF:FF:FF:FF:FF.

destination-mac-mask — Enter the mask of the destination MAC address. This is required if a destination MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

ether-type — Specify an Ethernet-type with 4 hexadecimal numbers.

dot1p-priority. The user priority ranges from 0 to 7. The default is No Limit.

vlan-id — The VLAN ID ranges from 1 to 4094.

time-range-name — The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create MAC ACL 50 and configure Rule 5 to permit packets with source MAC address 00:34:a2:d4:34:b5:

```
Switch (config)#access-list create 50  
Switch (config-mac-acl)#access-list mac 50 rule 5 permit logging disable  
smac 00:34:a2:d4:34:b5 smask ff:ff:ff:ff:ff:ff
```

78.5 access-list ip

Description

The **access-list ip** command is used to add IP ACL rule. To delete the corresponding rule, please use **no access-list ip** command. IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Syntax

```
access-list ip acl-id-or-name rule {auto | rule-id} {deny | permit} logging  
{enable | disable} [sip sip-address sip-mask sip-address-mask] [dip  
dip-address dip-mask dip-address-mask] [dscp dscp-value] [tos tos-value]
```

[pre *pre-value*] [frag enable | disable] [protocol *protocol*] [s-port *s-port-number*] [s-port-mask *s-port-mask*] [d-port *d-port-number*] [d-port-mask *d-port-mask*] [tcpflag *tcpflag*] [tseg *time-range-name*] [vrf *vrf-name*]

no access-list ip *acl-id-or-name* rule *rule-id*

Parameter

acl-id-or-name — Enter the ID or name of the ACL that you want to add a rule for.

auto — The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id — Assign an ID to the rule.

deny | permit — Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if "deny" is selected and forwarded if "permit" is selected.

logging {enable | disable} — Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

src-ip-address — Enter the source IP address.

src-ip-address-mask — Enter the mask of the source IP address. This is required if a source IP address is entered.

dst-ip-address — Enter the destination IP address.

dst-ip-address-mask — Enter the mask of the destination IP address. This is required if a destination IP address is entered.

dscp-value — Specify the DSCP value between 0 and 63.

tos-value — Specify an IP ToS value to be matched between 0 and 15.

pre-value — Specify an IP Precedence value to be matched between 0 and 7.

frag {enable | disable} — Enable or disable matching of fragmented packets. The default is disable. When enabled, the rule will apply to all fragmented packets and always permit to forward the last fragment of a packet.

Note: **frag {enable | disable}** is only available on certain devices.

protocol — Specify a protocol type.

s-port-number — Specify the source port number.

s-port-mask — Specify the source port mask with 4 hexadecimal numbers.

d-port-number — Specify the destination port number.

d-port-mask—— Specify the destination port mask with 4 hexadecimal numbers.

tcpflag—— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name—— The name of the time-range. The default is No Limit.

vrf-name—— VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create IP ACL 600, and configure Rule 1 to permit packets with source IP address 192.168.1.100 and VRF v1:

```
Switch (config)#access-list create 600
Switch (config)#access-list ip 600 rule 1 permit logging disable vrf v1 sip
192.168.1.100 sip-mask 255.255.255.255
```

78.6 access-list combined

Description

The **access-list combined** command is used to add Combined ACL rule. To delete the corresponding rule, please use **no access-list extended** command.

Syntax

access-list combined *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [**smac** *source-mac-address* **smask** *source-mac-mask*] [**dmac** *dest-mac-address* **dmask** *dest-mac-mask*] [**vid** *vlan-id*] [**type** *ether-type*] [**pri** *priority*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**protocol** *protocol*] [**s-port** *s-port-number* **s-port-mask** *s-port-mask*] [**d-port** *d-port-number* **d-port-mask** *d-port-mask*]

d-port-mask *d-port-mask* [**tcpflag** *tcpflag*] [**tseg** *time-range-name*] [**vrf** *vrf-name*]

no access-list combined *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name — Enter the ID or name of the ACL that you want to add a rule for.

auto — The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id — Assign an ID to the rule.

deny | *permit* — Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {*enable* | *disable*} — Enable or disable Logging function for the ACL rule. If “enable” is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac-address — Enter the source MAC address.

source-mac-mask — Enter the source MAC address mask.

dest-mac-address — Enter the destination MAC address.

dest-mac-mask — Enter the destination MAC address mask. This is required if a destination MAC address is entered.

vlan-id: The VLAN ID ranges from 1 to 4094.

ether-type — Specify the Ethernet-type with 4 hexadecimal numbers.

priority — The user priority ranges from 0 to 7. The default is No Limit.

source-ip: Enter the source IP address.

source-ip-mask — Enter the mask of the source IP address. It is required if source IP address is entered.

destination-ip — This is required if a source IP address is entered.

destination-ip-mask — Enter the destination IP address mask. This is required if a destination IP address is entered.

dscp-value — Specify the DSCP value between 0 and 63.

tos-value — Specify an IP ToS value to be matched between 0 and 15.

pre-value — Specify an IP Precedence value to be matched between 0 and 7.

protocol — Specify a protocol type.

s-port-number—— Specify the source port number.

s-port-mask—— Specify the source port mask with 4 hexadecimal numbers.

d-port-number—— Specify the destination port number.

d-port-mask—— Specify the destination port mask with 4 hexadecimal numbers.

tcpflag—— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name—— The name of the time-range. The default is No Limit.

vrf-name—— VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create Combined ACL 1100 and configure Rule 1 to deny packets with source IP address 192.168.3.100 and VRF v1 in VLAN 2:

```
Switch(config)# access-list create 1100
Switch(config)# access-list combined 1100 rule 1 deny logging disable vid
2 vrf v1 sip 192.168.3.100 sip-mask 255.255.255.255
```

78.7 access-list ipv6

Description

The **access-list ipv6** command is used to add IPv6 ACL rule. To delete the corresponding rule, please use **no access-list ipv6** command. IPv6 ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets, the DSCP and flow-label value, etc.

Syntax

access-list ipv6 *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [**class** *class-value*] [**flow-label** *flow-label-value*] [**sip**

source-ip-address **src-mask** *source-ip-mask* [**dip** *destination-ip-address*
dip-mask *destination-ip-mask*] [**s-port** *source-port-number*] [**d-port**
destination-port-number] [**tseg** *time-range-name*] [**vrf** *vrf-name*]
no access-list ipv6 *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name — Enter the ID or name of the ACL that you want to add a rule for.

auto — The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id — Assign an ID to the rule.

deny | **permit** — Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if "deny" is selected and forwarded if "permit" is selected.

logging {**enable** | **disable**} — Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

class-value — Specify a class value to be matched. It ranges from 0 to 63.

flow-label-value — Specify a Flow Label value to be matched.

source-ip-address — Enter the source IP address. Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.

source-ip-mask — Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

destination-ip-address — Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 addresses but only the first 64 bits will be valid.

destination-ip-mask: Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

source-port-number — Enter the TCP/UDP source port if TCP/UDP protocol is selected.

destination-port-number—— Enter the TCP/UDP destination port if TCP/UDP protocol is selected.

time-range-name—— The name of the time-range. The default is No Limit.

vrf-name—— VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Before binding an IPv6 ACL to a VLAN or interface, you should configure the SDM template as "enterpriseV6" and save your configurations.

Example

Create IPv6 ACL 1600 and configure Rule 1 to deny packets with source IPv6 address CDCD:910A:2222:5498:8475:1111:3900:2020 and VRF v1:

```
Switch(config)# access-list create 1600  
Switch(config)# access-list ipv6 1600 rule 1 deny logging disable vrf v1 sip  
CDCD:910A:2222:5498:8475:1111:3900:2020 sip-mask ffff:ffff:ffff:ffff
```

78.8 access-list packet-content config



Note: This command is only available on certain devices.

Description

The **access-list packet-content config** command is used to add Packet Content ACL rule. To delete the corresponding rule, please use **no access-list packet-content config** command. Packet content ACLs analyze and process data packets based on 4 chunk match conditions, each chunk can specify a user-defined 4-byte segment carried in the packet's first 128 bytes.

Syntax

access-list packet-content config *acl-id-or-name* **rule** {auto / *rule-id*} {deny | permit} **logging** {enable | disable} [**chunk0** *value* **mask0** *mask*] [**chunk1** *value*

mask1 mask [**chunk2 value mask2 mask**] [**chunk3 value mask3 mask**] [**tseg time-segment**]

no access-list packet-content config acl-id-or-name rule rule-id

Parameter

acl-id-or-name — Enter the ID or name of the ACL that you want to add a rule for.

auto — The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id — Assign an ID to the rule.

deny | permit — Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit.

logging {enable | disable} — Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

value — Specify the chunk value, ranging from 0-ffffff.

mask — Specify the chunk mask, ranging from 0-ffffff. Chunk mask here must be written completely in 4-byte hex mode, like '0000ffff'.

time-segment — The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a packet-content ACL rule with all 4 chunks configured, the rule id is 1 and the default action is permit:

```
SwitchSwitch(config)# access-list packet-content config rule 1 permit
logging disable chunk0 45ea mask0 0000ffff chunk1 1111ffff mask1 ffffffff
chunk2 ee34 mask2 ffff0000 chunk3 7878 mask3 000ffae3
```

78.9 access-list action

Description

The **access-list action** command is used to specify a rule to be configured with policies and enter Action Configuration mode. To delete the corresponding policies, please use **no access-list action** command.

Syntax

access-list action *acl-id-or-name* **rule** *rule-id*

no access-list action *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name—— Enter the ID or name of the ACL.

rule-id—— Enter the ID of the ACL rule.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the rule 1 of ACL 200 to be configured with policies:

```
Switch(config)#access-list action 200 rule 1
```

78.10 access-list mode action-stop

Description

The **access-list mode action-stop** command is used to configure the stop mode when multiple ACL rules match. When action-stop is enabled, ACLs are evaluated by priority and processing stops at the first matched ACL.

Subsequent ACL rules are not evaluated. When action-stop is disabled, the switch evaluates all matching ACLs, and the action of the later matched ACL may override the action of an earlier matched ACL. To disable this function, use the **no access-list mode action-stop** command.

Syntax

access-list mode action-stop

no access-list mode action-stop

Parameter

None.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Stop ACL processing at the first matched rule:

```
Switch(config-router)# access-list mode action-stop
```

78.11 access-list action harddrop

Description

The **access-list action harddrop** command is used to configure the deny drop policy as a hard drop. If this function is disabled, a soft drop policy is used. To disable this function, use the **no access-list action harddrop** command.

Syntax

access-list action harddrop

no access-list action harddrop

Parameter

None.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the ACL deny drop policy to hard drop:

```
Switch(config-router)# access-list action harddrop
```

78.12 redirect nexthops ipv4

Description

The **redirect nexthops ipv4** command is used to enter the IPv4 policy-based routing (PBR) next-hop configuration mode. IPv4 packets that match the associated ACL are redirected to the configured next hop(s) based on the PBR rule. To disable this function, use the **no redirect nexthops ipv4** command.

Syntax

redirect nexthops ipv4

no redirect nexthops ipv4

Parameter

None.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enter IPv4 PBR next-hop configuration mode:

```
Switch(config-action)#redirect nexthops ipv4
```

78.13 redirect nexthops ipv6

Description

The **redirect nexthops ipv6** command is used to enter the IPv6 policy-based routing (PBR) next-hop configuration mode. IPv6 packets that match the associated ACL are redirected to the configured next hop(s) based on the PBR rule. To disable this function, use the **no redirect nexthops ipv6** command.

Syntax

redirect nexthops ipv6

no redirect nexthops ipv6

Parameter

None.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enter IPv6 PBR next-hop configuration mode:

```
Switch(config-action)#redirect nexthops ipv6
```

78.14 nhtype ecmp

Description

The **nhtype ecmp** command is used to enable ECMP mode for PBR. To disable ECMP mode, use the **nhtype standby** command.

Syntax

nhtype ecmp

Parameter

None.

Command Mode

PBR Next-hop Configuration Mode (IPv4/IPv6)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable ECMP mode for IPv4 PBR:

```
Switch(redirect-nexthops-ipv4)#nhtype ecmp
```

78.15 nhtype standby

Description

The **nhtype standby** command is used to enable the primary/standby mode for PBR. When multiple next hops are configured, one next hop is selected as the primary path. If the primary path becomes unreachable, traffic is automatically switched to a backup next hop. This is the default mode.

Syntax

nhtype standby

Parameter

None.

Command Mode

PBR Next-hop Configuration Mode (IPv4/IPv6)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the primary/standby mode for IPv4 PBR:

```
Switch(redirect-nexthops-ipv4)#nhtype standby
```

78.16 vrf

Description

The **vrf** command is used to configure the VRF instance for the redirect next hop(s). The default VRF is default. To remove the VRF configuration and set it to the default VRF, use the **no vrf** command.

Syntax

vrf *vrf-name*

no vrf

Parameter

vrf-name — The VRF instance to which the next hop of redirect belongs.

Command Mode

PBR Next-hop Configuration Mode (IPv4/IPv6)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the redirect next hop to VRF instance v1 (IPv4 PBR):

```
Switch(redirect-nexthops-ipv4)#vrf v1
```

78.17 ip-address

Description

The **ip-address** command is used to configure an IPv4 next hop for PBR redirect. A maximum of 4 next hops can be configured. To remove a configured IPv4 next hop, use the **no ip-address** command.

Syntax

ip-address *address*

no ip-address *address*

Parameter

address — IPv4 address of the redirect next hop.

Command Mode

PBR IPv4 Next-hop Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure an IPv4 redirect next hop:

```
Switch(redirect-nexthops-ipv4)#ip-address 192.168.30.2
```

78.18 ipv6-address

Description

The **ipv6-address** command is used to configure an IPv6 next hop for PBR redirect. A maximum of 4 next hops can be configured. To remove a configured IPv4 next hop, use the **no ipv6-address** command.

Syntax

ipv6-address *address*

no ipv6-address *address*

Parameter

address — IPv6 address of the redirect next hop.

Command Mode

PBR IPv6 Next-hop Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure an IPv6 redirect next hop:

```
Switch(redirect-nexthops-ipv6)# ipv6-address 2001::2
```

78.19 s-condition

Description

The **s-condition** command is used to limit the rate of the matched packets. To restore the settings to the defaults, please use **no s-condition**.

Syntax

```
s-condition rate rate burst burst-size osd { none | discard | remark dscp dscp }  
no s-condition
```

Parameter

rate—— Specify a rate, ranging from 0 to 10000000kbps.

burst-size—— Specify the number of bytes allowed in one second ranging from 1 to 128.

osd ——Select either "none" or "discard" as the action to be taken for the packets whose rate is beyond the specified rate. The default is None. When "remark dscp" is selected, you also need to specify the DSCP value for the matched packets. The DSCP value ranges from 0 to 63.

Note: Remark DSCP is only available on certain devices.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a policy for rule 1 of ACL 6: limit the transmission rate of the matched packets as 1000 Kbps and if the number of bytes per second is beyond 100, the packets will be discarded by the switch:

```
Switch(config)#access-list action 6 rule 1
```

```
Switch(config-action)# s-condition rate 1000 burst 100 osd discard
```

78.20 s-mirror

Description

The **s-mirror** command is used to define the policy to mirror the matched packets to the desired port. To disable this policy, please use **no s-mirror** command.

Syntax

```
s-mirror interface { fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port }
```

Parameter

port — The destination port to which the packets will be mirrored.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a policy for rule 1 of ACL 6: specify the mirror port as Gigabit Ethernet port 1/0/2 for the data packets matching this rule:

```
Switch(config)#access-list action 6 rule 1
```

```
Switch(config-action)#s-mirror interface gigabitEthernet 1/0/2
```

78.21 qos-remark

Description

The **qos-remark** command is used to configure QoS Remark function of policy action. To restore the settings to the default, please use **no qos-remark**.

Syntax

```
qos-remark [ dscp dscp ] [ priority pri ] [dot1p dot1p-pri]  
no qos-remark
```

Parameter

dscp—— DSCP of QoS Remark. Specify the DSCP region for the data packets matching the corresponding ACL. DSCP ranges from 0 to 63. By default, it is not limited.

pri—— Local Priority of QoS Remark. Specify the local priority for the data packets matching the corresponding ACL. Local Priority ranges from 0 to 7.

dot1p-pri—— 802.1P priority of QoS Remark. This remark configuration will change the data packet's 802.1P priority field to the dot1p-pri you set. 802.1P priority ranges from 0 to 7.



Note: The DSCP and dot1p cannot be configured at the same time.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a policy for rule 1 of ACL 6: specify the DSCP region as 30 and local priority 2 for the packets matching this rule:

```
Switch(config)#access-list action 6 rule 1
```

```
Switch(config-action)# qos-remark dscp 30 priority 2
```

78.22 access bind

Description

The **access-list policy name** command is used to add Policy. To delete the corresponding Policy, please use **no access-list policy name** command. A Policy is used to control the data packets those match the corresponding ACL rules.

Syntax

```
access-list bind acl-id-or-name interface { [vlan vlan-list] | [fastEthernet port-list] | [gigabitEthernet port-list] | [ten-gigabitEthernet port-list] }
```

```
no access-list bind acl-id-or-name interface { [vlan vlan-list] | [fastEthernet port-list] | [gigabitEthernet port-list] | [ten-gigabitEthernet port-list] }
```

Parameter

acl-id-or-name—— Enter the ID or name of the ACL that you want to add a rule for.

vlan-list—— Specify the ID or the ID list of the VLAN(s) that you want to bind the ACL to. The valid values are from 1 to 4094, for example, 2-3,5.

port-list—— Specify the number or the list of the Ethernet port that you want to bind the ACL to.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind ACL 1 to port 3 and VLAN 4:

```
Switch(config)#access-list bind 1 interface vlan 4 gigabitEthernet 1/0/3
```

78.23 show access-list

Description

The **show access-list** command is used to display configuration of ACL.

Syntax

show access-list *acl-id-or-name*

Parameter

acl-id-or-name—— The ID or name of the ACL selected to display the configuration.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the MAC ACL whose ID is 20:

```
Switch(config)# show access-list 20
```

78.24 show access-list bind

Description

The **show access-list bind** command is used to display the configuration of ACL binding.

Syntax

show access-list bind

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Policy bind:

```
Switch(config)# show access-list bind
```

78.25 show access-list status

Description

The **show access-list status** command is used to display usage status of ACL entry resource.

Syntax

show access-list status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the usage status of ACL entry resource:

```
Switch(config)# show access-list status
```


78.26 show access-list counter

Description

The **show access-list counter** command is used to display the packet counter of a specified ACL.

Syntax

show access-list *acl-id-or-name* **counter**

Parameter

acl-id-or-name—— The ID or name of the ACL to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the packet counter of ACL 100:

```
Switch(config)# show access-list 100 counter
```

78.27 clear access-list

Description

The **clear access-list** command is used to clear the counter of matched packets of a specified ACL or rule.

Syntax

clear access-list *acl-id-or-name* [**rule** *rule-id*]

Parameter

acl-id-or-name—— The ID or name of the ACL.

rule-id—— The ID of the rule.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the packet counter of ACL 100:

```
Switch(config)# clear access-list 100
```


Chapter 79 IPv4 IMPB Commands

You can bind the IP address, MAC address, VLAN and the connected Port number of the Host together, which can be the condition for the ARP Inspection and IP verify source to filter the packets.

79.1 ip source binding

Description

The **ip source binding** command is used to bind the IP address, MAC address, VLAN ID and the Port number together manually. You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN. To delete the IP-MAC-VID-PORT entry from the binding table, please use **no ip source binding index** command.

Syntax

```
ip source binding hostname ip-addr mac-addr vlan vlan-id interface  
{ fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port |  
port-channel port-channel-id } { none | arp-detection | ip-verify-source |  
both }  
no ip source binding index ip-addr
```

Parameter

hostname——The Host Name, which contains 20 characters at most.

ip-addr—— The IP address of the Host.

mac-addr—— The MAC address of the Host.

vlan-id——The VLAN ID needed to be bound, ranging from 1 to 4094.

port—— The number of port connected to the Host.

none | arp-detection | ip-verify-source | both ——The protect type for the entry. "arp-detection" indicates ARP detection; "ip-verify-source" indicates IP source filter; "none" indicates applying none; "both" indicates applying both.

ip-addr—— The IP address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind an ACL entry with the IP 192.168.0.1, MAC 00:00:00:00:00:01, VLAN ID 2 and the Port number 5 manually. And then enable the entry for the ARP detection:

```
Switch(config)#ip source binding host1 192.168.0.1 00:00:00:00:00:01 vlan  
2 interface gigabitEthernet 1/0/5 arp-detection
```

Delete the IP-MAC-VID-PORT entry with the index 5:

```
Switch(config)#no ip source binding index 5
```

79.2 no ip source binding interface

Description

The **ip source binding interface** command is used to delete IMPB entries bound to a specified port in batches.

Syntax

```
no ip source binding interface { fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port }
```

Parameter

port — The number of port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete IMPB entries bound to port 1/0/1:

```
Switch(config)# no ip source binding interface gigabitEthernet 1/0/1
```

79.3 ip dhcp snooping

Description

The **ip dhcp snooping** command is used to enable DHCP Snooping function globally. To disable DHCP Snooping function globally, please use **no ip dhcp snooping** command. DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ip dhcp snooping

no ip dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Snooping function globally:

```
Switch(config)#ip dhcp snooping
```

79.4 ip dhcp snooping vlan

Description

The **ip dhcp snooping vlan** command is used to enable DHCP Snooping function on a specified VLAN. To disable DHCP Snooping function on this VLAN, please use **no ip dhcp snooping vlan** command.

Syntax

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the DHCP snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Snooping function on VLAN 1,4,6-7:

```
Switch(config)#ip dhcp snooping vlan 1,4,6-7
```

79.5 ip dhcp snooping max-entries

Description

The **ip dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCP Snooping. To restore to the default setting, please use **no ip dhcp snooping max-entries** command.

Syntax

ip dhcp snooping max-entries *value*

no ip dhcp snooping max-entries

Syntax

value—— Enter the value of maximum number of entries that can be learned on the port via DHCP Snooping.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of entries that can be learned on port 1 as 100:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#ip dhcp snooping max-entries 100
```

79.6 ip dhcp snooping trust

Description

The **ip dhcp snooping trust** command is used to configure the trust status of a specified interface, and only DHCP Server connected to a trusted port can assign packets to clients. To delete the status, please use **no ip dhcp snooping trust** command.

Syntax

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP Snooping trust function for port 1/0/3:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#ip dhcp snooping trust
```

79.7 ip arp scan vlan

Description

The **ip arp scan vlan** command is used to perform a one-time ARP scan on the specified VLAN and IP address range.

Syntax

```
ip arp scan vlan vlan-id from start-ip to end-ip
```

Syntax

vlan-id—— Specify the VLAN on which to run the ARP scan.

start-ip—— Specify the start IP address of the scan range, in the format A.B.C.D.

end-ip—— Specify the end IP address of the scan range, in the format A.B.C.D.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Run an ARP scan on VLAN 1 for the range 192.168.0.1 to 192.168.0.255:

```
Switch(config)# ip arp scan vlan 1 from 192.168.0.1 to 192.168.0.255
```

79.8 ip arp scan apply

Description

The **ip arp scan apply** command is used to apply an entry from the most recent ARP scan result and add it to the IMPB table. You can choose to add the entry to the ARP Detection table, the IP Verify Source table, both, or neither.

Syntax

```
ip arp scan apply sip hostname { arp-detection | both | ip-verify-source | none }
```

Syntax

sip—— Specify the IP address of the scanned entry.

hostname—— Specify the device hostname. Length: 1 to 20 characters.

arp-detection—— Add the entry to the ARP Detection table.

both—— Add the entry to both the ARP Detection and IP Verify Source tables.

ip-verify-source—— Add the entry to the IP Verify Source table.

none—— Do not add this entry.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the hostname of the entry for 192.168.0.77 to laptop and add it to both tables:

```
Switch(config)# ip arp scan apply 192.168.0.77 laptop both
```

79.9 show ip arp scan

Description

The **show ip arp scan** command is used to display the results of the most recent ARP scan.

Syntax

show ip arp scan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the results of the most recent ARP scan:

```
Switch(config)# show ip arp scan
```

79.10 show ip source binding

Description

The **show ip source binding** command is used to display the IP-MAC-VID-PORT binding table.

Syntax

show ip source binding

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP-MAC-VID-PORT binding table:

```
Switch(config)#show ip source binding
```

79.11 show ip source binding summary

Description

The **show ip source binding summary** command is used to display a summary of the IP-MAC-VID-PORT binding table, including the total number of entries and the number of entries by type.

Syntax

```
show ip source binding summary
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display a summary of the IP-MAC-VID-PORT binding table:

```
Switch(config)# show ip source binding summary
```

79.12 show ip dhcp snooping

Description

The **show ip dhcp snooping** command is used to display the running status of DHCP Snooping.

Syntax

show ip dhcp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of DHCP Snooping:

```
Switch#show ip dhcp snooping
```

79.13 show ip dhcp snooping interface

Description

The **show ip dhcp snooping interface** command is used to display the DHCP Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

show ip dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Snooping configuration of all Ethernet ports and port channels:

```
Switch#show ip dhcp snooping interface
```

Display the DHCP Snooping configuration of Gigabit Ethernet port 1/0/5:

```
Switch#show ip dhcp snooping interface gigabitEthernet 1/0/5
```

Chapter 80 IPv6 IMPB Commands

You can bind the IPv6 address, MAC address, VLAN and the connected Port number of the Host together, which can be the condition for the ARP Inspection and IP verify source to filter the packets.

80.1 ipv6 source binding

Description

The **ipv6 source binding** command is used to bind the IPv6 address, MAC address, VLAN ID and the Port number together manually. You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN. To delete the IPv6-MAC-VID-PORT entry from the binding table, please use **no ipv6 source binding index** command.

Syntax

```
ipv6 source binding hostname ipv6-addr mac-addr vlan vlan-id interface  
{ fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port |  
port-channel port-channel-id } { none | nd-detection | ipv6-verify-source |  
both }  
no ipv6 source binding index ipv6-addr
```

Parameter

hostname——The Host Name, which contains 20 characters at most.

ipv6-addr—— The IP address of the Host.

mac-addr—— The MAC address of the Host.

vlan-id——The VLAN ID needed to be bound, ranging from 1 to 4094.

port—— The number of port connected to the Host.

none | nd-detection | ipv6-verify-source | both ——The protect type for the entry. "nd-detection" indicates ND detection; "ipv6-verify-source" indicates IPv6 source filter; "none" indicates applying none; "both" indicates applying both.

ipv6-addr—— The IPv6 address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

The following example shows how to bind an entry with the hostname host1, IPv6 address 2001:0:9d38:90d5::34, MAC address AA-BB-CC-DD-EE-FF, VLAN ID 10, port number 1/0/5, and enable this entry for ND Detection.

```
Switch(config)# ipv6 source binding host1 2001:0:9d38:90d5::34  
aa:bb:cc:dd:ee:ff vlan 10 interface gigabitEthernet 1/0/5 nd-detection
```

80.2 no ipv6 source binding interface

Description

The **ipv6 source binding interface** command is used to delete IMPB entries bound to a specified port in batches.

Syntax

```
no ipv6 source binding interface { fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port }
```

Parameter

port — The number of port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete IMPB entries bound to port 1/0/1:

```
Switch(config)# no ipv6 source binding interface gigabitEthernet 1/0/1
```

80.3 ipv6 dhcp snooping

Description

The **ipv6 dhcp snooping** command is used to enable DHCPv6 Snooping function globally. To disable DHCPv6 Snooping function globally, please use **no ipv6 dhcp snooping** command. DHCPv6 Snooping functions to monitor the process of the Host obtaining the IP address from DHCPv6 server, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ipv6 dhcp snooping

no ipv6 dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Snooping function globally:

```
Switch(config)#ipv6 dhcp snooping
```

80.4 ipv6 dhcp snooping vlan

Description

The **ipv6 dhcp snooping vlan** command is used to enable DHCP Snooping function on a specified VLAN. To disable DHCP Snooping function on this VLAN, please use **no ipv6 dhcp snooping vlan** command.

Syntax

ipv6 dhcp snooping vlan *vlan-range*

no ipv6 dhcp snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the DHCP snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Snooping function on VLAN 1,4,6-7:

```
Switch(config)#ipv6 dhcp snooping vlan 1,4,6-7
```

80.5 ipv6 dhcp snooping max-entries

Description

The **ipv6 dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCPv6 Snooping. To restore to the default setting, please use **no ipv6 dhcp snooping max-entries** command.

Syntax

ipv6 dhcp snooping max-entries *value*

no ipv6 dhcp snooping max-entries

Syntax

value: Enter the value of maximum number of entries that can be learned on the port via DHCPv6 Snooping.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of entries that can be learned on port 1 as 100:


```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#ipv6 dhcp snooping max-entries 100
```

80.6 ipv6 nd snooping

Description

The **ipv6 nd snooping** command is used to enable ND snooping function globally. To disable ND Snooping function globally, please use **no ipv6 nd snooping** command. ND Snooping functions to monitor the process of the duplication address detection, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ipv6 nd snooping
no ipv6 nd snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ND snooping function globally:

```
T160G-28TS(config)#ipv6 nd snooping
```

80.7 ipv6 nd snooping vlan

Description

The **ipv6 nd snooping vlan** command is used to enable ND snooping function on a specified VLAN. To disable ND Snooping function on this VLAN, please use **no ipv6 nd snooping vlan** command.

Syntax

ipv6 nd snooping vlan *vlan-range*
no ipv6 nd snooping vlan *vlan-range*

Parameter

vlan-range—— Specify the VLANs to enable the ND snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ND snooping function on VLAN 1,4,6-7:

```
Switch(config)#ipv6 nd snooping vlan 1,4,6-7
```

80.8 ipv6 nd snooping max-entries

Description

The **ipv6 nd snooping max-entries** command is used to specify the maximum number of binding entries that are allow to be bound to a port. To return the default, please use **no ipv6 nd snooping max-entries** command.

Syntax

ipv6 nd snooping max-entries *value*

no ipv6 nd snooping max-entries

Parameter

value—— Specify the maximum number of ND snooping entries on this interface.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of binding entries from ND Snooping of Gigabit Ethernet port 1/0/2 is 100:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#ipv6 nd snooping max-entries 100
```

80.9 show ipv6 source binding

Description

The **show ipv6 source binding** command is used to display the IPv6-MAC-VID-PORT binding table.

Syntax

```
show ipv6 source binding
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6-MAC-VID-PORT binding table:

```
Switch(config)#show ipv6 source binding
```

80.10 show ipv6 source binding summary

Description

The **show ipv6 source binding summary** command is used to display a summary of the IPV6-MAC-VID-PORT binding table, including the total number of entries and the number of entries by type.

Syntax

```
show ipv6 source binding summary
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display a summary of the IPV6-MAC-VID-PORT binding table:

```
Switch(config)# show ipv6 source binding summary
```

80.11 show ipv6 dhcp snooping

Description

The **show ipv6 dhcp snooping** command is used to display the running status of DHCPv6 Snooping.

Syntax

```
show ipv6 dhcp snooping
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of DHCPv6 Snooping:

```
Switch#show ipv6 dhcp snooping
```

80.12 show ipv6 dhcp snooping interface

Description

The **show ipv6 dhcp snooping interface** command is used to display the DHCPv6 Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

show ipv6 dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Snooping configuration of all Ethernet ports and port channels:

```
Switch#show ipv6 dhcp snooping interface
```

Display the DHCPv6 Snooping configuration of Gigabit Ethernet port 1/0/5:

```
Switch#show ipv6 dhcp snooping interface gigabitEthernet 1/0/5
```

80.13

show ipv6 nd snooping

Description

The **show ipv6 nd snooping** command is used to display the running status of ND Snooping.

Syntax

show ipv6 nd snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of ND Snooping:

```
Switch#show ipv6 nd snooping
```

80.14 show ipv6 nd snooping interface



Note: This command is only available on certain devices.

Description

The **show ipv6 nd snooping interface** command is used to display the ND Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

```
show ipv6 nd snooping interface [ gigabitEthernet port | port-channel port-channel-id ]
```

Parameters

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ND Snooping configuration of all Ethernet ports and port channels:

```
Switch#show ipv6 nd snooping interface
```

Display the ND Snooping configuration of Gigabit Ethernet port 1/0/5:

```
Switch#show ipv6 nd snooping interface gigabitEthernet 1/0/5
```

Chapter 81 IP Verify Source Commands

IP Verify Source is to filter the IP packets based on the IP-MAC Binding entries. Only the packets matched to the IP-MAC Binding rules can be processed, which can enhance the bandwidth utility.

81.1 ip verify source

Description

The **ip verify source** command is used to configure the IP Verify Source mode for a specified port. To disable the IP Verify Source function, please use **no ip verify source** command.

Syntax

```
ip verify source { sip+mac | sip }  
no ip verify source
```

Parameter

sip+mac —— Security type. "sip+mac" indicates that only the packets with its source IP address, source MAC address and port number matched to the IP-MAC binding rules can be processed.

sip —— Security type. "sip" indicates that only the packets with its source IP address and port number matched to the IP-MAC binding rules can be processed.

Note: sip is only available on certain devices.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IP Verify Source function for Gigabit Ethernet ports 5-10.
Configure that only the packets with its source IP address, source MAC

address and port number matched to the IP-MAC binding rules can be processed:

```
Switch(config)#interface range gigabitEthernet 1/0/5-10  
Switch(config-if-range)#ip verify source sip+mac
```

81.2 ip verify source logging

Description

The **ip verify source logging** command is used to enable the log feature. With this feature enabled, the switch will generate a log when illegal packets are received. To disable the log feature, please use **no ip verify source logging** command.

Syntax

```
ip verify source logging  
no ip verify source logging
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the log feature to make the switch generate logs when receiving illegal packets:

```
Switch(config)#ip verify source logging
```

81.3 show ip verify source

Description

The **show ip verify source** command is used to display the IP Verify Source configuration information.

Syntax

```
show ip verify source
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP Verify Source configuration information:

```
Switch(config)#show ip verify source
```

81.4 show ip verify source interface

Description

The **show ip verify source interface** command is used to display the IP verify source configuration of a desired Gigabit Ethernet port.

Syntax

```
show ip verify source interface [fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port | port-channel port-channel-id]
```

Parameters

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP verify source configuration of Gigabit Ethernet port 1/0/5:

```
Switch#show ip verify source interface gigabitEthernet 1/0/5
```

Chapter 82 IPv6 Verify Source Commands

IPv6 Verify Source is to filter the IPv6 packets based on the IPv6-MAC Binding entries. Only the packets matched to the IPv6-MAC Binding rules can be processed, which can enhance the bandwidth utility.

82.1 ipv6 verify source

Description

The **ipv6 verify source** command is used to configure the IPv6 Verify Source mode for a specified port. To disable the IPv6 Verify Source function, please use **no ipv6 verify source** command.

Syntax

ipv6 verify source { sipv6+mac | sipv6 }

no ipv6 verify source

Parameter

sipv6+mac —— Security type. "sipv6+mac" indicates that only the packets with its source IPv6 address, source MAC address and port number matched to the IPv6-MAC binding rules can be processed.

sipv6 —— Security type. "sipv6" indicates that only the packets with its source IPv6 address and port number matched to the IPv6-MAC binding rules can be processed.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IPv6 Verify Source function for Gigabit Ethernet ports 5-10.
Configure that only the packets with its source IPv6 address, source MAC address and port number matched to the IPv6-MAC binding rules can be processed:

```
Switch(config)#interface range gigabitEthernet 1/0/5-10
Switch(config-if-range)#ipv6 verify source sipv6+mac
```

82.2 show ipv6 verify source

Description

The **show ipv6 verify source** command is used to display the IPv6 Verify Source configuration information.

Syntax

```
show ipv6 verify source
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 Verify Source configuration information:

```
Switch(config)#show ipv6 verify source
```

82.3 show ipv6 verify source interface

Description

The **show ipv6 verify source interface** command is used to display the IPv6 verify source configuration of a desired Gigabit Ethernet port.

Syntax

```
show ipv6 verify source interface gigabitEthernet port
```

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 verify source configuration of Gigabit Ethernet port 1/0/5:

```
Switch#show ipv6 verify source interface gigabitEthernet 1/0/5
```

Chapter 83 DHCPv4 Filter Commands

DHCPv4 Filter function allows the user to not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

83.1 ip dhcp filter

Description

The **ip dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCP Filter function globally, please use **no ip dhcp filter** command.

Syntax

ip dhcp filter
no ip dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Filter function globally:

```
Switch(config)#ip dhcp filter
```

83.2 ip dhcp filter vlan

Description

The **ip dhcp filter vlan** command is used to enable the DHCP Filter function on the specified VLANs. By default, the DHCP Filter function is enabled on all VLANs. After this command is configured, the DHCP Filter function is enabled only on the specified VLANs and is disabled on all other VLANs. To disable

the DHCP Filter function on specified VLANs, use the **no ip dhcp filter vlan** command.

Syntax

ip dhcp filter vlan *vlan-range*
no ip dhcp filter vlan *vlan-range*

Parameter

vlan-range——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Filter function only on VLANs 1, 3, 5, and 7 through 10:

```
Switch(config)#ip dhcp filter vlan 1,3,5,7-10
```

83.3 ip dhcp filter (interface)

Description

The **ip dhcp filter (interface)** command is used to enable DHCP Filter function on a specified port. To disable DHCP Filter function on this port, please use **no ip dhcp filter (interface)** command.

Syntax

ip dhcp filter
no ip dhcp filter

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Filter on port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(Config-if)#ip dhcp filter
```

83.4 ip dhcp filter mac-verify

Description

The **ip dhcp filter mac-verify** command is used to enable the MAC Verify feature. To disable the MAC Verify feature, please use **no ip dhcp filter mac-verify** command. There are two fields of the DHCP packet containing the MAC address of the Host. The MAC Verify feature is to compare the two fields and discard the packet if the two fields are different.

Syntax

```
ip dhcp filter mac-verify
no ip dhcp filter mac-verify
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MAC Verify feature for the Gigabit Ethernet port 10/2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#ip dhcp filter mac-verify
```

83.5 ip dhcp filter limit rate

Description

The **ip dhcp filter limit rate** command is used to enable the Flow Control feature for the DHCP packets. The excessive DHCP packets will be discarded.

To restore to the default configuration, please use **no ip dhcp filter limit rate** command.

Syntax

ip dhcp filter limit rate *value*
no ip dhcp filter limit rate

Parameter

value—— The value of Flow Control. The options are 5/10/15/20/25/30 (packet/second). The default value is 0, which stands for "disable".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the Flow Control of GigabitEthernet port 2 as 20 pps:

```
Switch(config)#interface gigabitEthernet 1/0/2  
Switch(config-if)#ip dhcp filter limit rate 20
```

83.6 ip dhcp filter decline rate

Description

The **ip dhcp filter decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decline packets. The excessive DHCP Decline packets will be discarded. To disable the Decline Protect feature, please use **no ip dhcp filter decline rate** command.

Syntax

ip dhcp filter decline rate *value*
no ip dhcp filter decline rate

Parameter

value—— Specify the rate limit of DHCP Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). Its default value is 0, which stands for "disable".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the rate limit of DHCP Decline packets as 20 packets per second on Gigabit Ethernet port 1/0/2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#ip dhcp filter decline rate 20
```

83.7 ip dhcp filter server permit-entry

Description

The **ip dhcp filter server permit-entry** command is used to add entry for the legal DHCP server. To restore to the default option, please use **no ip dhcp snooping information strategy** command.

Syntax

```
ip dhcp filter server permit-entry server-ip ipAddr client-mac macAddr  
interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | interface port-channel port-channel-id }  
no ip dhcp filter server permit-entry server-ip ipAddr client-mac macAddr  
interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | interface port-channel port-channel-id }
```

Parameter

ipAddr—— Specify the IP address of the legal DHCPv4 server.

macAddr—— Specify the MAC address of the DHCP Client. The value “all” means all client mac addresses.

port-list / port-channel-id—— Specify the port that the legal DHCPv4 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an entry for the legal DHCPv4 server whose IP address is 192.168.0.100 and connected port number is 1/0/1 without client MAC address restricted:

```
Switch(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100
client-mac all interface gigabitEthernet 1/0/1
```

83.8 show ip dhcp filter

Description

The **show ip dhcp filter** command is used to display the configuration of DHCP Filter.

Syntax

show ip dhcp filter

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration:

```
Switch#show ip dhcp filter
```

83.9 show ip dhcp filter interface

Description

The **show ip dhcp filter interface** command is used to display the configuration of DHCP Filter on ports.

Syntax

show ip dhcp filter interface [**fastEthernet** *port*] **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration on port 1/0/3:

```
Switch#show ip dhcp filter interface gigabitEthernet 1/0/3
```

83.10 show ip dhcp filter server permit-entry

Description

The **show ip dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

show ip dhcp filter server permit-entry

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCP server configuration:

```
Switch#show ip dhcp filter server permit-entry
```

Chapter 84 DHCPv6 Filter Commands

DHCPv6 Filter function allows the user to not only to restrict all DHCPv6 Server packets but also to receive any specified DHCPv6 server packet by any specified DHCPv6 client, it is useful when one or more DHCPv6 servers are present on the network and both provide DHCPv6 services to different distinct groups of clients.

84.1 ipv6 dhcp filter

Description

The **ipv6 dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCPv6 Filter function globally, please use **no ipv6 dhcp filter** command.

Syntax

ipv6 dhcp filter
no ipv6 dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Filter function globally:

```
Switch(config)#ipv6 dhcp filter
```

84.2 ipv6 dhcp filter (interface)

Description

The **ipv6 dhcp filter (interface)** command is used to enable DHCPv6 Filter function on a specified port. To disable DHCPv6v Filter function on this port, please use **no ipv6 dhcp filter (interface)** command.

Syntax

ipv6 dhcp filter

no ipv6 dhcp filter

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Filter on port 1/0/1

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(Config-if)#ipv6 dhcp filter
```

84.3 ipv6 dhcp filter limit rate

Description

The **ipv6 dhcp filter limit rate** command is used to enable the Flow Control feature for the DHCPv6 packets. The excessive DHCPv6 packets will be discarded. To restore to the default configuration, please use **no ipv6 dhcp filter limit rate** command.

Syntax

ipv6 dhcp filter limit rate *value*

no ipv6 dhcp filter limit rate

Parameter

value—— The value of Flow Control. The options are 5/10/15/20/25/30 (packet/second). The default value is 0, which stands for "disable".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the Flow Control of GigabitEthernet port 2 as 20 pps:

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#ipv6 dhcp filter limit rate 20
```

84.4 ipv6 dhcp filter decline rate

Description

The **ipv6 dhcp filter decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decline packets. The excessive DHCPv6 Decline packets will be discarded. To disable the Decline Protect feature, please use **no ipv6 dhcp filter decline rate** command.

Syntax

ipv6 dhcp filter decline rate *value*

no ipv6 dhcp filter decline rate

Parameter

value—— Specify the rate limit of DHCPv6 Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). Its default value is 0, which stands for "disable".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the rate limit of DHCPv6 Decline packets as 20 packets per second on Gigabit Ethernet port 1/0/2:

```
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#ipv6 dhcp filter decline 20
```

84.5 ipv6 dhcp filter server permit-entry

Description

The **ipv6 dhcp filter server permit-entry** command is used to add entry for the legal DHCPv6 server. To restore to the default option, please use **no ipv6 dhcp snooping information strategy** command.

Syntax

```
ipv6 dhcp filter server permit-entry server-ip ipAddr interface
{ fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port |
interface port-channel port-channel-id }

no ipv6 dhcp filter server permit-entry server-ip ipAddr interface
{ fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port |
interface port-channel port-channel-id }
```

Parameter

ipAddr—— Specify the IPv6 address of the legal DHCPv6 server.

port-list / port-channel-id—— Specify the port that the legal DHCPv6 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an entry for the legal DHCPv6 server whose IP address is 192.168.0.100 and connected port number is 1/0/1:

```
Switch(config)#ipv6 dhcp filter server permit-entry server-ip 2003::1  
interface gigabitEthernet 1/0/1
```

84.6 show ipv6 dhcp filter

Description

The **show ipv6 dhcp filter** command is used to display the configuration of DHCPv6 Filter.

Syntax

```
show ipv6 dhcp filter
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration:

```
Switch#show ipv6 dhcp filter
```

84.7 show ipv6 dhcp filter interface

Description

The **show ipv6 dhcp filter interface** command is used to display the configuration of DHCPv6 Filter on ports.

Syntax

```
show ipv6 dhcp filter interface [fastEthernet port | gigabitEthernet port |  
ten-gigabitEthernet port | port-channel port-channel-id]
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration on port 1/0/3:

```
Switch#show ipv6 dhcp filter interface gigabitEthernet 1/0/3
```

84.8 show ipv6 dhcp filter server permit-entry

Description

The **show ipv6 dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

```
show ipv6 dhcp filter server permit-entry
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCPv6 server configuration:

```
Switch#show ipv6 dhcp filter server permit-entry
```

Chapter 85 Dying Gasp Commands

Dying Gasp is a communication technology term, primarily used in broadband communications (e.g., DSL - Digital Subscriber Line). When a communication device (such as a DSL modem) experiences a power failure or malfunction, a Dying Gasp signal is sent to notify the service provider about the issue.

Devices located at the network edge often have relatively poor power supply conditions, making them susceptible to unexpected power loss. Dying Gasp provides a mechanism for issuing an unexpected power failure alert to monitoring systems before the device loses connection. When a power failure event occurs, a hardware capacitor briefly delays the device shutdown. During this period, the device will send a Dying Gasp message to the configured syslog server or SNMP trap recipient. This information can be used to determine the cause of the problem and aid in troubleshooting.

The purpose of the Dying Gasp signal is to allow network operators and service providers to quickly identify issues, thereby enabling more efficient fault handling and improving user satisfaction. This signal helps avoid prolonged fault detection and localization processes, accelerating service recovery.

85.1 dying-gasp enable oam

Description

The **dying-gasp enable oam** command is used to enable the OAM packet notification for dying-gasp. To disable this function, please use **no dying-gasp enable oam** command.

Syntax

dying-gasp enable oam [**vlan** *vid*]

no dying-gasp enable oam

Parameter

vid—— VLAN ID, ranging from 1 to 4094. The default is 1.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable OAM packet notification for VLAN 1:

```
Switch(config)# dying-gasp enable oam vlan 1
```

85.2 dying-gasp enable syslog

Description

The **dying-gasp enable syslog** command is used to enable the syslog packet notification for dying-gasp. To disable this function, please use **no dying-gasp enable syslog** command. The destination server is the server configured with index=1 in the log host configuration.

Syntax

dying-gasp enable syslog
no dying-gasp enable syslog

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the syslog packet notification for dying-gasp:

```
Switch(config)# dying-gasp enable syslog
```

85.3 dying-gasp enable snmp

Description

The **dying-gasp enable snmp** command is used to enable the SNMP trap notification for dying-gasp. To disable this function, please use **no dying-gasp enable snmp** command. The destination server is the server configured with index=1 in the SNMP server configuration.

Syntax

dying-gasp enable snmp
no dying-gasp enable snmp

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the SNMP trap notification for dying-gasp:

```
Switch(config)# dying-gasp enable snmp
```

85.4 show dying-gasp status

Description

The **show dying-gasp status** command is used to view the status of the dying-gasp function.

Syntax

show dying-gasp status

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Check if the dying-gasp function is enabled:

```
Switch(config)# show dying-gasp status
```

85.5 show dying-gasp packets

Description

The **show dying-gasp packets** command is used to view the packet information for dying-gasp.

Syntax

show dying-gasp packets

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View dying-gasp packet information:

```
Switch(config)# show dying-gasp packets
```

Chapter 86 DoS Defend Commands

DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host. With the DoS Defend enabled, the switch can analyze the specific field of the received packets and provide the defend measures to ensure the normal working of the local network.

86.1 ip dos-prevent

Description

The **ip dos-prevent** command is used to enable the DoS defend function globally. To disable the DoS defend function, please use **no ip dos-prevent** command.

Syntax

ip dos-prevent

no ip dos-prevent

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DoS defend function globally:

```
Switch(config)#ip dos-prevent
```

86.2 ip dos-prevent type

Description

The **ip dos-prevent type** command is used to select the DoS Defend Type. To disable the corresponding Defend Type, please use **no ip dos-prevent type** command.

Syntax

ip dos-prevent type { land | scan-synfin | xma-scan | null-scan |
port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death |
smurf }

no ip dos-prevent type { land | scan-synfin | xma-scan | null-scan |
port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death |
smurf }

Parameter

land —The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both of the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection.

scan-synfin —The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal.

xma-scan —The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.

null-scan —The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.

port-less-1024 —The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024.

blat —The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker.

ping-flood —The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for the system to respond to legal communication.

syn-flood —The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.

win-nuke —Because the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this

type of packets to the TCP port 139 (NetBIOS) of the host with the Operation System bugs, which will cause the host with a blue screen.

ping-of-death — Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer.

Note: ping-of-death is only available on certain devices.

smurf — Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

Note: smurf is only available on certain devices.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DoS Defend Type named Land attack:

```
Switch(config)#ip dos-prevent type land
```

86.3 show ip dos-prevent

Description

The **show ip dos-prevent** command is used to display the DoS information of the detected DoS attack, including enable/disable status, the DoS Defend Type, the count of the attack, etc.

Syntax

show ip dos-prevent

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DoS information of the detected DoS attack globally:

```
Switch(config)#show ip dos-prevent
```

Chapter 87 sFlow Commands (Only for Certain Devices)



Note: sFlow commands are only available on certain devices.

sFlow (Sampled Flow) is a technology for accurately monitoring network traffic at high speeds. The sFlow monitoring system consists of a sFlow agent (embedded in a switch or router or in a standalone probe) and a central sFlow collector. The sFlow agent is a virtual entity using sampling technology to capture traffic statistics from the device it is monitoring. The sFlow collector can be a host receiving sFlow datagrams from the sFlow agent.

The sFlow feature is implemented as follows: the sFlow sampler take samples of traffic statistics and send sFlow datagrams to the sFlow agent for processing. The sFlow agent will forward sFlow datagrams to the sFlow collector for analysis. The analytic results can be displayed on the sFlow collector.

87.1 sflow address

Description

The **sflow address** command is used to configure the sFlow agent's IP address. To delete the configured address, please use **no sflow address** command.

Syntax

sflow address { *ipv4-addr* }

no sflow address { *ipv4-addr* }

Parameter

ipv4-addr —The IP address of the sFlow agent. The type of the IP address should be IPv4. For example, you can set the switch's management IP as the IP address of the sFlow agent.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the sFlow agent with the IP address as 192.168.0.1:

```
Switch(config)#sflow address 192.168.0.1
```

87.2 sflow enable

Description

The **sflow enable** command is used to enable sFlow function. To disable the sFlow function, please use **no sflow enable** command.

Syntax

sflow enable

no sflow enable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

User Guidelines

A valid agent address should be assigned to the sFlow agent embedded in the switch before you enable the sFlow function.

Example

Enable sFlow function globally:

```
Switch(config)#sflow enable
```

87.3 sflow collector collector-ID

Description

The **sflow collector collector-ID** command is used to configure the parameters about the sFlow collector.

Syntax

sflow collector collector-ID *value* { [**descript** *descript*] | [**ip** *ip*] | [**port** *port*] | [**maxData** *maxData*] | [**timeout** *timeout*] }

Parameter

value—— The ID of the sFlow collector you desire to configure. The value ranges from 1 to 4.

descript——Give a Description to the sFlow collector, which contains 16 characters at most.

ip——The IP address of the sFlow collector. The type of the IP address should be IPv4, for example 192.168.0.100.

port——The number of the udp port which is selected for the sFlow collector.

maxData——Specify the maximum number of data bytes that can be sent in a single sample datagram. The value ranges from 300 to 1400 and the default value is 300 bytes.

timeout——Specify the aging time of the sFlow collector, ranging from 0 to 2000000 seconds. When the timeout is set to 0, it means the life cycle of the collector is infinite.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the ip of the sFlow collector 1 as 192.168.0.100, the port as 3000:

```
Switch(config)# sflow collector collector-ID 1 ip 192.168.0.100
```

```
Switch(config)# sflow collector collector-ID 1 port 3000
```

87.4 sflow sampler

Description

The **sflow sampler** command is used to configure the parameters about the sFlow sampler.

Syntax

```
sflow sampler {[ collector-ID value] | [ingRate ingress-rate] [egRate egress-rate] | [maxHeader maxHeader] }
```

Parameter

value—— The ID of the sFlow collector which the sFlow sampler will send sFlow datagrams to. The value ranges from 0 to 4. When the value is zero, it means no collector is selected.

ingress-rate——Specify the ingress sampling frequency of the sFlow sampler. When a sample is taken, the value indicates how many packets to skip before the next sample is taken. The value ranges from 1024 to 65535 and the default value is 0 which means no packets will be sampled.

egress-rate——Specify the egress sampling frequency of the sFlow sampler. When a sample is taken, the value indicates how many packets to skip before

the next sample is taken. The value ranges from 1024 to 65535 and the default value is 0 which means no packets will be sampled.

maxHeader——Specify the maximum number of bytes that should be copied from a sampled packet. The value ranges from 18 to 256 and the default value is 128 bytes.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure Gigabit Ethernet port 1 as the sFlow sampler: specify the Collector-ID as 1, the ingress rate as 1024:

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#sflow sampler collector-ID 1
```

For L2/L2+ switches:

```
Switch(config-if)#sflow sampler ingRate 1024
```

For L3 switches:

```
Switch(config)#sflow sampler ingRate 1024
```

87.5 show sflow global

Description

The **show sflow global** command is used to display the global configuration of sFlow.

Syntax

```
show sflow global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of sFlow:

```
Switch#show sflow global
```

87.6 show sflow collector

Description

The **show sflow collector** command is used to display the global configuration of the sFlow collector.

Syntax

```
show sflow collector
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of the sFlow collector:

```
Switch#show sflow collector
```

87.7 show sflow sampler

Description

The **show sflow sampler** command is used to display the global configuration of the sFlow sampler.

Syntax

```
show sflow sampler
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of the sFlow sampler:

```
Switch#show sflow sampler
```


Chapter 88 Ethernet OAM Commands (Only for Certain Devices)



Note: Ethernet OAM commands are only available on certain devices.

Ethernet OAM (standing for Operation, Administration, and Maintenance) is Layer 2 protocol that is used for monitoring and troubleshooting Ethernet networks. It can report the network status to network administrators through the OAMPDUs exchanged between two OAM entities. The operation of OAM on an Ethernet interface does not adversely affect data traffic as OAM is a slow protocol with very limited bandwidth potential.

88.1 ethernet-oam

Description

The **ethernet-oam** command is used to enable the Ethernet OAM function for the desired port. To disable the Ethernet OAM function, please use **no ethernet-oam** command.

Syntax

ethernet-oam

no ethernet-oam

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the Ethernet OAM function for Gigabit Ethernet port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#ethernet-oam
```

88.2 ethernet-oam mode

Description

The **ethernet-oam mode** command is used to configure the OAM mode for the desired port. To return to the default configurations, please use **no ethernet-oam mode** command. The default mode is active.

Syntax

```
ethernet-oam mode { passive | active }  
no ethernet-oam mode
```

Parameter

passive —— Specify the OAM mode as passive.
active —— Specify the OAM mode as active.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure Ethernet OAM client to operate in passive mode for Gigabit Ethernet port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2  
Switch(config-if)#ethernet-oam mode passive
```

88.3 ethernet-oam link-monitor symbol-period

Description

The **ethernet-oam link-monitor symbol-period** command is used to configure the parameters about one of the link events, error symbol period event. To return to the default configurations, please use **no ethernet-oam link-monitor symbol-period** command.

Syntax

ethernet-oam link-monitor symbol-period { **threshold** *threshold* | **window** *window* | **notify** { disable | enable } }

no ethernet-oam link-monitor symbol-period { threshold | window | notify }

Parameter

threshold—— Configure the error threshold for generating error symbol-period event. The range is from 1 to 4294967295 and the default value is 1.

window—— Configure the error symbol-period event detection interval. The range is from 10 to 600, in terms of 100 ms intervals. The default value is 10.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error symbol-period event, configure the error threshold as 5 and the event detection interval as 3 seconds on Gigabit Ethernet port 1/0/2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# ethernet-oam link-monitor symbol-period threshold 5
window 30
```

88.4 ethernet-oam link-monitor frame

Description

The **ethernet-oam link-monitor frame** command is used to configure the parameters about one of the link events, error frame event. To return to the

default configurations, please use **no ethernet-oam link-monitor frame** command.

Syntax

ethernet-oam link-monitor frame { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame { threshold | window | notify }

Parameter

threshold — Configure the error threshold for generating error frame event. The range is from 1 to 4294967295 and the default value is 1.

window — Configure the error symbol-period event detection interval. The range is from 10 to 600, in terms of 100 ms intervals. The default value is 10.

notify — Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify — The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error frame event, configure the error threshold as 6 and the event detection interval as 9 seconds on Gigabit Ethernet port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# ethernet-oam link-monitor frame threshold 6 window
90
```

88.5 ethernet-oam link-monitor frame-period

Description

The **ethernet-oam link-monitor frame-period** command is used to configure the parameters about one of the link events, error frame period

event. To return to the default configurations, please use **no ethernet-oam link-monitor frame-period** command.

Syntax

ethernet-oam link-monitor frame-period { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame-period { threshold | window | notify }

Parameter

threshold—— Configure the error threshold for generating error frame period event. The range is from 1 to 89285999 and the default value is 1.

window—— Configure the error frame period event detection interval. The range is from 148810 to 89286000. The default value is 148810 for Fast Ethernet port and 1488100 for Gigabit Ethernet port.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error frame period event, configure the error threshold as 6 and the event detection interval as 150000 frames on Gigabit Ethernet port 1/0/4:

```
Switch(config)# interface gigabitEthernet 1/0/4
```

```
Switch(config-if)# ethernet-oam link-monitor frame-period threshold 6
```

```
window 150000
```

88.6 ethernet-oam link-monitor frame-seconds

Description

The **ethernet-oam link-monitor frame-seconds** command is used to configure the parameters about one of the link events, error frame seconds event. To return to the default configurations, please use **no ethernet-oam link-monitor frame-seconds** command.

Syntax

```
ethernet-oam link-monitor frame-seconds { [threshold threshold]  
[ window window] [notify { disable | enable } ] }  
no ethernet-oam link-monitor frame-seconds { threshold | window | notify }
```

Parameter

threshold—— Configure the error threshold for generating error frame seconds event. The range is from 1 to 899 and the default value is 1.

window—— Configure the error frame seconds event detection interval. The range is from 100 to 9000, in terms of 100 ms intervals. The default value is 600.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error frame seconds event, configure the error threshold as 8 and the event detection interval as 30 seconds on Gigabit Ethernet port 5:

```
Switch(config)# interface gigabitEthernet 1/0/5  
Switch(config-if)# ethernet-oam link-monitor frame-seconds threshold 8  
window 300
```

88.7 ethernet-oam remote-failure

Description

The ethernet-oam remote-failure command is used to configure whether to notify the link faults or not. The link faults include dying gasp and critical event. To return to the default configurations, please use **no ethernet-oam remote-failure** command.

Syntax

ethernet-oam remote-failure { dying-gasp | critical-event } **notify** { disable | enable }

no ethernet-oam remote-failure { dying-gasp | critical-event } **notify**

Parameter

dying-gasp — Dying Gasp link event. Dying gasp means an unrecoverable fault, such as power failure, occurs.

critical-event — Critical Event. Critical-event means unspecified critical event occurs.

notify — Enable/Disable the event notification. By default, it is enabled.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Disable the Dying Gasp link event notification on Gigabit Ethernet port 1/0/7:

```
Switch(config)# interface gigabitEthernet 1/0/7
```

```
Switch(config-if)# ethernet-oam remote-failure dying-gasp notify disable
```

88.8 ethernet-oam

remote-loopback

received-remote- loopback

Description

The **ethernet-oam remote-loopback received-remote-loopback** command is used to configure the client to process or to ignore the received remote loopback request. To return to the default configurations, please use **no ethernet-oam remote-loopback received-remote-loopback** command.

Syntax

```
ethernet-oam remote-loopback received-remote-loopback { process |  
ignore }  
  
no ethernet-oam remote-loopback received-remote-loopback
```

Parameter

process — Process the received remote loopback request.
ignore — Ignore the received remote loopback request.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the client to process the received remote loopback request on Gigabit Ethernet port 1:

```
Switch(config)# interface gigabitEthernet 1/0/1  
  
Switch(config-if)# ethernet-oam remote-loopback received  
-remote-loopback process
```


88.9 ethernet-oam remote-loopback

Description

The **ethernet-oam remote-loopback** command is used to request the remote peer to start or stop the Ethernet OAM remote loopback mode.

Syntax

ethernet-oam remote-loopback { start | stop }

Parameter

start — Request the remote peer to start the Ethernet OAM remote loopback mode.

stop — Request the remote peer to stop the Ethernet OAM remote loopback mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Request the remote peer to start the Ethernet OAM remote loopback mode on Gigabit Ethernet port 1/0/3:

```
Switch(config)# interface gigabitEthernet 1/0/3
```

```
Switch(config-if)# ethernet-oam remote-loopback start
```

88.10 clear ethernet-oam statistics

Description

The **clear ethernet-oam statistics** command is used to clear Ethernet OAM statistics.

Syntax

```
clear ethernet-oam statistics [ interface [ fastEthernet port]  
[ gigabitEthernet port] [ ten-gigabitEthernet port] [ two-gigabitEthernet  
port]]
```

Parameter

port—— The Gigabit Ethernet port number. By default, the Ethernet OAM statistics of all ports are cleared.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Clear Ethernet OAM statistics of Gigabit Ethernet port 1/0/3:

```
Switch(config)# clear ethernet-oam statistics interface gigabit Ethernet  
1/0/3
```

88.11 clear ethernet-oam event-log

Description

The **clear ethernet-oam event-log** command is used to clear the Ethernet OAM event log.

Syntax

```
clear ethernet-oam event-log [ interface gigabitEthernet port]
```

Parameter

port——The Gigabit Ethernet port number. By default, the Ethernet OAM event logs of all ports are cleared.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Clear Ethernet OAM event log of Gigabit Ethernet port 1/0/3:

```
Switch(config)# clear ethernet-oam event-log interface gigabitEthernet  
1/0/3
```

88.12 show ethernet-oam configuration

Description

The **show ethernet-oam configuration** command is used to display Ethernet OAM configuration information.

Syntax

show ethernet-oam configuration [**interface gigabitEthernet** *port*]

Parameter

port — The Gigabit Ethernet port number. By default, the Ethernet OAM configuration information of all ports is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM configuration information of Gigabit Ethernet port 1/0/2:

```
Switch(config)# show ethernet-oam configuration interface  
gigabitEthernet 1/0/2
```

88.13 show ethernet-oam event-log

Description

The **show ethernet-oam event-log** command is used to display the Ethernet OAM event log.

Syntax

show ethernet-oam event-log [**interface gigabitEthernet** *port*]

Parameter

port — The Gigabit Ethernet port number. By default, the Ethernet OAM event logs of all ports are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM event log of Gigabit Ethernet port 1/0/2:

```
Switch(config)# show ethernet-oam event-log interface gigabitEthernet  
1/0/2
```

88.14 show ethernet-oam statistics

Description

The **show ethernet-oam statistics** command is used to display the Ethernet OAM statistics.

Syntax

show ethernet-oam statistics [**interface gigabitEthernet** *port*]

Parameter

port—— The Gigabit Ethernet port number. By default, the Ethernet OAM statistics of all ports are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM statistics of Gigabit Ethernet port 1/0/2:

```
Switch(config)# show ethernet-oam statistics interface gigabitEthernet  
1/0/2
```

88.15 show ethernet-oam status

Description

The **show ethernet-oam status** command is used to display the Ethernet OAM status of both the local and the remote client.

Syntax

show ethernet-oam status [interface gigabitEthernet *port*]

Parameter

port—— The Gigabit Ethernet port number. By default, the Ethernet OAM status of all ports is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM status of Gigabit Ethernet port 1/0/2:

```
Switch(config)# show ethernet-oam status interface gigabitEthernet 1/0/2
```

Chapter 89 MPLS Commands (Only for Certain Devices)

Multiprotocol Label Switching (MPLS) was initially developed to improve router forwarding speed. Compared to traditional IP routing, it analyzes IP packet headers only at the network edge during data forwarding, saving processing time by avoiding analysis at every hop.

With the development of ASIC technology, route lookup speed is no longer a bottleneck for network development, rendering MPLS less of a significant advantage in improving forwarding speed. However, MPLS's support for multi-layer labeling and connection-oriented forwarding plane makes it widely used in Virtual Private Networks (VPNs), traffic engineering, and Quality of Service (QoS).

89.1 mpls (global)

Description

The **mpls** command enables the MPLS function globally. The **no** command deletes MPLS configuration information and disables MPLS globally.

Global MPLS status controls whether the switch's global MPLS forwarding function is active.

Syntax

mpls

no mpls

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the MPLS function globally:

```
Switch(config)# mpls
```

89.2 mpls ttl-mode

Description

The **mpls ttl-mode** command changes the TTL mode used by the switch for MPLS forwarding.

The MPLS label contains an 8-bit TTL field, with the same meaning as the TTL field in the IP header. MPLS TTL processing is used not only to prevent routing loops but also to implement traceroute functionality.

MPLS TTL processing includes two modes: Uniform and Pipe.

Uniform: When an IP packet passes through an MPLS network, at the ingress node, the IP TTL is decremented by 1 and mapped to the MPLS TTL field. The packet is then processed according to standard TTL handling within the MPLS network. At the egress node, the MPLS TTL is decremented by 1 and mapped back to the IP TTL field.

Pipe: At the ingress node, the IP TTL value is decremented by 1, while the MPLS TTL field remains a fixed value. The packet is then processed according to standard TTL handling within the MPLS network. At the egress node, the IP TTL field value is decremented by 1. In other words, when an IP packet passes through an MPLS network, regardless of the number of hops, the IP TTL is decremented by 1 only at both the ingress and egress nodes.

By default, MPLS uses the Pipe mode for TTL processing.

Syntax

mpls ttl-mode { *pipe* / *uniform* }

Parameter

pipe — Set the MPLS TTL mode to pipe.

uniform — Set the MPLS TTL mode to uniform.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the MPLS TTL mode to uniform:

```
Switch(config)# mpls ttl-mode uniform
```

89.3 mpls ingress-lsp binding ipv4

Description

The **mpls ingress-lsp binding ipv4** command configures the ingress node for a static MPLS LSP tunnel. After packets pass through the tunnel ingress node, they will be tagged with the configured static MPLS label, which is used for subsequent forwarding by transit or egress nodes. The **no** command deletes the configuration information and cancels MPLS forwarding on the ingress node. You can specify a destination IPv4 address to delete ingress node configurations in batches.

Syntax

```
mpls ingress-lsp binding ipv4 ip-address ip-mask out-label out-label  
nexthop nexthop-address  
  
no mpls ingress-lsp binding ipv4 ip-address ip-mask [out-label out-label]  
[nexthop nexthop-address]
```

Parameter

ip-address — The IP address of the static LSP. Values are in dotted decimal notation.

ip-mask — The subnet mask of the static LSP.

out-label — The out label value. Values are integers, ranging from {<16-1048575> | 0 | 3}.

nexthop-address — The next-hop address. Values are in dotted decimal notation.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the switch as an LSP ingress node, with LSP destination address 1.1.1.1, next hop 2.2.2.2, and outgoing label 50:

```
Switch(config)# mpls ingress-lsp binding ipv4 1.1.1.1 255.255.255.0  
out-label 50 nexthop 2.2.2.2
```


89.4 mpls transmit-lsp binding ipv4

Description

The **mpls transmit-lsp binding ipv4** command configures the transit node for a static MPLS LSP tunnel. After a packet passes through the tunnel transit node, its MPLS static label is replaced or stripped for subsequent transit/egress nodes or IP forwarding. The **no** command deletes the configuration information and cancels MPLS forwarding on the transit node. You can specify a destination IPv4 address to delete transit node configurations in batches.

Syntax

```
mpls transmit-lsp binding ipv4 ip-address ip-mask in-label in-label  
opcode { swap out-label | pop } nexthop nexthop-address  
no mpls transmit-lsp binding ipv4 ip-address ip-mask [ in-label in-label ]  
opcode { swap out-label | pop } nexthop nexthop-address ]]
```

Parameter

ip-address — The IP address of the static LSP. Values are in dotted decimal notation.

ip-mask — The subnet mask of the static LSP.

in-label — The in label value. Values are integers, ranging from <16 to 1024>.

swap — The transit node replaces the label.

pop — The transit node removes the label.

out-label — The out label value. Values are integers, ranging from { <16 to 1048575> | 0 }.

nexthop-address — The next-hop address. Values are in dotted decimal notation.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the switch as an LSP transit node with destination address 1.1.1.1, next hop 3.3.3.4, inbound label 50, and outbound label 60:

```
Switch(config)# mpls transit-lsp binding ipv4 1.1.1.1 255.255.255.255  
in-label 50 opcode swap 60 nexthop 3.3.3.4
```

89.5 mpls egress-lsp binding

Description

The **mpls egress-lsp binding** command configures the egress node for a static MPLS LSP tunnel. After a packet passes through the tunnel egress node, its MPLS static label is removed, and subsequent IP forwarding is performed. The **no** command deletes the configuration information and cancels MPLS forwarding on the egress node. You can specify a destination IPv4 address to delete egress node configurations in batches.

Syntax

mpls egress-lsp binding *ipv4 ip-address ip-mask in-label in-label*
no mpls egress-lsp binding *ipv4 ip-address ip-mask in-label in-label*

Parameter

ip-address — The IP address of the static LSP. Values are in dotted decimal notation.
ip-mask — The subnet mask of the static LSP.
in-label — The in label value. Values are integers, ranging from <16 to 1024>.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the switch as an LSP egress node, with LSP destination address 1.1.1.1 and inbound label 80:

```
Switch(config)# mpls egress-lsp binding ipv4 1.1.1.1 255.255.255.0  
in-label 80
```

89.6 mpls (interface)

Description

The **mpls** command enables the MPLS function on an interface. The **no** command deletes MPLS configuration information and disables MPLS on the interface.

Interface MPLS status controls whether the current interface can participate in MPLS forwarding.

Syntax

mpls
no mpls

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable MPLS on the interface:

```
Switch(config-if)# mpls
```

89.7 show mpls

Description

The **show mpls** command is used to display the device's global MPLS status information and interface MPLS status information.

Syntax

show mpls

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the MPLS status information on the switch:

```
Switch(config-if)# show mpls
```

89.8 show mpls ftn

Description

The **show mpls ftn** command is used to display FTN entry information, including forwarding and status information.

Syntax

```
show mpls ftn
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the FTN entry information on the switch:

```
Switch(config-if)# show mpls ftn
```

89.9 show mpls ilm

Description

The **show mpls ilm** command is used to display ILM entry information, including forwarding and status information.

Syntax

show mpls ilm

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the ILM entry information on the switch:

```
Switch(config-if)# show mpls ilm
```

89.10 show mpls static-lsp

Description

The **show mpls static-lsp** command displays the configuration information of a static LSP.

Syntax

show mpls static-lsp [*ip-address* / *masklen*]

Parameter

ip-address — The destination IPv4 address for the static LSP, in dotted decimal notation.

masklen — The length of the IPv4 address mask.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the static LSP information on the switch:

```
Switch(config)# show mpls static-lsp
```

89.11 ping mpls ipv4

Description

The **ping mpls ipv4** command is used to check the connectivity of the LSP and whether the LSP can forward data normally.

Syntax

```
ping mpls ipv4 ip-address / mask-length [ source source-address ]  
[ destination destination-address ] [ repeat repeat-times ] [ timeout timeout ]  
[ interval interval ] [ ttl t ] [ reply-mode reply-mode ] [ fec-type fec-type ]  
[ detail ]
```

Parameter

ip-address—— The destination address, in dotted decimal notation.

masklen—— The mask length, integer, range 0-32.

source-address—— The source IP address, in dotted decimal notation.

destination-address—— The loopback address of the destination IP, in dotted decimal notation, default is 127.0.0.12.

repeat-times—— Number of times packets are sent. Integer, range 1-10, default is 5.

time-out—— Timeout period. Integer, range 1-10, default is 2, unit: seconds.

interval—— Packet transmission interval. Integer, range 1-10, default is 1, unit: seconds.

t—— TTL value. Integer, range 0-255, default is 255.

reply-mode—— The response method after the peer end receives the message. Currently, the following response methods are supported:

- No-reply: The peer does not receive a reply packet.
- Ip-udp-reply: The peer receives a UDP reply packet.
- Ip-udp-ra-reply: The peer receives a UDP packet in response to the router alert.

fec-type—— The FEC type. Currently, the following FEC types are supported:

- generic: General type
- static: Static MPLS configuration
- ldp: LDP generation

detail—— Displays detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Perform an MPLS ping operation on the destination address 192.168.2.1/24, sending 8 request packets:

```
Switch# ping mpls ipv4 192.168.2.1/24 repeat 8
```

89.12 tracert mpls ipv4

Description

The **tracert mpls ipv4** command tests the path information from the source to the destination on an LSP (IPv4).

Syntax

```
tracert mpls ipv4 ip-address / mask-length [ source source-address ]  
[ destination destination-address ] [ repeat repeat-times ] [ timeout timeout ]  
[ interval interval ] [ tll tll ] [ reply-mode reply-mode ] [ fec-type fec-type ]  
[ detail ]
```

Parameter

ip-address—— The destination address, in dotted decimal notation.

masklen—— The mask length, integer, range 0-32.

source-address—— The source IP address, in dotted decimal notation.

destination-address—— The loopback address of the destination IP, in dotted decimal notation, default is 127.0.0.12.

repeat-times—— Number of times packets are sent. Integer, range 1-10, default is 5.

time-out—— Timeout period. Integer, range 1-10, default is 2, unit: seconds.

interval—— Packet transmission interval. Integer, range 1-10, default is 1, unit: seconds.

ttl—— TTL value. Integer, range 0-255, default is 255.

reply-mode—— The response method after the peer end receives the message. Currently, the following response methods are supported:

- No-reply: The peer does not receive a reply packet.
- Ip-udp-reply: The peer receives a UDP reply packet.
- Ip-udp-ra-reply: The peer receives a UDP packet in response to the router alert.

fec-type—— The FEC type. Currently, the following FEC types are supported:

- generic: General type
- static: Static MPLS configuration
- ldp: LDP generation

detail—— Displays detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Perform MPLS tracert operation on destination address 3.3.3.3/32:

```
Switch# tracert mpls ipv4 3.3.3.3/32
```


Chapter 90 LDP Commands (Only for Certain Devices)

LDP (Label Distribution Protocol) is a key protocol in MPLS (Multi-Protocol Label Switching) networks, used for dynamic label allocation and management. MPLS supports multi-layer labels and is connection-oriented, offering high scalability for various services over a unified MPLS/IP infrastructure. Through LDP, Label Switched Routers (LSRs) map network layer routing information directly to data link layer switching paths, dynamically establishing Label Switched Paths (LSPs).

90.1 mpls ldp

Description

This command is used to enable LDP globally. The no version deletes the configuration and disables global LDP. This control determines whether the LDP function is active for the entire switch.

Syntax

mpls ldp
no mpls ldp

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable LDP globally:

```
Switch(config)# mpls ldp
```

90.2 lsr-id

Description

This command is used to configure the LSR-ID used for LDP protocol interaction between devices. The device uses this ID as an identifier for discovering and recognizing LDP neighbors. The no command deletes the LSR-ID configuration.

Syntax

lsr-id *address*

no lsr-id

Parameter

address — The global LSR-ID for LDP, in dotted-decimal format.

Command Mode

LDP Configuration View

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the LDP LSR-ID as 1.1.1.1:

```
Switch(config)# mpls ldp
Switch(config-ldp)# lsr-id 1.1.1.1
```

90.3 transport-address

Description

This command configures the source IP address used by LDP when establishing TCP connections. This address must be the IP of a loopback interface on the device. The no command removes the set transport address.

Syntax

transport-address *ip-address*

no transport-address

Parameter

address — The global LSR-ID for LDP, in dotted-decimal format.

Command Mode

LDP Configuration View

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the LDP transport address as 1.1.1.1:

```
Switch(config)# mpls ldp
Switch(config-ldp)# transport-address 1.1.1.1
```

90.4 explicit-null

Description

This command configures LDP to assign an explicit-null label when allocating the penultimate hop label. The no command cancels the assignment of the explicit-null label.

Syntax

explicit-null
no explicit-null

Parameter

None.

Command Mode

LDP Configuration View

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the device to allocate an explicit-null label for the penultimate hop:

```
Switch(config)# mpls ldp
Switch(config-ldp)# explicit-null
```

90.5 timer

Description

This command sets the hold-time and interval for global LDP protocol messages. The no version restores the default values. Note: For certain message types (e.g., LDP Hello), the interval must be at least one-third of the hold-time.

Syntax

timer hello hold *hello-hold*

timer hello interval *hello-interval*

timer keepalive hold *keepalive-hold*

timer keepalive interval *keepalive-interval*

timer targeted-hello hold *tgt-hello-hold*

timer targeted-hello interval *tgt-hello-hold*

no timer hello hold

no timer hello interval

no timer keepalive hold

no timer keepalive interval

no timer target-hello hold

no timer target-hello interval

Parameter

hello-hold—— Global LDP Hello hold-time, range 3 - 65535. The default value is 15s.

hello-interval—— Global LDP Hello send interval, range 1 - 65535. The default value is 5s.

keepalive-hold—— Global LDP Keepalive hold-time, range 30 - 65535. The default value is 30s.

keepalive-interval—— Global LDP Keepalive send interval, range 1 - 65535. The default value is 10s.

tgt-hello-hold—— Global Targeted-Hello hold-time, range 3 - 65535. The default value is 15s.

tgt-hello-interval—— Global Targeted-Hello send interval, range 1 - 65535. The default value is 45s.

Command Mode

LDP Configuration View

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set Hello interval to 10s/hold 30s; Keepalive interval 20s/hold 60s; and Targeted-Hello interval 10s/hold 30s:

```
Switch(config)# mpls ldp
Switch(config-ldp)# timer hello hold 30
Switch(config-ldp)# timer hello interval 10
Switch(config-ldp)# timer keepalive hold 60
Switch(config-ldp)# timer keepalive interval 20
Switch(config-ldp)# timer targeted-hello hold 30
Switch(config-ldp)# timer targeted-hello interval 10
```

90.6 targeted-peer

Description

This command is used to configure remote LDP neighbors to establish remote LDP sessions. The no command removes the configuration.

Syntax

targeted-peer *ip-address*

no targeted-peer

Parameter

ip-address — The address of the remote neighbor, in dotted-decimal format.

Command Mode

LDP Configuration View

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure a remote neighbor with the address 3.3.3.3:

```
Switch(config)# mpls ldp
Switch(config-ldp)# targeted-peer 3.3.3.3
```

90.7 pwe3

Description

This command is used to configure the LDP PWE3 (Pseudo Wire Emulation Edge-to-Edge) mode, which is an extension of L2VPN. The no command disables the PWE3 mode.

Syntax

pwe3
no pwe3

Parameter

None.

Command Mode

LDP Configuration View

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable LDP PWE3 mode:

```
Switch(config)# mpls ldp
Switch(config-ldp)# pwe3
```

90.8 label control-mode

Description

This command is used to configure the LDP label distribution mode. The LDP label distribution modes include the following two types:

- Independent: This device can independently allocate a label and bind it to a certain FEC, then notify the upstream devices without waiting for labels from downstream devices.

- **Ordered:** For a label mapping of a certain FEC on the device, the device can only send the label mapping for this FEC to the upstream devices when the device already has the label mapping message for the next hop of this FEC, or if this device itself is the egress node for this FEC.

The default LDP label distribution mode is Independent. The `no` command is used to delete the configuration and restore the LDP label distribution mode to the default mode.

Syntax

label control-mode { ordered | independent }
no label control-mode

Parameter

ordered — Sets the LDP label distribution mode to ordered.

independent — Sets the LDP label distribution mode to independent.

Command Mode

LDP Configuration View

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the device's LDP label distribution mode to ordered:

```
Switch(config)# mpls ldp
Switch(config-ldp)# label control-mode ordered
```

90.9 mpls ldp

Description

This command enables LDP packet forwarding on a specific interface. The `no` version disables it.

Syntax

mpls ldp
no mpls ldp

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable MPLS LDP capability on Interface VLAN 10:

```
Switch(config)# interface vlan 10
```

```
Switch(config-if)# mpls
```

```
Switch(config-if)# mpls ldp
```

90.10 LDP Interface Timer

Description

This command configures the hold-time and interval for LDP protocol messages at the interface level. Interface-level settings override global settings. For Hello messages, the interval must be at least one-third of the hold-time.

Syntax

mpls ldp timer hello hold *hello-hold*

mpls ldp timer hello interval *hello-interval*

mpls ldp timer keepalive hold *keepalive-hold*

mpls ldp timer keepalive interval *keepalive-interval*

no mpls ldp timer hello

no mpls ldp timer keepalive

Parameter

hello-hold—— Interface Hello hold-time, range 3 - 65535. The default value is 15s.

hello-interval—— Interface Hello interval, range 1-65535s The default value is 5s.

keepalive-hold—— Interface Keepalive hold-time, range 30 - 65535. The default value is 30s.

keepalive-interval—— Interface Keepalive interval, range 1-65535. The default value is 30s.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure interface vlan 10 with Hello interval 10s/hold 30s and Keepalive interval 20s/hold 60s:

```
Switch(config)# interface vlan 10
Switch(config-if)# mpls ldp timer hello hold 30
Switch(config-if)# mpls ldp timer hello interval 10
Switch(config-if)# mpls ldp timer keepalive hold 60
Switch(config-if)# mpls ldp timer keepalive interval 20
```

90.11 show mpls ldp global

Description

This command used to display global LDP configuration and status information.

Syntax

```
show mpls ldp global
```

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display global LDP configuration:

```
Switch(config)# show mpls ldp global
```

90.12 show mpls ldp instance

Description

This command used to display the information about created LDP instances.

Syntax

show mpls ldp instance [*detail*]

Parameter

detail — Displays detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display LDP instance information:

```
Switch(config)# show mpls ldp instance
```

90.13 show mpls ldp fec

Description

This command used to display FEC (Forwarding Equivalence Class) entry information.

Syntax

show mpls ldp fec [*ipv4 ip-address masklen*]

Parameter

ip-address — The IP address of the FEC, in dotted-decimal format.

masklen — The length of the subnet mask.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display FEC table entries:

```
Switch(config)# show mpls ldp fec
```

90.14 show mpls ldp route

Description

This command used to display routing information received by LDP.

Syntax

show mpls ldp route [**ipv4** *ip-address* / *masklen*]

Parameter

ip-address — The IP prefix of the routing information, in dotted-decimal format.

masklen — The length of the subnet mask.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display routing information received via LDP:

```
Switch(config)# show mpls ldp route
```

90.15 show mpls ldp adjacency

Description

This command used to display information about all LDP adjacencies established by the device.

Syntax

show mpls ldp adjacency [*ip-address*]

Parameter

ip-address — The IP address of the adjacency, in dotted-decimal format.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display discovered LDP adjacencies:

```
Switch(config)# show mpls ldp adjacency
```

90.16 show mpls ldp session

Description

This command used to display information about the LDP sessions established by the device.

Syntax

```
show mpls ldp session [ ip-address ]
```

Parameter

ip-address — The IP address of the session peer, in dotted-decimal notation.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display the established LDP session information on the device:

```
Switch(config)# show mpls ldp session
```

90.17 show mpls ldp interface

Description

This command used to display the LDP interface enablement information on the device.

Syntax

```
show mpls ldp interface [ interface-type interface-number ]
```

Parameter

Interface-type — Interface type.

Interface-number — Interface identifier.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display the LDP interface enablement information on the device:

```
Switch(config)# show mpls ldp interface
```

90.18 show mpls ldp upstream

Description

This command used to display the label information sent upstream by the device to the LDP session.

Syntax

```
show mpls ldp upstream [ session session-address | fec  
fec-address/masklen ]
```

Parameter

session-address — The IP address of the session peer, in dotted-decimal notation. Displays detailed information.

fec-address — The IP address of the FEC, in dotted-decimal notation. Displays detailed information.

masklen — The mask length of the IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display the label information allocated upstream by the LDP session on the device:

```
Switch(config)# show mpls ldp upstream
```

90.19 show mpls ldp downstream

Description

This command is used to display the label information received by the device from the LDP session downstream.

Syntax

```
show mpls ldp downstream [ session session-address | fec  
fec-address/masklen ]
```

Parameter

session-address—— The IP address of the session peer, in dotted-decimal notation. Displays detailed information.

fec-address—— The IP address of the FEC, in dotted-decimal notation. Displays detailed information.

masklen—— The mask length of the IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display the label information allocated downstream by the LDP session on the device:

```
Switch(config)# show mpls ldp downstream
```

90.20 show mpls ldp targeted-peer

Description

This command is used to display neighbor information for the LDP remote sessions established by the device.

Syntax

show mpls ldp targeted-peer [*ip-address*]

Parameter

ip-address—— The IP address of the remote session peer, in dotted-decimal notation. Displays detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display the neighbor information for LDP remote sessions on the device:

```
Switch(config)# show mpls ldp targeted-peer
```

90.21 show mpls ldp entity

Description

This command is used to display the LDP entity information created by the device.

Syntax

show mpls ldp entity [**interface** *interface-type interface-number* |
remote *ip-address*]

Parameter

Interface-type—— Interface type.

Interface-number—— Interface identifier.

ip-address — The IP address of the remote session, in dotted-decimal notation.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display all created LDP entity information on the device:

```
Switch(config)# show mpls ldp entity
```

90.22 show mpls ldp label-space

Description

This command is used to display the label space information used by LDP on the device.

Syntax

```
show mpls ldp label-space [ ip-address ]
```

Parameter

ip-address — The IP route address prefix for the session, in dotted-decimal notation.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display the label space information used by LDP on the device:

```
Switch(config)# show mpls ldp label-space
```


90.23 show mpls ldp vc

Description

This command is used to display dynamic VPWS information created by LDP on the device.

Syntax

show mpls ldp vc [*vc-id* | **statistics**]

Parameter

vc-id—— The VC-ID used for the VPWS connection. Displays detailed VC connection information.

statistics—— Displays statistics for dynamic VPWS connections.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display the dynamic VPWS connection information created by LDP on the device:

```
Switch(config)# show mpls ldp vc
```

90.24 show mpls ldp vpls

Description

This command is used to display dynamic VPLS connection information created by LDP.

Syntax

show mpls ldp vpls [**detail**]

Parameter

detail—— Displays detailed dynamic VPLS connection information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands

Example

Display all dynamic VPLS connection information created by LDP on the device:

```
Switch(config)# show mpls ldp vpls
```

Chapter 91 DLDP Commands (Only for Certain Devices)

DLDP (Device Link Detection Protocol) is used to monitor the link state of fiber-optic or twisted-pair Ethernet cables. When a unidirectional link is detected, the corresponding port will be shut down automatically or manually (depending on the shut mode configured).

91.1 dldp (global)

Description

The **dldp** command is used to enable the DLDP function globally. To disable it, please use **no dldp** command.

Syntax

dldp
no dldp

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the DLDP function globally:

```
Switch(config)# dldp
```

91.2 dldp interval

Description

The **dldp interval** command is used to define the interval of sending advertisement packets on ports that are in the advertisement state.

Syntax

dldp interval *interval-time*

Parameter

interval-time—— The interval of sending advertisement packets. It ranges from 1 to 30 seconds. By default, it is 5 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the interval of sending advertisement packets as 10 seconds:

```
Switch(config)# dldp interval 10
```

91.3 dldp shut-mode

Description

The **dldp shut-mode** command is used to configure the shutdown mode when a unidirectional link is detected.

Syntax

dldp shut-mode { auto /manual }

Parameter

auto —— The switch automatically shuts down ports when a unidirectional link is detected. By default, the shut-mode is auto.

manual ——The switch displays an alert when a unidirectional link is detected. The operation to shut down the unidirectional link ports is accomplished by the users.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the shut-mode as manual:

```
Switch(config)# dldp shut-mode manual
```

91.4 dldp reset (global)



Note: This command is only available on certain devices

Description

The **dldp reset** command is used to reset all the unidirectional links and restart the link detect process.

Syntax

dldp reset

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Reset the DLDP function globally:

```
Switch(config)# dldp reset
```

91.5 dldp(interface)

Description

The **dldp** command is used to enable the DLDP function of the specified port. To disable it, please use **no dldp** command.

Syntax

dldp

no dldp

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the DLDP function of ports 1/0/2-4:

```
Switch (config)# interface range gigabitEthernet 1/0/2-4
Switch (config-if-range)# dldp
```

91.6 dldp reset (interface)



Note: This command is only available on certain devices

Description

The **dldp reset** command is used to reset the specified port and restart the link detect process.

Syntax

dldp reset

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Reset the DLDP function of ports 2-4:

```
Switch (config)# interface range gigabitEthernet 1/0/2-4
Switch (config-if-range)# dldp reset
```

91.7 show dldp

Description

The **show dldp** command is used to display the global configuration of DLDP function such as DLDP global state, DLDP interval and shut mode.

Syntax

show dldp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of DLDP function:

```
Switch# show dldp
```

91.8 show dldp interface

Description

The **show dldp interface** command is used to display the configuration and state of all ports. By default, the configuration and state of all the ports will be displayed.

Syntax

```
show dldp interface
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration and state of all ports:

```
Switch# show dldp interface
```

Chapter 92 SNMP Commands

SNMP (Simple Network Management Protocol) functions are used to manage the network devices for a smooth communication, which can facilitate the network administrators to monitor the network nodes and implement the proper operation.

92.1 snmp-server

Description

The **snmp-server user** command is used to add User. To delete the corresponding User, please use **no snmp-server user** command. The User in an SNMP Group can manage the switch via the management station software. The User and its Group have the same security level and access right.

Syntax

```
snmp-server user name { local | remote } group-name [ smode v3 ] [ slev noAuthNoPriv ] [ cmode none ] [ cpwd confirm-pwd ] [ emode none ] [ epwd encrypt-pwd ]
```

```
snmp-server user name { local | remote } group-name [ smode v3 ] slev authNoPriv cmode { MD5 | SHA } cpwd confirm-pwd [ emode none ] [ epwd encrypt-pwd ]
```

```
snmp-server user name { local | remote } group-name [ smode v3 ] slev authPriv cmode { MD5 | SHA } cpwd confirm-pwd emode { DES | AES-128 } epwd encrypt-pwd
```

Parameter

name — User Name, ranging from 1 to 16 characters.

local | remote — User Type, with local and remote options. Local indicates that the user is connected to a local SNMP engine, while remote means that the user is connected to a remote SNMP engine. As the remote engine ID and user password are used to compute the authentication and privacy digests, before configuring a remote user, you need to set the remote engine ID first.

group-name — The Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

v3 — The security mode for the user. v3 indicates SNMPv3, the most secure model.

slev — The Security Level of SNMP v3 User. There are three options, including *noAuthNoPriv* (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), *authNoPriv* (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and *authPriv* (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). The security level from lowest to highest is: *noAuthNoPriv*, *authNoPriv*, *authPriv*, and the default is *noAuthNoPriv*. The security level of the user should not be lower than the group it belongs to.

cmode — The Authentication Mode of the SNMP v3 User, with *none*, MD5 and SHA options. *None* indicates no authentication method is used, MD5 indicates the port authentication is performed via HMAC-MD5 algorithm and SHA indicates the port authentication is performed via SHA (Secure Hash Algorithm). SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is "none".

confirm-pwd — Authentication Password, ranging from 1 to 32 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

emode — The Privacy Mode of the SNMP v3 User, with *none*, DES and AES-128 options. *None* indicates no privacy method is used, and DES indicates DES encryption method is used, and AES-128 indicates AES-128 encryption method is used. By default, the Privacy Mode is "none".

encrypt-pwd — Privacy Password, ranging from 1 to 32 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add Local User *admin* to Group *group2*, and configure the Security Model of the user as *v3*, the Security Level of the group as *authPriv*, the Authentication Mode of the user as MD5, the Authentication Password as 11111, the Privacy Mode as DES, and the Privacy Password as 22222:

```
Switch(config)# snmp-server user admin local group2 smode v3 slev  
authPriv cmode MD5 cpwd 11111 emode DES epwd 22222
```

92.2 snmp-server view

Description

The **snmp-server view** command is used to add View. To delete the corresponding View, please use **no snmp-server view** command. The OID (Object Identifier) of the SNMP packets is used to describe the managed objects of the switch, and the MIB (Management Information Base) is the set of the OIDs. The SNMP View is created for the SNMP management station to manage MIB objects.

Syntax

snmp-server view *name mib-oid*{ include | exclude }

no snmp-server view *name mib-oid*

Parameter

name — The entry name of View, ranging from 1 to 16 characters. Each View includes several entries with the same name.

mib-oid — MIB Object ID. It is the Object Identifier (OID) for the entry of View, ranging from 1 to 61 characters.

include | exclude — View Type, with include and exclude options. They represent the view entry can/cannot be managed by the SNMP management station individually.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a View named view1, configuring the OID as 1.3.6.1.6.3.20, and this OID can be managed by the SNMP management station:

```
Switch(config)# snmp-server view view1 1.3.6.1.6.3.20 include
```

92.3 snmp-server group

Description

The **snmp-server group** command is used to manage and configure the SNMP group. To delete the corresponding SNMP group, please use **no snmp-server group** command. SNMP v3 provides the VACM (View-based Access Control Model) and USM (User-Based Security Model) mechanisms

for authentication. The users in the SNMP Group can manage the device via the Read View, Write View and Notify View. And the authentication mode and the privacy mode guarantee the high security for the communication between the management station and the managed device.

Syntax

snmp-server group *name* [**smode** v3] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*]

no snmp-server group *name* **smode** v3 **slev** { noAuthNoPriv | authNoPriv | authPriv }

Parameter

name — The SNMP Group name, ranging from 1 to 16 characters. The Group Name, Security Model and Security Level compose the identifier of the SNMP Group. These three items of the Users in one group should be the same.

v3 — The security mode for the group, v3 indicates SNMPv3, the most secure level.

slev — The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). By default, the Security Level is noAuthNoPriv. There is no need to configure this in SNMP v1 Mode and SNMP v2c Mode.

read-view — Select the View to be the Read View. The management access is restricted to read-only, and changes cannot be made to the assigned SNMP View.

write-view — Select the View to be the Write View. The management access is writing only and changes can be made to the assigned SNMP View. The View defined both as the Read View and the Write View can be read and modified.

notify-view — Select the View to be the Notify View. The management station can receive notification messages of the assigned SNMP view generated by the switch's SNMP agent.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a group, and configure the name as group 1, the Security Model as SNMP v3, the security level as authNoPriv, the management access to the assigned View viewDefault as read-write, besides the notification messages sent by View viewDefault can be received by Management station:

```
Switch(config)# snmp-server group group1 smode v3 slev authNoPriv read  
viewDefault write viewDefault notify viewDefault
```

Delete group 1:

```
Switch(config)# no snmp-server group group1 smode v3 slev authNoPriv
```

92.4 snmp-server user

Description

The **snmp-server user** command is used to add User. To delete the corresponding User, please use **no snmp-server user** command. The User in an SNMP Group can manage the switch via the management station software. The User and its Group have the same security level and access right.

Syntax

For L2/L2+ switches:

```
snmp-server user name { local | remote } group-name [ smode v3 ] [ slev  
noAuthNoPriv ] [ cmode none ] [ cpwd confirm-pwd ] [ emode none ] [ epwd  
encrypt-pwd ]
```

```
snmp-server user name { local | remote } group-name [ smode v3 ] slev  
authNoPriv cmode { MD5 | SHA } cpwd confirm-pwd [ emode none ] [ epwd  
encrypt-pwd ]
```

```
snmp-server user name { local | remote } group-name [ smode v3 ] slev  
authPriv cmode { MD5 | SHA } cpwd confirm-pwd emode { DES | AES-128 }  
epwd encrypt-pwd
```

```
no snmp-server user name
```

For L3 switches:

```
snmp-server user name { local | remote } group-name [ smode v3 ] [ slev  
noAuthNoPriv ]
```

```
snmp-server user name { local | remote } group-name [ smode v3 ] slev  
authNoPriv cmode { MD5 | SHA } cpwd confirm-pwd
```

```

snmp-server user name { local | remote } group-name [ smode v3 ] slev
authPriv cmode { MD5 | SHA } cpwd confirm-pwd emode { DES | AES-128 }
epwd encrypt-pwd
no snmp-server user name

```

Parameter

name — User Name, ranging from 1 to 16 characters.

local | remote — User Type, with local and remote options. Local indicates that the user is connected to a local SNMP engine, while remote means that the user is connected to a remote SNMP engine. As the remote engine ID and user password are used to compute the authentication and privacy digests, before configuring a remote user, you need to set the remote engine ID first.

group-name — The Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

v3 — The security mode for the user. v3 indicates SNMPv3, the most secure model.

slev — The Security Level of SNMP v3 User. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). The security level from lowest to highest is: noAuthNoPriv, authNoPriv, authPriv, and the default is noAuthNoPriv. The security level of the user should not be lower than the group it belongs to.

cmode — The Authentication Mode of the SNMP v3 User, with none, MD5 and SHA options. None indicates no authentication method is used, MD5 indicates the port authentication is performed via HMAC-MD5 algorithm and SHA indicates the port authentication is performed via SHA (Secure Hash Algorithm). SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is "none".

confirm-pwd — Authentication Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

emode — The Privacy Mode of the SNMP v3 User, with none DES and AES-128 options. None indicates no privacy method is used, and DES indicates DES encryption method is used, and AES-128 indicates AES-128

encryption method is used, AES-128 privacy mode has a higher security than DES mode. By default, the Privacy Mode is "none".

encrypt-pwd—— Privacy Password, ranging from 1 to 32 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add Local User admin to Group group2, and configure the Security Model of the user as v3, the Security Level of the group as authPriv, the Authentication Mode of the user as MD5, the Authentication Password as 11111, the Privacy Mode as DES, and the Privacy Password as 22222:

```
Switch(config)# snmp-server user admin local group2 smode v3 slev  
authPriv cmode MD5 cpwd 11111 emode AES-128 epwd 2222
```

92.5 snmp-server community

Description

The **snmp-server community** command is used to add Community. To delete the corresponding Community, please use **no snmp-server community** command. SNMP v1 and SNMP v2c adopt community name authentication. The community name can limit access to the SNMP agent from SNMP network management station, functioning as a password.

Syntax

```
snmp-server community name { read-only | read-write } mib-view  
no snmp-server community name
```

Parameter

name—— Community Name, ranging from 1 to 16 characters.

read-only | read-write —— The access rights of the community, with read-only and read-write options.

mib-view—— The MIB View for the community to access.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add community public, and the community has read-write management right to View viewDefault:

```
Switch(config)# snmp-server community public read-write viewDefault
```

92.6 snmp-server host

Description

The **snmp-server host** command is used to add Notification. To delete the corresponding Notification, please use **no snmp-server host** command.

Syntax

```
snmp-server host ip udp-port user-name [vrf vrfName] [smode { v1 | v2c | v3 }] [slev { noAuthNoPriv | authNoPriv | authPriv }] [type { trap | inform }] [retries retries] [timeout timeout]  
no snmp-server host ip user-name
```

Parameter

ip — The IP Address of the management Host. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.100 or fe80::1234.

udp-port — UDP port, which is used to send notifications. The UDP port functions with the IP address for the notification sending. It ranges from 1 to 65535.

user-name — The User name of the management station.

vrfName — The name of the VRF instance where the administrator is located.

smode — The Security Model of the management station, with v1, v2c and v3 options. By default, the option is v1.

slev — The Security Level of SNMP v3 User. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). By default, the Security Level is noAuthNoPriv.

type — The type of the notifications, with trap and inform options. Trap indicates traps are sent, while inform indicates informs are sent. The inform type has a higher security than the trap type and resend and timeout need to be configured if you select this option. You can only select the trap type in Security Model v1. By default, the type of the notifications is "trap".

retries — The amount of times the switch retries an inform request, ranging from 1 to 255. The switch will resend the inform request if it doesn't get the response from the management station during the Timeout interval, and it will terminate resending the inform request if the resending times reach the specified Retry times.

timeout — The maximum time for the switch to wait for the response from the management station before resending a request, ranging from 1 to 3600 in seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a Notification entry, and configure the IP address of the management Host as 192.168.0.146, the UDP port as 162, the User name of the management station as admin, the Security Model of the management station as v2c, the type of the notifications as inform, the maximum time for the switch to wait as 1000 seconds, and the retries time as 100:

For L2/L2+ switches:

```
Switch(config)#snmp-server host 192.168.0.146 162 admin smode v2c  
type inform retries 100 timeout 1000
```

For L3 switches:

```
Switch(config)#snmp-server host 192.168.0.146 162 admin smode v2c  
slev noAuthNoPriv type inform retries 100 timeout 1000
```

```
Switch(config)#snmp-server host fe80::1234 162 admin smode v2c slev  
noAuthNoPriv type inform retries 100 timeout 1000
```

Add a Notification entry, and configure the IP Address of the management Host as fe80::1234, the UDP port as 162, the User name of the management station as admin, the Security Model of the management station as v2c, the

type of the notifications as inform, the maximum time for the switch to wait as 1000 seconds, and the retries time as 100:

```
Switch(config)# snmp-server host fe80::1234 162 admin smode v2c type  
inform retries 100 timeout 1000
```

92.7 snmp-server source-interface

Description

The **snmp-server source-interface** command is used to configure the source interface for sending SNMP trap messages. By default, no source interface is specified for sending traps. After specifying a source interface, the IP address of the source interface will be used as the source IP address of trap messages, helping network management systems identify the alarm source. The source interface for sending traps must be a Layer 3 interface with a configured IP address; otherwise, the command will not take effect. For device security, it is recommended to configure the loopback address as the source interface. To remove this configuration, please use the **no snmp-server source-interface** command.

Syntax

```
snmp-server source-interface [ gigabitEthernet port | port-channel  
port-channel-id | loopback id | vlan vlan-id ]  
no snmp-server source-interface
```

Parameter

port——The port number.

port-channel-id——The ID of the port channel. Member ports in this port channel should all be routed ports.

id——The loopback interface ID.

vlan-id——The VLAN interface ID.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the source interface for SNMP traps as the IP address of loopback 1:

```
Switch(config)# snmp-server source-interface loopback 1
```

92.8 snmp-server engineID

Description

The **snmp-server engineID** command is used to configure the local and remote engineID of the switch. To restore to the default setting, please use **no snmp-server engineID** command.

Syntax

```
snmp-server engineID { [local local-engineID] [remote remote-engineID] }  
no snmp-server engineID
```

Parameter

local-engineID—— Local Engine ID for local clients. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the switch. Its length ranges from 10 to 64 hexadecimal characters, which must be even number meanwhile.

remote-engineID—— Remote Engine ID for the switch. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the remote device which receives informs from the switch. Its length ranges from 10 to 64 hexadecimal characters, which must be even number meanwhile. The **snmp-server engineID** will be disabled if the **local** and **remote** are both not configured.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Specify the local engineID as 1234567890, and the remote engineID as abcdef123456:

```
Switch(config)# snmp-server engineID local 1234567890
```

```
Switch(config)# snmp-server engineID remote abcdef123456
```

92.9 snmp-server traps snmp

Description

The **snmp-server traps snmp** command is used to enable SNMP standard traps which include four types: linkup, linkdown, warmstart and coldstart. The command without parameter enables all SNMP standard traps. All SNMP standard traps are enabled by default. To disable the sending of SNMP standard traps, please use **no snmp-server traps snmp** command.

Syntax

snmp-server traps snmp [linkup | linkdown | warmstart | coldstart |
auth-failure]

no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart |
auth-failure]

Parameter

linkup — Indicates a port status changes from linkdown to linkup, and can be triggered when you connect a device to a port.

linkdown — Indicates a port status changes from linkup to linkdown, and can be triggered when you disconnect a device to a port.

warmstart — Indicates the SNMP feature on the switch is reinitialized with the physical configuration unchanged. The trap can be triggered if you disable and then enable SNMP after the SNMP is completely configured and enabled.

coldstart — Indicates an SNMP initialization caused by the reinitialization of the switch system. The trap can be triggered when you reboot the switch.

auth-failure — Triggered when a received SNMP request fails the authentication.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP standard linkup trap for the switch:

```
Switch(config)# snmp-server traps snmp linkup
```

92.10 snmp-server traps

Description

The **snmp-server traps** command is used to enable SNMP extended traps.

To disable the sending of SNMP extended traps, please use **no snmp-server traps** command. All SNMP extended traps are disabled by default.

Syntax

```
snmp-server traps { rate-limit | cpu | flash | lldp remtableschange | lldp  
topologychange | loopback-detection | storm-control | spanning-tree |  
memory }
```

```
no snmp-server traps { rate-limit | cpu | flash | lldp remtableschange | lldp  
topologychange | loopback-detection | storm-control | spanning-tree |  
memory }
```

Parameter

rate-limit —Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.

cpu —Monitors the load status of the switch CPU. The trap can be triggered when the utilization rate of the CPU has exceeded the limit that you have set. The limit of CPU utilization rate for the switch is 80% by default.

flash —Triggered when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, and so on.

lldp remtableschange —An lldp RemTablesChange notification is sent when the value of lldp StatsRemTableLastChangeTime changes. It can be utilized by an NMS host to trigger LLDP remote systems table maintenance polls.

lldp topologychange —A notification generated by the local device to sense the change in the topology that indicates a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.

loopback-detection —The feature is used to detect loopbacks. And the trap is disabled by default. The system will generate the trap when a loopback is detected or cleared.

storm-control —The feature is used to monitor network storms. And the trap is disabled by default. The system will generate the trap when the rate of broadcast or multicast reaches the limit of storm control.

spanning-tree —The feature is used to monitor the spanning tree status. And the trap is disabled by default. The system will generate the trap in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a packet with TC flag or a TCN packet.

memory —The feature is used to monitor the memory. And the trap is disabled by default. The system will generate the trap when the memory utilization exceeds 80%.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP extended rate-limit trap for the switch:

```
Switch(config)# snmp-server traps rate-limit
```

92.11 snmp-server traps ddm



Note: This command is only available on certain devices.

Description

The **snmp-server traps ddm** command is used to enable the corresponding DDM traps. DDM function is used to monitor the status of the SFP modules inserted into the SFP ports on the switch. The command without parameter enables all SNMP DDM traps. To disable the sending of SNMP DDM traps, use **no snmp-server traps ddm** command. All DDM traps are disabled by default.

Syntax

```
snmp-server traps ddm [ temperature | voltage | bias_current | tx_power |  
rx_power ]
```

```
no snmp-server traps ddm [ temperature | voltage | bias_current | tx_power |  
rx_power ]
```

Parameter

temperature —Monitors the temperature of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold.

voltage —Monitors the voltage of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold.

bias_current —Monitors the bias current of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold.

tx_power —Monitors the TX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold.

rx_power —Monitors the RX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold.

User guidelines

The **snmp-server traps ddm** command without any parameter is used to enable all the types of DDM traps. And the **no snmp-server traps ddm** command without any parameter is used to disable all the types of DDM traps.

For more instructions about the alarm threshold or warning threshold, refer to [Chapter 11 DDM Commands](#).

Command Mode

Global Configuration Mode

Example

Enable all the SNMP DDM traps for the switch:

```
Switch(config)# snmp-server traps ddm
```

92.12 snmp-server traps vlan

Description

The **snmp-server traps vlan** command is used to enable the corresponding VLAN traps. The command without parameter enables all SNMP VLAN traps. To disable this function, please use **no snmp-server traps vlan** command. All VLAN traps are disabled by default.

Syntax

snmp-server traps vlan [create | delete]

no snmp-server traps vlan [create | delete]

Parameter

create — Triggered when certain VLANs are created successfully.

delete — Triggered when certain VLANs are deleted successfully.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all SNMP extended VLAN-related traps for the switch:

```
Switch(config)# snmp-server traps vlan
```

Enable VLAN-created trap only for the switch:

```
Switch(config)# snmp-server traps vlan create
```

92.13 snmp-server traps security

Description

The **snmp-server traps security** command is used to enable the corresponding security traps. To disable this feature, please use **no snmp-server traps security** command. All security traps are disabled by default.

Syntax

```
snmp-server traps security { dhcp-filter | ip-mac-binding }
```

```
no snmp-server traps security { dhcp-filter | ip-mac-binding }
```

Parameter

dhcp-filter — Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server.

ip-mac-binding — Triggered when the ARP Inspection feature is enabled and the switch receives an illegal ARP packet, or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the DHCP filter trap for the switch:

```
Switch(config)# snmp-server traps security dhcp-filter
```

92.14 snmp-server traps security dhcp6-filter

Description

The **snmp-server traps security dhcp6-filter** command is used to enable the IPv6 DHCP Filter illegal message snmp trap and log function. To disable this function, please use **no snmp-server traps security dhcp6-filter** command. All security traps are disabled by default.

Syntax

```
snmp-server traps security dhcp6-filter
```

```
no snmp-server traps security dhcp6-filter
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the IPv6 DHCP Filter illegal message snmp trap and log function:

```
Switch(config)# snmp-server traps security dhcp6-filter
```

92.15 snmp-server traps acl

Description

The **snmp-server traps acl** command is used to enable the ACL trap. To disable this feature, please use **no snmp-server traps acl** command. It is disabled by default.

The trap monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

Syntax

```
snmp-server traps acl
```

```
no snmp-server traps acl
```


Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the ACL trap for the switch:

```
Switch(config)# snmp-server traps acl
```

92.16 snmp-server traps ip

Description

The **snmp-server traps ip** command is used to enable IP traps. To disable this feature, please use **no snmp-server traps ip** command. All IP traps are disabled by default.

Syntax

snmp-server traps ip { change | duplicate }

no snmp-server traps ip { change | duplicate }

Parameter

change — Enable SNMP IP change traps. The trap monitors the IP changed of each interface. The trap can be triggered when the IP address of any interface is changed.

duplicate — Enable SNMP IP duplicate traps. The trap can be triggered when the switch detects an IP conflict event.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the IP-Change trap for the switch:

```
Switch(config)# snmp-server traps ip change
```

92.17 snmp-server traps power

(Only for Certain Devices)



Note: This command is only available on certain devices

Description

The **snmp-server traps power** command is used to enable PoE traps. The command without parameter enables all PoE traps. To disable this feature, please use **no snmp-server traps power** command. All PoE traps are disabled by default.

Syntax

snmp-server traps power [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown]

no snmp-server traps power [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown]

Parameter

over-max-pwr-budget —Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply.

port-pwr-change —Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply.

port-pwr-deny —Triggered when the switch powers off PDs on low-priority PoE ports. When the total power required by the connected PDs exceeds the system power limit, the switch will power off PDs on low-priority PoE ports to ensure stable running of the other PDs.

port-pwr-over-30w —Triggered when the power required by the connected PD exceeds 30 watts.

port-pwr-overload —Triggered when the power required by the connected PD exceeds the maximum power the port can supply.

port-short-circuit —Triggered when a short circuit is detected on a port.

thermal-shutdown —Triggered when the PSE chip overheats. The switch will stop supplying power in this case.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all PoE traps for the switch:

```
Switch(config)# snmp-server traps power
```

92.18 snmp-server traps

link-status

Description

The **snmp-server traps link-status** command is used to enable SNMP link status trap for the specified port. To disable the sending of SNMP link status trap, please use **no snmp-server traps link-status** command. By default, it is enabled.

Syntax

snmp-server traps link-status

no snmp-server traps link-status

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP link status trap for port 3:

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# snmp-server traps link-status
```

92.19 rmon history

Description

The **rmon history** command is used to configure the history sample entry. To return to the default configuration, please use **no rmon history** command.

RMON (Remote Monitoring), basing on SNMP architecture, functions to monitor the network. History Group is one of the commonly used RMON Groups. After a history group is configured, the switch collects network statistics information periodically, based on which the management station can monitor network effectively.

Syntax

rmon history *index* **interface** **gigabitEthernet** *port* [**interval** *interval*]
[**owner** *owner-name*] [**buckets** *number*]
no rmon history *index*

Parameter

index—— The index number of the entry, ranging from 1 to 12, in the format of 1-3,5.

port——The Ethernet port number.

interval—— The interval to take samplings from the port, ranging from 10 to 3600 in seconds. By default, it is 1800.

owner-name—— The owner of the history sample entry, ranging from 1 to 16 characters. By default, it is "monitor".

number—— The maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 130. The default is 50 buckets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the sample port as Gi1/0/2 and the sample interval as 100 seconds for the entry 1-3:

```
Switch(config)# rmon history 1-3 interface gigabitEthernet 1/0/2 interval  
100 owner owner1
```

92.20 rmon event

Description

The **rmon event** command is used to configure the entries of SNMP-RMON Event. To return to the default configuration, please use **no rmon event** command. Event Group, as one of the commonly used RMON Groups, is used to define RMON events. Alarms occur when an event is detected.

Syntax

```
rmon event index [user user-name] [description descript] [type { none |  
log | notify | log-notify }] [owner owner-name]  
no rmon event index
```

Parameter

index—— The index number of the event entry, ranging from 1 to 12. You can only select one entry for each command.

user-name — The name of the User to which the event belongs, ranging from 1 to 16 characters. By default, it is "public".

descript — The description of the event, ranging from 1 to 16 characters. By default, it is empty.

type — The event type, with none, log, notify and both options. None indicates no processing, log indicates logging the event, notify indicates sending trap messages to the management station, and both indicates logging the event and sending trap messages to the management station.

owner-name — The owner of the event entry, ranging from 1 to 16 characters. By default, it is "monitor".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the user name of entry 1, 2, 3 and 4 as user1, the description of the event as description1, the type of event as log and the owner of the event as owner1:

```
Switch(config)# rmon event 1-4 user user1 description description1 type  
log owner owner1
```

92.21 rmon alarm

Description

The **rmon alarm** command is used to configure SNMP-RMON Alarm Management. To return to the default configuration, please use **no rmon alarm** command. Alarm Group is one of the commonly used RMON Groups. RMON alarm management allows monitoring the specific alarm variables. When the value of a monitored variable exceeds the threshold, an alarm event is generated, which triggers the switch to act in the set way.

Syntax

```
rmon alarm index { stats-index sindex } [ alarm-variable { revbyte | revpkt |  
bpkt | mpkt | crc-lign | undersize | oversize | jabber | collision | 64 | 65-127 |  
128-511 | 512-1023 | 1024-10240 } ] [ s-type { absolute | delta } ]  
[ rising-threshold r-hold ] [ rising-event-index r-event ] [ falling-threshold
```

f-hold] [**falling-event-index** *f-event*] [**a-type** {rise | fall | all}] [**owner**
owner-name] [**interval** *interval*]
no rmon alarm *index*

Parameter

index—— The index number of the Alarm Management entry, ranging from 1 to 12, in the format of 1-3,5.

sindex—— Specify the statistics index.

alarm-variable —— The alarm variable. By default, the option is revbyte.

s-type —— Sample Type, which is the sampling method for the selected variable and comparing the value against the thresholds. There are two options, absolute and delta. Absolute indicates comparing the values directly with the thresholds at the end of the sampling interval. Delta indicates subtracting the last sampled value from the current value, and then comparing the difference in the values with the threshold. By default, the Sample Type is absolute.

r-hold—— The rising counter value that triggers the Rising Threshold alarm, ranging from 1 to 2147483647. By default, it is 100.

r-event—— Rise Event, which is the index of the corresponding event which will be triggered if the sampled value is larger than the Rising Threshold. It ranges from 1 to 12.

f-hold—— The falling counter value that triggers the Falling Threshold alarm, ranging from 1 to 2147483647. By default, it is 100.

f-event—— Fall Event, which is the index of the corresponding event which will be triggered if the sampled value is lower than the Falling Threshold. It ranges from 1 to 12.

a-type —— Alarm Type, with rise, fall and all options. Rise indicates that the alarm event will be triggered when the sampled value exceeds the Rising Threshold, fall indicates that the alarm event will be triggered when the sampled value is under the Falling Threshold, and all indicates that the alarm event will be triggered either the sampled value exceeds the Rising Threshold or is under the Falling Threshold. By default, the Alarm Type is all.

owner-name—— The owner of the entry, ranging from 1 to 16 characters. By default, it is monitor.

interval—— The alarm interval time, ranging from 10 to 3600 in seconds. By default, it is 1800.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure rmon alarm entries 1-3 binding with statistics entry 2, the owners as owner1 and the alarm intervals as 100 seconds:

```
Switch(config)#rmon alarm 1-3 stats-index 2 owner owner1 interval 100
```

92.22 rmon statistics

Description

The **rmon statistics** command is used to configure the entries of SNMP-RMON statistics. To delete the corresponding entry, please use **no rmon statistics** command. The maximum supported entries are 1000.

Syntax

```
rmon statistics index interface gigabitEthernet port [owner owner-name]  
[ status { underCreation | valid } ]  
no rmon statistics index
```

Parameter

index — The index number of the statistics entry, ranging from 1 to 65535, in the format of 1-3,5.

port — The statistics port number, in the format of 1/0/1.

owner-name — The creator of the event entry, ranging from 1 to 16 characters. By default, it is "monitor".

status — The status of the statistics entry, either "underCreation" or "valid". "underCreation" means this entry won't take effect until it is modified to "valid"; "valid" means this entry takes effect immediately after it is created.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the statistics entries 1-3 with the statistics port as 1/0/1, owner as owner1 and status as valid:

```
Switch(config)#rmon statistics 1-3 interface gigabitEthernet 1/0/1 owner  
owner1 status valid
```

92.23 show snmp-server

Description

The **show snmp-server** command is used to display SNMP configuration globally.

Syntax

```
show snmp-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display SNMP configuration globally:

```
Switch# show snmp-server
```

92.24 show snmp-server view

Description

The **show snmp-server view** command is used to display the View table.

Syntax

```
show snmp-server view
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the View table:

```
Switch# show snmp-server view
```


92.25 show snmp-server group

Description

The **show snmp-server group** command is used to display the Group table.

Syntax

```
show snmp-server group
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Group table:

```
Switch# show snmp-server group
```

92.26 show snmp-server user

Description

The **show snmp-server user** command is used to display the User table.

Syntax

```
show snmp-server user
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the User table:

```
Switch# show snmp-server user
```

92.27 show snmp-server community

Description

The **show snmp-server community** command is used to display the Community table.

Syntax

show snmp-server community

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Community table:

```
Switch# show snmp-server community
```

92.28 show snmp-server host

Description

The **show snmp-server host** command is used to display the Host table.

Syntax

show snmp-server host

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Host table:

```
Switch# show snmp-server host
```

92.29 show snmp-server engineID

Description

The **show snmp-server engineID** command is used to display the engineID of the SNMP.

Syntax

show snmp-server engineID

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the engineID:

```
Switch# show snmp-server engineID
```

92.30 show rmon history

Description

The **show rmon history** command is used to display the configuration of the history sample entry.

Syntax

```
show rmon history [ index ]
```

Parameter

index — The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all history sample entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of all history sample entries:

```
Switch# show rmon history
```

92.31 show rmon event

Description

The **show rmon event** command is used to display the configuration of SNMP-RMON Event.

Syntax

```
show rmon event [ index ]
```

Parameter

index — The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all SNMP-RMON enabled entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Event configuration of entry1-4:

```
Switch# show rmon event 1-4
```

92.32 show rmon alarm

Description

The **show rmon alarm** command is used to display the configuration of the Alarm Management entry.

Syntax

```
show rmon alarm [ index ]
```

Parameter

index — The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all Alarm Management entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of the Alarm Management entry 1-2:

```
Switch# show rmon alarm 1-2
```

92.33 show rmon statistics

Description

The **show rmon statistics** command is used to display the configuration of the specified statistics entry.

Syntax

show rmon statistics [*index*]

Parameter

index — The index number of the statistics entry selected to display the configuration, ranging from 1 to 65535. By default, the configuration of all statistics entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of the statistics entry 1:

```
Switch#show rmon statistics 1
```

Chapter 93 NETCONF Commands (Only for Certain Devices)



Note: NETCONF commands are only available on certain devices.

The Network Configuration Protocol (NETCONF) defines a simple mechanism for managing network devices by allowing the retrieval of configuration data information and enabling the uploading and manipulation of new configuration data. This protocol permits devices to expose a full-fledged formal Application Programming Interface (API). Applications can utilize this straightforward API to send and receive complete or partial sets of configuration.

93.1 netconf ssh

Description

The **netconf ssh** command is used to enable the NETCONF SSH connection function. Only when the NETCONF SSH connection function is enabled can the network administrator configure and manage the switch through NETCONF through port 830. To disable NETCONF SSH connection, please use the **no netconf ssh** command.

Syntax

netconf ssh

no netconf ssh

Parameter

None

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the NETCONF SSH connection on the switch:

```
Switch(config)#netconf ssh
```

Chapter 94 PoE Commands (Only for Certain Devices)



Note: PoE commands are only available on certain devices.

PoE (Power over Ethernet) technology describes a system to transmit electrical power along with data to remote devices over standard twisted-pair cable in an Ethernet network. It is especially useful for supplying power to IP telephones, wireless LAN access points, cameras and so on.

94.1 power inline consumption (global)

Description

The **power inline consumption** command is used to configure the max power the PoE switch can supply globally.

Syntax

power inline consumption *power-limit*

Parameter

power-limit——The max power the PoE switch can supply.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the max power the PoE switch can supply as 160 W:

```
Switch(config)# power inline consumption 160
```

94.2 power profile

Description

The **power profile** command is used to create a PoE profile for the switch. To delete the configured PoE profile configuration, please use **no power profile**

command. PoE Profile is a short cut for the configuration of the PoE port. In a PoE profile, the PoE status, PoE priority and power limit are configured. You can specify a PoE profile for each PoE port individually.

Syntax

```
power profile name [supply {enable | disable} [priority {low | middle | high}  
[consumption { power-limit | auto | class1 | class2 | class3 | class4 } ] ] ]  
no power profile [name]
```

Parameter

name — The PoE profile name, ranging from 1 to 16 characters. If the name being assigned contains spaces then put it inside double quotes.

supply — The PoE status of the port in the profile. By default, the PoE status is "enable".

priority — The PoE priority of the port in the profile. The priority levels include "high", "middle" and "low" in descending order. When the supply power exceeds the system power limit, the PD linked to the port with lower priority will be disconnected. By default, the PoE priority is "low".

consumption — The max power the port in the profile can supply, with five options: "power-limit", "auto", "class1", "class2", "class3" and "class4".

"Power-limit" indicates you can manually enter a value ranging from 1 to 300. The value is in the unit of 0.1 watt. For instance, if you want to configure the max power as 5w, you should enter 50. "Auto" indicates the value is assigned automatically by the PoE switch. "Class1" represents 4w. "Class2" represents 7w. "Class3" represents 15.4w. "Class4" represents 30w.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Create a PoE profile named "IP Camera" whose PoE status is "enable", PoE priority is "low" and the power limit is "5w":

```
Switch(config)# power profile "IP Camera" supply enable priority low  
consumption 50
```


94.3 power inline consumption (interface)

Description

The **power inline consumption** command is used to configure the power limit the corresponding port can supply.

Syntax

```
power inline consumption { power-limit | auto | class1 | class2 | class3 | class4 }
```

Parameter

power-limit—— The max power the port in the profile can supply, with five options: "power-limit", "auto", "class1", "class2", "class3" and "class4". "Power-limit" indicates you can manually enter a value ranging from 1 to 300. The value is in the unit of 0.1 watt. For instance, if you want to configure the max power as 5w, you should enter 50. "Auto" indicates the value is assigned automatically by the PoE switch. "Class1" represents 4w. "Class2" represents 7w. "Class3" represents 15.4w. "Class4" represents 30w.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the power limit as "5w" for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power inline consumption 50
```

94.4 power inline consumption (unit)

Description

The **power inline unit consumption** command is used to specify the maximum power a stack unit can supply.

Syntax

power inline unit {*unit id*} **consumption** {power-limit}

Parameter

unit id—— Stack unit ID, ranging from 1-4

power-limit —— Specify the maximum power the PoE switch can supply, which depends on actual power usage.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the maximum power unit 1 can supply to 402W:

```
Switch(config)#power inline unit 1 consumption 402
```

94.5 power inline priority

Description

The **power inline priority** command is used to configure the PoE priority for the corresponding port

Syntax

power inline priority { low | middle | high }

Parameter

priority —— The PoE priority of the port. The priority levels include "high", "middle" and "low" in descending order. When the supply power exceeds the system power limit, the PD linked to the port with lower priority will be disconnected. By default, the priority level is "low".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the PoE priority as "low" for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power inline priority low
```

94.6 power inline supply

Description

The **power inline supply** command is used to configure the PoE status of the corresponding port.

Syntax

```
power inline supply { enable | disable }
```

Parameter

enable | disable — The PoE status of the port. By default, the PoE status is "enable".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the PoE feature for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power inline supply enable
```

94.7 power inline profile

Description

The **power inline profile** command is used to bind a PoE profile to the corresponding port. To cancel the bind relation, please use **no power inline profile** command.

Syntax

```
power inline profile name
no power inline profile
```

Parameter

name — The name of the PoE profile to be bound to the port. If the name

being assigned contains spaces then put it inside double quotes.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Bind the PoE profile named "IP Camera" to port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power inline profile "IP Camera"
```

94.8 power inline time-range

Description

The **power inline time-range** command is used to bind a PoE time-range to the corresponding port. To cancel the bind relation, please use **no power inline time-range** command.

Syntax

power inline time-range *name*
no power inline time-range

Parameter

name — The name of the PoE time-range to be bound to the port.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Bind the PoE time-range named "tRange2" to port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power inline time-range tRange2
```

94.9 show power inline

Description

The **show power inline** command is used to display the global PoE information of the system.

Syntax

show power inline

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the PoE information of the system:

```
Switch# show power inline
```

94.10 show power inline configuration interface

Description

The **show power inline configuration interface** command is used to display the PoE configuration of the certain port.

Syntax

show power inline configuration interface [**fastEthernet** *port* |
gigabitEthernet *port* | **ten-gigabitEthernet** *port*]

Parameter

port — The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the PoE configuration of all ports:

```
Switch# show power inline configuration interface
```

94.11 show power inline information interface

Description

The **show power inline information** command is used to display the PoE information of the certain port.

Syntax

```
show power inline information interface [ fastEthernet port |  
gigabitEthernet port | ten-gigabitEthernet port ]
```

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the PoE information of all ports:

```
Switch# show power inline information interface
```

94.12 show power profile

Description

The **show power profile** command is used to display the defined PoE profile.

Syntax

```
show power profile
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined PoE profile:

```
Switch# show power profile
```

94.13 power recovery status enable

Description

The **power recovery status enable** command is used to enable the power auto recovery function globally. To disable this function, please use **power recovery status disable** command

Syntax

power recovery status enable
power recovery status disable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the power auto recovery function globally:

```
Switch(config)# power recovery status enable
```

94.14 power recovery status

Description

The **power recovery ststus** command is used to configure the power recovery status and parameters of a specified port..

Syntax

power recovery ststus {disable|enable} ip *ipv4_addr* startup *startup delay* interval *ping interval* retry *failure threshold* break *break time*

Parameter

ipv4_addr—— lpv4 address, in string format, for example, 192.168.0.1.

startup delay—— Feature startup delay(S), ranging from 30 to 600.

ping interval—— Ping package interval(S), ranging from 10 to 120.

failure threshold—— Number of ping failures, ranging from 1 to 10.

break time—— Break time after detecting abnormal POE status(S), ranging from 3 to 120.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the power recovery status of port 2 and configure relevant parameters:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power recovery status enable ip 192.168.0.1 startup 60
interval 60 retry 5 break 60
```

94.15 show power recovery

Description

The **show power recovery** command is used to display all POE auto recovery configurations.

Syntax

show power recovery

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display all POE auto recovery configurations:

```
Switch(config)#show power recovery
```


94.16 show power recovery interface

Description

The **show power recovery interface** command is used to display power auto recovery configurations of the selected port.

Syntax

show power recovery *interface* [fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet] *port list*

Parameter

interface—— Port type.

port list—— Port number list.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display power auto recovery configurations of:

```
Switch(config)#show power recovery
```

Chapter 95 ARP Inspection Commands

ARP (Address Resolution Protocol) Detect function is to protect the switch from the ARP cheating, such as the Network Gateway Spoofing and Man-In-The-Middle Attack, etc.

95.1 ip arp inspection

Description

The **ip arp inspection** command is used to enable the ARP Detection function globally. To disable the ARP Detection function, please use **no ip arp detection** command.

Syntax

ip arp inspection
no ip arp inspection

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ARP Detection function globally:

```
Switch(config)#ip arp inspection
```

95.2 ip arp inspection validate

Description

The **ip arp inspection validate** command is used to enable the switch to check whether the received ARP packet is illegal. To disable the feature please use **no ip arp inspection validate** command.

Syntax

ip arp inspection validate { src-mac | dst-mac | ip }
no ip arp inspection validate { src-mac | dst-mac | ip }

Syntax

src-mac — Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.

dst-mac — Enable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

ip — Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet

```
Switch(config)#ip arp inspection validate src-mac
```

95.3 ip arp inspection vlan

Description

The **ip arp inspection vlan** command is used to enable the ARP Detection function on VLANs. To disable the ARP Detection function on VLANs, please use **no ip arp detection vlan** command.

Syntax

ip arp inspection vlan *vlan-list*

no ip arp inspection vlan *vlan-list*

Syntax

vlan-list — Enter the VLAN ID. The format is 1,5-9.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ARP Detection function on VLAN 2:

```
Switch(config)#ip arp inspection vlan 2
```

95.4 ip arp inspection vlan logging

Description

The **ip arp inspection vlan logging** command is used to enable the Log function on the specific VLAN. To disable the Log function on the VLAN, please use **no ip arp inspection vlan logging** command.

Syntax

ip arp inspection vlan *vlan-list* logging

no ip arp inspection vlan *vlan-list* logging

Syntax

vlan-list — Enter the VLAN ID. The format is 1,5-9.

logging — Enable the Log feature to make the switch generate a log when an ARP packet is discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the log feature on VLAN 2:

```
Switch(config)#ip arp inspection vlan 2 logging
```

95.5 ip arp inspection trust

Description

The **ip arp inspection trust** command is used to configure the port for which the ARP Detect function is unnecessary as the Trusted Port. To clear the Trusted Port list, please use **no ip arp detection trust** command. The specific ports, such as up-linked port and routing port and LAG port, should be set as Trusted Port. To ensure the normal communication of the switch, please configure the ARP Trusted Port before enabling the ARP Detect function.

Syntax

ip arp inspection trust

no ip arp inspection trust

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Gigabit Ethernet ports 1/0/2-5 as the Trusted Port:

```
Switch(config)#interface range gigabitEthernet 1/0/2-5
Switch(config-if-range)#ip arp inspection trust
```

95.6 ip arp inspection limit-rate

Description

The **ip arp inspection limit-rate** command is used to configure the ARP speed of a specified port. To restore to the default speed, please use **no ip arp inspection limit-rate** command.

Syntax

ip arp inspection limit-rate *value*

no ip arp inspection limit-rate

Parameter

value——The value to specify the maximum amount of the received ARP packets per second, ranging from 1 to 300 in pps(packet/second). By default, the value is 100.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum amount of the received ARP packets per second as 50 pps for Gigabit Ethernet port 5:

```
Switch(config)#interface gigabitEthernet 1/0/5
Switch(config-if)#ip arp inspection limit-rate 50
```

95.7 ip arp inspection burst-interval

Description

The **ip arp inspection burst-interval** command is used to configure the burst interval of a specified port. To restore to the default speed, please use **no ip arp inspection burst-interval** command.

Syntax

```
ip arp inspection burst-interval value
no ip arp inspection burst-interval
```

Parameter

value—— Specify a time range. If the speed of received ARP packets in this time range reaches the limit for this time range, the port will be shut down. The valid values are from 1 to 15 seconds, and the default value is 1 second.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the burst interval as 2 seconds for Gigabit Ethernet port 5:

```
Switch(config)#interface gigabitEthernet 1/0/5
Switch(config-if)#ip arp inspection burst-interval 2
```

95.8 ip arp inspection recover

Description

The **ip arp inspection recover** command is used to restore a port to the ARP transmit status from the ARP filter status.

Syntax

ip arp inspection recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Restore Gigabit Ethernet port 1/0/5 to the ARP transmit status:

```
Switch(config)#interface gigabitEthernet 1/0/5
Switch(config-if)#ip arp inspection recover
```

95.9 ip arp inspection exceed

Description

The **ip arp inspection exceed** command is used to configure the overspeed action. To delete this action, please use **no ip arp inspection exceed** command.

Syntax

ip arp inspection exceed [**drop** | **shutdown**] *recover-time*
no ip arp inspection exceed

Parameter

drop—— Drop messages when speeding.
shutdown—— Shut ports down when speeding.
recover-time—— Configure self-recovery time.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the overspeed action as dropping messages when speeding and self-recovery time as 2 seconds for Gigabit Ethernet port 5:

```
Switch(config)#interface gigabitEthernet 1/0/5  
Switch(config-if)#ip arp inspection exceed drop 2
```

95.10 show ip arp inspection

Description

The **show ip arp inspection** command is used to display the ARP detection global configuration including the enable/disable status and the Trusted Port list.

Syntax

show ip arp inspection

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP detection configuration globally:

```
Switch(config)#show ip arp inspection
```

95.11 show ip arp inspection interface

Description

The **show ip arp inspection interface** command is used to display the interface configuration of ARP detection.

Syntax

show ip arp inspection interface [**gigabitEthernet** *port*]

Parameter

port —The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Gigabit Ethernet port 1/0/1:

```
Switch(config)#show ip arp inspection interface gigabitEthernet 1/0/1
```

Display the configuration of all Ethernet ports:

```
Switch(config)#show ip arp inspection interface
```

95.12 show ip arp inspection vlan

Description

The **show ip arp inspection vlan** command is used to display the VLAN configuration of ARP detection.

Syntax

show ip arp inspection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP Inspection configuration of VLAN:

```
Switch(config)#show ip arp inspection vlan
```

95.13 show ip arp inspection statistics

Description

The **show ip arp inspection statistics** command is used to display the number of the illegal ARP packets received.

Syntax

show ip arp inspection statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the number of the illegal ARP packets received:

```
Switch(config)#show ip arp inspection statistics
```

95.14 clear ip arp inspection statistics

Description

The **clear ip arp inspection statistics** command is used to clear the statistic of the illegal ARP packets received.

Syntax

clear ip arp inspection statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the statistic of the illegal ARP packets received:

```
Switch(config)#clear ip arp inspection statistics
```

Chapter 96 ND Detection Commands

The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configurations.

96.1 ipv6 nd detection

Description

The **ipv6 nd detection** command is used to enable the ND Detection function globally. To disable the ND Detection function, please use **no ipv6 nd detection** command.

Syntax

ipv6 nd detection
no ipv6 nd detection

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function globally:

```
Switch(config)#ipv6 nd detection
```

96.2 ipv6 nd detection vlan

Description

The **ipv6 nd detection vlan** command is used to enable ND Detection function on a specified VLAN. To disable ND Detection function on this VLAN, please use **no ipv6 nd detection vlan** command.

Syntax

ipv6 nd detection vlan *vlan-range*
no ipv6 nd detection vlan *vlan-range*

Parameter

vlan-range——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function on VLAN 1,4,6-7:

```
Switch(config)#ipv6 nd detection vlan 1,4,6-7
```

96.3 ipv6 nd detection vlan logging

Description

The **ipv6 nd detection vlan logging** command is used to enable Log function on a specified VLAN. To disable Log function on this VLAN, please use **no ipv6 nd detection vlan logging** command.

Syntax

ipv6 nd detection vlan *vlan-range* **logging**

no ipv6 nd detection vlan *vlan-range* **logging**

Parameter

vlan-range——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the Log function on VLAN 1,4,6-7:

```
Switch(config)#ipv6 nd detection vlan 1,4,6-7 logging
```

96.4 ipv6 nd detection trust

Description

The **ipv6 nd detection trust** command is used to configure the port for which the ND Detection function is unnecessary as the Trusted Port. To clear the

Trusted Port list, please use **no ipv6 nd detection trust** command .The specific port, such as up-linked port, routing port and LAG port, should be set as Trusted Port. To ensure the normal communication of the switch, please configure the ND Detection Trusted Port before enabling the ND Detection function.

Syntax

ipv6 nd detection trust

no ipv6 nd detection trust

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet/ interface port-channel / interface range port-channel)

Example

Configure the Gigabit Ethernet ports 1/0/2-5 as the Trusted Port:

```
Switch(config)#interface range gigabitEthernet 1/0/2-5
```

```
Switch(config-if-range)#ipv6 nd detection trust
```

96.5 show ipv6 nd detection

Description

The **show ipv6 nd detection** command is used to display the ND detection global configuration including the enable/disable status.

Syntax

show ipv6 nd detection

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ND Detection configuration globally:

```
Switch(config)#show ipv6 nd detection
```

96.6 show ipv6 nd detection interface

Description

The **show ipv6 nd detection interface** command is used to display the interface configuration of ND Detection.

Syntax

show ipv6 nd detection interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port——The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the configuration of Gigabit Ethernet port 1/0/1:

```
Switch(config)#show ipv6 nd detection interface gigabitEthernet 1/0/1
```

Display the configuration of all Ethernet ports:

```
Switch(config)#show ipv6 nd detection interface
```

96.7 show ipv6 nd detection statistics



Note: This command is only available on certain devices.

Description

The **show ipv6 nd detection statistics** command is used to display the ND statistics of each VLAN, including the number of forwarded and dropped ND packets.

Syntax

show ipv6 nd detection statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ipv6 ND Detection statistics of each VLAN.

```
Switch(config)#show ipv6 nd detection statistics
```

96.8 show ipv6 nd detection vlan

Description

The **show ipv6 nd detection vlan** command is used to display the VLAN configuration of ND Detection.

Syntax

show ipv6 nd detection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ipv6 ND Detection configuration of VLAN.

```
Switch(config)#show ipv6 nd detection vlan
```


Chapter 97 System Log Commands

The log information will record the settings and operation of the switch respectively for you to monitor operation status and diagnose malfunction.

97.1 logging buffer

Description

The **logging buffer** command is used to store the system log messages to an internal buffer. To disable the log buffer function, please use the **no logging buffer** command. Local Log is the system log information saved in the switch. It has two output channels, that is, it can be saved to two different positions, log buffer and log flash memory. The log buffer indicates the RAM for saving system log and the information in the log buffer can be got by [show logging buffer](#) command. It will be lost when the switch is restarted.

Syntax

logging buffer

no logging buffer

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the system log buffer:

```
Switch(config)#logging buffer
```

97.2 logging buffer level

Description

The **logging buffer level** command is used to configure the severity level and the status of the configuration input to the log buffer. To return to the default configuration, please use **no logging buffer level** command.

Syntax

logging buffer level *level*

no logging buffer level

Parameter

level—— Severity level of the log information output to each channel. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output. By default, it is 6 indicating that the log information with level 0-6 will be saved in the log buffer.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Set the severity level as 5:

```
Switch(config)#logging buffer level 5
```

97.3 logging file flash

Description

The **logging file flash** command is used to store the log messages in a file in the flash on the switch. To disable the log file flash function, please use **no logging file flash** command. This function is disabled by default. The log file flash indicates the flash sector for saving system log. The information in the log file of the flash will not be lost after the switch is restarted and can be got by the [show logging flash](#) command.

Syntax

logging file flash

no logging file flash

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the log file flash function:

```
Switch(config)#logging file flash
```

97.4 logging file flash frequency

Description

The **logging file flash frequency** command is used to specify the frequency to synchronize the system log file in the log buffer to the flash. To resume the default synchronizing frequency, please use the **no logging file flash frequency** command.

Syntax

logging file flash frequency { *periodic* *periodic* | immediate }

no logging file flash frequency

Parameter

periodic — The frequency to synchronize the system log file in the log buffer to the flash, ranging from 1 to 48 hours. By default, the synchronization process takes place every 24 hours.

Immediate — The system log file in the buffer will be synchronized to the flash immediately. This option will reduce the life of the flash and is not recommended.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Specify the log file synchronization frequency as 10 hours:

```
Switch(config)#logging file flash frequency periodic 10
```

97.5 logging file flash level

Description

The **logging file flash level** command is used to specify the system log message severity level. Messages with a severity level equal to or higher than this value will be stored to the flash. To restore to the default level, please use **no logging file flash level** command.

Syntax

logging file flash level *level*

no logging file flash level

Parameter

level—— Severity level of the log message. There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be saved to the flash. By default, it is 3 indicating that the log message marked with 0–3 will be saved in the log flash.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Save the log messages with their severities equal or higher than 7 to the flash :

```
Switch(config)#logging file flash level 7
```

97.6 logging host index

Description

The **logging host index** command is used to configure the Log Host. To clear the configuration of the specified Log Host, please use **no logging host index** command. Log Host is to receive the system log from other devices. You can remotely monitor the settings and operation status of other devices through the log host.

Syntax

logging host index *index ip-address level*

logging host index *index ip-address protocol* { udp|tcp|tls|dtls } [**port** *port*]
level level

no logging host index *idx*

Parameter

index—— Index of the syslog server, range 1–4.

ip-address—— IP address of the syslog server, supports IPv4 and IPv6.

level—— Filter level for syslogs sent to this server. Syslogs with a severity higher than this level will be filtered out.

port—— Listening port of the syslog server, range 1–65535.

protocol—— Transport protocol used for communication with the syslog server. Supports four protocols: udp, tcp, dtls, and tls.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a logging host without specifying a transport protocol:

```
Switch(config)# logging host index 1 192.168.0.148 5
```

Create a logging host specifying TLS as the transport protocol:

```
Switch(config)# logging host index 1 192.168.0.148 protocol tls level 5
```

97.7 logging host verify-peer

Description

The **logging host verify-peer** command only applies to log hosts using TLS or DTLS transport protocols. It configures whether the device verifies the legitimacy of the peer syslog server's certificate. Verification is enabled by default.

Syntax

logging host verify-peer

no logging host verify-peer

Parameter

None.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the device to not verify the syslog server's certificate legitimacy, only using the encryption feature of TLS:

```
Switch(config)# no logging host verify-peer
```

97.8 logging host source-interface

Description

The **logging host source-interface** command is used to specify the source interface used when the switch sends syslog messages to a configured log host. When configured, the switch uses the IP address of the specified interface as the source IP for syslog packets.

Syntax

logging host source-interface vlan *vlan-id*

logging host source-interface loopback *loopback-interface-number*

logging host source-interface port-channel *port-channel-interface-number*

logging host

source-interface { **fastEthernet** | **gigabitEthernet** | **two-gigabitEthernet** | **ten-gigabitEthernet** | **twentyFive-gigabitEthernet** | **hundred-gigabitEthernet** } *port*

Parameter

vlan-id—— VLAN ID. Valid values are 1 to 4094.

loopback-interface-number—— Loopback interface number. Valid values are 1 to 64.

port-channel-interface-number — Port-channel interface number. Valid values are 1 to 64.

fastEthernet port — 100M Ethernet port number.

gigabitEthernet port — 1G Ethernet port number.

two-gigabitEthernet port — 2.5G Ethernet port number.

ten-gigabitEthernet port — 10G Ethernet port number.

twentyFive-gigabitEthernet port — 25G Ethernet port number.

hundred-gigabitEthernet port — 100G Ethernet port number.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure VLAN interface 2 and set it as the source interface for syslog messages sent to the log host:

```
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface vlan 2
Switch(config-if)#ip address 192.168.0.1 255.255.255.0
Switch(config)#logging host source-interface vlan 2
```

97.9 logging host download

Description

The **logging host download** command is used to download the root certificate, client certificate, and client private key to the device through TFTP.

Syntax

```
logging host download ip-address ip-address [ca-cert ca-cert]
[client-cert client-cert] [client-key client-key]
```

Parameter

ip-address — IP address of the TFTP server.

ca-cert—— Root certificate file name stored on the TFTP server.

client-cert—— Client certificate file name stored on the TFTP server.

client-key—— Client private key file name stored on the TFTP server.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Download a client certificate named client.crt from a TFTP server with IP address 192.168.0.148:

```
switch(config)# logging host download ip-address 192.168.0.148  
client-cert client.crt
```

Download the root certificate, client certificate, and client private key named root.crt, client.crt, and client.key respectively from a TFTP server with IP address 192.168.0.148:

```
switch(config)# logging host download ip-address 192.168.0.148 ca-cert  
root.crt client-cert client.crt client-key client.key
```

97.10 logging host remove

Description

The **logging host remove** command is used to delete certificates downloaded to the device for use by log hosts.

Syntax

```
logging host remove [ ca-cert ] [ client-cert ] [ client-key ]
```

Parameter

ca-cert —— Root certificate stored on the device.

client cert —— Client certificate stored on the device.

client-key —— Client private key stored on the device.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Simultaneously delete the root certificate, client certificate, and client private key downloaded to the device:

```
switch(config)# logging host remove ca-cert client-cert client-key
```

97.11 logging console

Description

The **logging console** command is used to send the system logs to the console port. To disable logging to the console, please use **no logging console** command. This function is enabled by default.

Syntax

logging console

no logging console

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable logging to the console port:

```
Switch(config)# logging console
```

97.12 logging console level

Description

The **logging console level** command is used to limit messages logged to the console port. System logs no higher than the set threshold level will be displayed on the console port. To restore the threshold level to default value, please use **no logging console level** command.

Syntax

logging console level *level*

no logging console level

Parameter

level — Severity level of the log information output to the console port.

There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0–5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Output the log information with severity levels between 0–7 to the console port:

```
Switch(config)# logging console level 7
```

97.13 logging monitor

Description

The **logging monitor** command is used to display the system logs on the terminal devices. To disable logging to the terminal, please use **no logging monitor** command. This function is enabled by default.

Syntax

logging monitor

no logging monitor

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Disable logging to the terminal devices:

```
Switch(config)# no logging monitor
```

97.14 logging monitor level

Description

The **logging monitor level** command is used to limit messages logged to the terminal devices. System logs no higher than the set threshold level will be displayed on the terminal devices. To restore the threshold level to default value, please use **no logging monitor level** command.

Syntax

logging monitor level *level*

no logging monitor level

Parameter

level—— Severity level of the log information output to the terminal devices. There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0–5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Output the log information with severity levels between 0–7 to the terminal devices:

```
Switch(config)# logging monitor level 7
```

97.15 clear logging

Description

The **clear logging** command is used to clear the information in the log buffer and log file.

Syntax

clear logging [buffer | flash]

Parameter

buffer | flash —The output channels: buffer and flash. Clear the information of the two channels, by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Clear the information in the log file:

```
Switch(config)# clear logging buffer
```

97.16 show logging local-config

Description

The **show logging local-config** command is used to display the configuration of the Local Log output to the console, the terminal, the log buffer and the log file.

Syntax

show logging local-config

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the Local Log:

```
Switch(config)# show logging local-config
```

97.17 show logging

Description

The **show logging** command is used to display all filtered logs from both the buffer and flash storage.

Syntax

```
show logging | [include include] [exclude exclude]
```

Parameter

include—— A string that the log message must contain. Length range: 1-255 characters.

exclude—— A string that the log message must not contain. Length range: 1-255 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Filter for all logs that contain the string "SNMP" but do not contain the string "Add"

```
Switch(config)# show logging | include SNMP exclude Add
```

97.18 show logging loghost

Description

The **show logging loghost** command is used to display the configuration of the log host.

Syntax

```
show logging loghost [ index ]
```

Parameter

index——The index of the log host whose configuration will be displayed, ranging from 1 to 4. Display the configuration of all the log hosts by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the log host 2:

```
Switch(config)# show logging loghost 2
```

97.19 show logging loghost certificate-files

Description

The **show logging loghost certificate-files** command is used to display the digest information of certificates related to log hosts on the device.

Syntax

show logging loghost certificate-files

Parameter

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display digest information of certificates downloaded to the device:

```
Switch(config)# show logging loghost certificate-files
```

97.20 show logging buffer

Description

The **show logging buffer** command is used to display all filtered logs from the buffer only.

Syntax

show logging buffer | [**include** *include*] [**exclude** *exclude*]

Parameter

include—— A string that the log message must contain. Length range: 1-255 characters.

exclude—— A string that the log message must not contain. Length range: 1-255 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Filter for all logs that do not contain the string "AAA":

```
Switch(config)# show logging buffer | exclude AAA
```

97.21 show logging flash

Description

The **show logging flash** command is used to display all filtered logs from the flash storage only.

Syntax

show logging buffer | [**include** *include*] [**exclude** *exclude*]

Parameter

include—— A string that the log message must contain. Length range: 1-255 characters.

exclude—— A string that the log message must not contain. Length range: 1-255 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Filter for all logs that contain the string "vlan":

```
Switch(config)# show logging flash | include
```