

# PIXIETECH

CLI configuration guide

## Table Content

Chapter 1 System Management Commands.....	34
1.1 Commands for Managing Configuration Files.....	34
1.1.1 copy.....	34
1.1.2 delete.....	34
1.1.3 dir.....	35
1.1.4 show configuration.....	35
1.1.5 format.....	35
1.1.6 more.....	35
1.2 Basic System Management Commands.....	36
1.2.1 boot flash.....	36
1.2.2 cd.....	37
1.2.4 date.....	37
1.2.6 md.....	37
1.2.7 pwd.....	38
1.2.8 rd.....	38
1.2.9 rename.....	38
1.2.10 reboot.....	38
1.2.11 alias.....	39
1.2.12 boot system flash.....	39
1.2.13 help.....	40
1.2.14 history.....	40
1.2.15 show.....	41
1.2.16 show alias.....	42
1.2.17 show break.....	42
Chapter 2 Terminal Service Configuration Commands.....	43
2.1 Telnet Configuration Commands.....	43
2.1.1 telnet.....	43
2.1.2 ip telnet.....	45
2.1.3 ctrl-shift-6+x (the current connection is mounted).....	47
2.1.4 where.....	47
2.1.5 resume.....	48
2.1.6 disconnect.....	49
2.1.7 clear telnet.....	51
2.1.8 show telnet.....	51
2.1.9 debug telnet.....	52
2.2 Terminal Configuration Commands.....	52

2.2.1	attach-port.....	53
2.2.2	autocommand .....	54
2.2.3	clear line .....	54
2.2.4	connect.....	55
2.2.5	disconnect .....	55
2.2.6	exec-timeout .....	55
2.2.7	length.....	56
2.2.8	line.....	56
2.2.9	location.....	57
2.2.10	login authentication .....	57
2.2.11	monitor.....	57
2.2.12	no debug all .....	58
2.2.13	password .....	58
2.2.14	resume.....	59
2.2.15	show debug .....	59
2.2.16	show line.....	60
2.2.17	terminal length .....	60
2.2.18	terminal monitor .....	61
2.2.19	terminal width .....	61
2.2.20	terminal-type.....	62
2.2.21	where.....	62
2.2.22	width.....	62
Chapter 3 Maintenance and Debugging Tool Commands .....		63
3.1	Network Testing Tool Commands .....	63
3.1.1	ping.....	63
3.1.2	traceroute.....	65
3.2	Fault Diagnosis Commands .....	66
3.2.1	logging .....	67
3.2.2	logging buffered .....	68
3.2.3	logging console .....	69
3.2.4	logging facility.....	70
3.2.5	logging monitor .....	71
3.2.6	logging on .....	72
3.2.7	logging trap.....	74
3.2.8	logging command .....	75
3.2.9	logging source-interface.....	75
3.2.10	logging history alerts .....	76

3.2.11	logging history critical.....	76
3.2.12	logging history debugging .....	77
3.2.13	logging history emergencies.....	77
3.2.14	logging history errors .....	77
3.2.15	logging history informational .....	78
3.2.16	logging history notifications .....	78
3.2.17	logging history warnings.....	79
3.2.18	logging history rate-limit .....	79
3.2.19	logging history size .....	79
3.2.20	service timestamps.....	80
3.2.21	clear logging .....	81
3.2.22	show break .....	81
3.2.23	show debug .....	83
3.2.24	show logging.....	83
Chapter 4 SSH Configuration Commands.....		84
4.1	SSH Configuration Commands.....	84
4.1.1	ip sshd enable.....	84
4.1.2	ip sshd timeout.....	85
4.1.3	ip sshd auth-method .....	85
4.1.4	ip sshd access-class.....	86
4.1.5	ip sshd auth-retries.....	86
4.1.6	ip sshd clear .....	87
4.1.7	ip sshd silence-period .....	87
4.1.8	ip sshd sftp.....	88
4.1.9	ip sshd save.....	89
4.1.10	ip sshd disable-aes.....	89
4.1.11	ssh.....	90
4.1.12	show ssh .....	91
4.1.13	show ip sshd .....	91
Chapter 5 Network Management Configuration .....		92
5.1	SNMP Commands.....	92
5.1.1	snmp-server community .....	92
5.1.2	snmp-server contact.....	94
5.1.3	snmp-server engineID local.....	94
5.1.4	snmp-server group .....	95
5.1.5	snmp-server [host   hostv6] .....	96
5.1.6	snmp-server location.....	98

5.1.7	snmp-server packetsize .....	98
5.1.8	snmp-server queue-length .....	99
5.1.9	snmp-server trap-source .....	100
5.1.10	snmp-server trap-timeout .....	100
5.1.11	snmp-server user .....	101
5.1.12	snmp-server view .....	102
5.1.13	snmp-server source-addr .....	103
5.1.14	snmp-server udp-port .....	104
5.1.15	snmp-server encryption .....	105
5.1.16	snmp-server trap-add-hostname .....	105
5.1.17	snmp-server trap-logs .....	106
5.1.18	snmp-server set-snmp-dos-max .....	107
5.1.19	snmp-server keep-alive .....	107
5.1.20	snmp-server nocode .....	108
5.1.21	snmp-server event-id .....	108
5.1.22	snmp-server getbulk-timeout .....	109
5.1.23	snmp-server getbulk-delay .....	110
5.1.24	show snmp .....	110
5.1.25	debug snmp .....	113
5.2	RMON Configuration Commmands .....	115
5.2.1	rmon alarm .....	116
5.2.2	rmon event .....	116
5.2.3	rmon collection stats .....	117
5.2.4	rmon collection history .....	118
5.2.5	show rmon .....	118
Chapter 6	AAA Configuration Commands .....	119
6.1	Authentication Configuration Commands .....	119
6.1.1	aaa authentication banner .....	120
6.1.2	aaa authentication fail-message .....	120
6.1.3	aaa authentication username-prompt .....	121
6.1.4	aaa authentication password-prompt .....	122
6.1.5	aaa authentication dot1x .....	123
6.1.6	aaa authentication enable default .....	124
6.1.7	aaa authentication login .....	125
6.1.8	aaa group server .....	127
6.1.9	server .....	127
6.1.10	debug aaa authentication .....	129

6.1.11	enable password .....	129
6.1.12	enable(enter).....	130
6.1.13	service password-encryption .....	131
6.2	Authorization Configuration Commands .....	132
6.2.1	aaa authorization.....	132
6.2.2	debug aaa authorization .....	134
6.3	Accounting Configuration Commands .....	135
6.3.1	aaa accounting .....	135
6.3.2	aaa accounting update .....	136
6.3.3	aaa accounting suppress null-username .....	137
6.3.4	debug aaa accounting .....	138
6.4	Local Account Policy Configuration Commands.....	138
6.4.1	localauthen.....	139
6.4.2	localauthor .....	140
6.4.3	localpass .....	141
6.4.4	localgroup.....	142
6.4.5	local authen-group .....	143
6.4.6	local author-group.....	144
6.4.7	local pass-group.....	144
6.4.8	local user .....	145
6.4.9	username.....	146
6.4.10	show local-users .....	148
6.4.11	show aaa users .....	149
Chapter 7	RADIUS Configuration Commands.....	150
7.1	RADIUS Configuration Commands .....	150
7.1.1	debug radius.....	151
7.1.2	ip radius source-interface.....	151
7.1.3	radius-server attribute .....	152
7.1.4	radius-server challenge-noecho .....	153
7.1.5	radius-server deadtime .....	154
7.1.6	radius-server directed-resquest .....	155
7.1.7	radius-server host.....	155
7.1.8	radius-server key .....	156
7.1.9	radius-server optional-passwords.....	157
7.1.10	radius-server retransmit.....	158
7.1.11	radius-server timeout.....	159
7.1.12	radius-server vsa send.....	159

7.1.13	radius-server acct-on.....	160
Chapter 8	TACACS+ Configuration Commands .....	162
8.1	TACACS+ Configuration Commands .....	162
8.1.1	debug tacacs.....	162
8.1.2	ip tacacs source-interface .....	163
8.1.3	tacacs-server host.....	164
8.1.4	tacacs-server key .....	165
8.1.5	tacacs-server timeout.....	165
Chapter 9	HTTP Configuration Commands .....	167
9.1	ip http language.....	167
9.2	ip http port .....	167
9.3	ip http secure-port .....	168
9.4	ip http server .....	168
9.5	ip http http-access enable .....	168
9.6	ip http ssl-access enable.....	169
9.7	ip http web use-footer .....	169
9.8	ip http web max-vlan.....	169
9.9	ip http web max-macaddr-table.....	170
9.10	ip http web igmp-groups .....	171
9.11	ip http web portpanel update-interval .....	171
9.12	ip http web portpanel visible .....	172
9.13	ip http web max-syslogs .....	172
9.14	show ip http.....	173
Chapter 10	Interface Configuration Commands .....	173
10.1	Interface Configuration Commands .....	173
10.1.1	interface .....	173
10.1.2	Description .....	174
10.1.3	bandwidth .....	175
10.1.4	delay .....	175
10.1.5	shutdown.....	176
10.1.6	show interface .....	176
10.1.7	show running-config interface .....	177
10.2	Configuration Example .....	178
Chapter 11	Interface Range Commands .....	180
11.1	Interface Range .....	180
Chapter 12	Port Physical Characteristic Configuration Commands .....	181
12.1	Port Physical Characteristic Configuration Commands.....	181

12.1.1	speed .....	181
12.1.2	duplex .....	181
12.1.3	flow-control .....	182
Chapter 13	Port Additional Characteristics Configuration Commands .....	183
13.1	Configuring Port Isolation (Private VLAN-EDGE) .....	183
13.1.1	port-protected .....	183
13.1.2	Description .....	184
13.1.3	switchport protected .....	184
13.2	Configuring the Storm Control Command .....	185
13.3	Configuring Switchport Rate Limit .....	185
13.4	Configuring Port Loop Check .....	186
13.5	Configuring MAC Address Learning .....	187
13.6	Configuring Port Security .....	187
13.6.1	switchport port-security mode .....	187
13.6.2	switchport port-security dynamic .....	188
13.6.3	switchport port-security static mac-address .....	188
13.6.4	switchport port-security sticky .....	189
13.7	Configuring Port Binding .....	190
13.8	SVL/IVL .....	190
13.9	Configuring Link Scan Commands .....	191
13.10	Configuring the Enhanced Link State Detection Command .....	192
13.11	Configuring System MTU .....	192
Chapter 14	Port Mirroring Configuration Commands .....	193
14.1	Port Mirroring Configuration Commands .....	193
14.1.1	mirror .....	193
14.1.2	show mirror .....	194
Chapter 15	MAC Address Configuration Commands .....	195
15.1	MAC Address Configuration Commands .....	195
15.1.1	mac address-table static .....	195
15.1.2	mac address-table aging-time .....	195
15.1.3	mac address-table blackhole .....	196
15.1.4	show mac address-table .....	196
15.1.5	clear mac address-table .....	197
Chapter 16	MAC Access List Configuration Commands .....	198
16.1	MAC Access List Configuration Commands .....	198
16.1.1	mac access-list .....	198
16.1.2	permit .....	199



16.1.3	deny .....	199
16.1.4	mac access-group .....	200
Chapter 17 802.1x Configuration Commands .....		201
17.1	802.1x Configuration Commands .....	201
17.1.1	dot1x enable .....	202
17.1.2	dot1x port-control .....	203
17.1.3	dot1x authentication multiple-hosts .....	203
17.1.4	dot1x authentication multiple-auth .....	204
17.1.5	dot1x default .....	205
17.1.6	dot1x reauth-max .....	205
17.1.7	dot1x re-authentication .....	206
17.1.8	dot1x timeout quiet-period .....	206
17.1.9	dot1x timeout re-authperiod .....	207
17.1.10	dot1x timeout tx-period .....	208
17.1.11	dot1x mab .....	208
17.1.12	dot1x mabformat .....	209
17.1.13	dot1x user-permit .....	210
17.1.14	dot1x authentication method .....	210
17.1.15	dot1x accounting enable .....	211
17.1.16	dot1x accounting method .....	212
17.1.17	dot1x authen-type, dot1x authentication type .....	213
17.1.18	dot1x guest-vlan .....	214
17.1.19	dot1x guest-vlan id .....	214
17.1.20	dot1x forbid multi-network-adapter .....	215
17.1.21	dot1x keepalive .....	215
17.1.22	aaa authentication dot1x .....	216
17.1.23	debug dot1x errors .....	217
17.1.24	debug dot1x state .....	217
17.1.25	debug dot1x packet .....	218
17.1.26	show dot1x .....	218
Chapter 18 VLAN Configuration Commands .....		220
18.1	VLAN Configuration Commands .....	220
18.1.1	vlan .....	220
18.1.2	name .....	221
18.1.3	dot1q-tunnel .....	221
18.1.4	switchport pvid .....	222
18.1.5	switchport mode .....	222

18.1.6 switchport trunk.....	224
18.1.7 show vlan.....	225
18.1.8 show interface vlan .....	226
Chapter 19 Voice VLAN Configuration Commands .....	228
19.1 lldp.....	228
19.2 voice-vlan mac-address .....	228
19.3 Interface configuration.....	228
Chapter 20 GVRP Configuration Commands.....	229
20.1 GVRP Configuration Commands.....	229
20.1.1 gvrp.....	229
20.1.2 gvrp dynamic-vlan-pruning .....	230
20.1.3 show gvrp statistics .....	230
20.1.4 show gvrp status.....	231
20.1.5 debug gvrp event.....	231
20.1.6 debug gvrp packet .....	232
20.2 GARPC onfiguration Commands.....	232
20.2.1 garp timer leaveall.....	232
20.2.2 garp timer hold.....	233
20.2.3 garp timer join .....	234
20.2.4 garp timer leave .....	234
20.2.5 show garp timers.....	235
20.2.6 show garp status .....	236
20.2.7 debug garp.....	236
Chapter 21 STP Configuration Commands.....	237
21.1 SSTP Configuration Commands .....	237
21.1.1 spanning-tree .....	237
21.1.2 spanning-tree mode sstp.....	237
21.1.3 spanning-tree sstp priority .....	238
21.1.4 spanning-tree sstp hello-time .....	239
21.1.5 spanning-tree sstp max-age .....	239
21.1.6 spanning-tree sstp forward-time .....	240
21.1.7 spanning-tree sstp cost .....	241
21.1.8 spanning-tree cost.....	241
21.1.9 spanning-tree sstp port-priority .....	242
21.1.10 spanning-tree port-priority .....	243
21.1.11 show spanning-tree.....	243
21.1.12 spanning-tree management trap .....	244

21.2 VLAN STP Configuration Commands .....	245
21.2.1 spanning-tree mode pvst .....	245
21.2.2 spanning-tree vlan.....	245
21.2.3 spanning-tree vlan priority .....	246
21.2.4 spanning-tree vlan forward-time .....	247
21.2.5 spanning-tree vlan max-age .....	247
21.2.6 spanning-tree vlan hello-time .....	248
21.2.7 spanning-tree vlan cost .....	249
21.2.8 spanning-tree vlan port-priority.....	250
21.2.9 show spanning-tree vlan .....	250
21.2.10 show spanning-tree pvst instance-list.....	252
Chapter 22 RSTP Configuration Commands.....	252
22.1 RSTP Configuration Commands.....	252
22.1.1 spanning-tree mode rstp.....	252
22.1.2 spanning-tree rstp forward-time.....	253
22.1.3 spanning-tree rstp hello-time .....	253
22.1.4 spanning-tree rstp max-age .....	254
22.1.5 spanning-tree rstp priority .....	254
22.1.6 spanning-tree rstp cost .....	255
22.1.7 spanning-tree rstp port-priority .....	256
22.1.8 spanning-tree rstp edge .....	256
22.1.9 spanning-tree rstp point-to-point .....	257
22.1.10 spanning-tree rstp migration-check.....	257
Chapter 23 MSTP Configuration Commands.....	258
23.1 MSTP Configuration Commands .....	258
23.1.1 spanning-tree mode mstp .....	258
23.1.2 spanning-tree mstp name .....	258
23.1.3 spanning-tree mstp revision.....	259
23.1.4 spanning-tree mstp instance.....	259
23.1.5 spanning-tree mstp root .....	260
23.1.6 spanning-tree mstp priority .....	261
23.1.7 spanning-tree mstp hello-time.....	262
23.1.8 spanning-tree mstp forward-time.....	263
23.1.9 spanning-tree mstp max-age.....	263
23.1.10 spanning-tree mstp diameter.....	264
23.1.11 spanning-tree mstp max-hops .....	265
23.1.12 spanning-tree mstp port-priority .....	265

23.1.13 spanning-tree mstp cost.....	266
23.1.14 spanning-tree mstp edge .....	267
23.1.15 spanning-tree mstp point-to-point .....	267
23.1.16 spanning-tree mstp mst-compatible.....	268
23.1.17 spanning-tree mstp migration-check .....	268
23.1.18 spanning-tree mstp restricted-role .....	269
23.1.19 spanning-tree mstp restricted-tcn .....	269
23.1.20 show spanning-tree mstp.....	270
23.1.21 show spanning-tree mstp region .....	271
23.1.22 show spanning-tree mstp detail.....	272
23.1.23 show spanning-tree mstp interface .....	274
23.1.24 show spanning-tree mstp protocol-migration .....	276
Chapter 24 STP Optional Characteristic Configuration Commands .....	277
24.1 STP Optional Characteristic Configuration Commands.....	277
24.1.1 spanning-tree portfast .....	277
24.1.2 spanning-tree bpduguard.....	278
24.1.3 spanning-tree bpdufilter .....	278
24.1.4 spanning-tree uplinkfast.....	279
24.1.5 spanning-tree backbonefast.....	280
24.1.6 spanning-tree guard .....	280
24.1.7 spanning-tree loopguard.....	281
24.1.8 spanning-tree loopfast .....	282
24.1.9 spanning-tree fast-aging .....	282
24.1.10 spanning-tree fast-aging flush-fdb .....	283
24.1.11 spanning-tree bpdu-terminal .....	284
Chapter 25 Port Aggregation Commands .....	285
25.1 Port Aggregation Commands .....	285
25.1.1 aggregator-group .....	285
25.1.2 aggregator-group load-balance.....	286
25.1.3 show aggregator-group.....	287
25.1.4 show interface port-aggregator .....	287
25.1.5 debug lacp errors.....	288
25.1.6 debug lacp state .....	289
25.1.7 debug lacp packet.....	289
Chapter 26 PDP Configuration Commands .....	290
26.1 PDP Configuration Cmmands .....	290
26.1.1 pdp timer .....	290

26.1.2 pdp holdtime .....	291
26.1.3 pdp version .....	291
26.1.4 pdp run .....	292
26.1.5 pdp enable .....	292
26.1.6 show pdp traffic .....	293
26.1.7 show pdp neighbor .....	293
Chapter 27 LLDP Configuration Commands .....	294
27.1 LLDP Commands .....	294
27.1.1 lldp run .....	294
27.1.2 lldp holdtime .....	294
27.1.3 lldp timer .....	295
27.1.4 lldp reinit .....	296
27.1.5 lldp tlv-select .....	296
27.1.6 lldp dot1-tlv-select .....	297
27.1.7 lldp dot3-tlv-select .....	298
27.1.8 lldp med-tlv-select .....	299
27.1.9 lldp transmit .....	299
27.1.10 lldp receive .....	300
27.1.11 lldp management-ip .....	301
27.1.12 lldp trap-send .....	301
27.1.13 location elin identifier id WORD .....	302
27.1.14 location civic identifier id .....	303
27.1.15 location elin/civic id .....	304
27.1.16 show lldp errors .....	305
27.1.17 show lldp interface .....	306
27.1.18 show lldp neighbors .....	306
27.1.19 show lldp neighbors detail .....	307
27.1.20 show lldp traffic .....	309
27.1.21 show location elin .....	309
27.1.22 show location civic [identifier id] .....	310
27.1.23 clear lldp counters .....	311
27.1.24 clear lldp table .....	312
Chapter 28 Backuplink Configuration Commands .....	313
28.1 Global Commands .....	313
28.1.1 backup-link-group id .....	313
28.1.2 backup-link-group id preemption-mode forced {delay value} .....	313
28.1.3 backup-link-group id preemption-mode bandwidth {delay value} .....	314

28.1.4 monitor-link-group id .....	315
28.2 Port Configuration Commands.....	316
28.2.1 backup-link-group id active .....	316
28.2.2 backup-link-group id backup .....	316
28.2.3 share-load vlan vlanmap .....	317
28.2.4 backup-link-group mmu transmit .....	318
28.2.5 backup-link-group mmu receive.....	319
28.2.6 monitor-link-group id uplink .....	319
28.2.7 monitor-link-group id downlink .....	320
28.3 Show .....	321
28.3.1 show backup-link-group id .....	321
28.3.2 show monitor-link-group id.....	322
Chapter 29 EAPS Configuration Commands.....	323
29.1 Global Commands .....	323
29.1.1 ether-ring.....	323
29.1.2 control-vlan .....	323
29.1.3 master-node .....	324
29.1.4 transit-node.....	325
29.1.5 hello-time .....	325
29.1.6 fail-time .....	326
29.1.7 pre-forward-time.....	327
29.2 Port Configuration Commands.....	328
29.2.1 ether-ring primary-port.....	328
29.2.2 ether-ring secondary-port.....	329
29.2.3 ether-ring transit-port.....	329
29.3 Show.....	330
29.3.1 show ether-ring.....	330
Chapter 30 MEAPS Configuration Commands .....	332
30.1 Global Commands .....	332
30.1.1 mether-ring id1 domain id2 .....	332
30.1.2 master-node.....	332
30.1.3 transit-node.....	333
30.1.4 edge-node .....	334
30.1.5 assistant-node .....	335
30.1.6 major-ring.....	335
30.1.7 sub-ring.....	336
30.1.8 control-vlan .....	337

30.1.9	single-subring-mode.....	338
30.1.10	hello-time .....	339
30.1.11	fail-time .....	340
30.1.12	pre-forward-time.....	341
30.2	Port Configuration Commands.....	341
30.2.1	mether-ring id1 domain id2 primary-port.....	341
30.2.2	mether-ring id1 domain id2 secondary-port.....	342
30.2.3	mether-ring id1 domain id2 transit-port.....	343
30.2.4	mether-ring id1 domain id2 common-port.....	344
30.2.5	mether-ring id1 domain id2 edge-port .....	345
30.3	Show .....	346
30.3.1	show mether-ring.....	346
Chapter 31	UDLD Configuration Commands.....	347
31.1	UDLD Configuration Commands.....	347
31.1.1	udld enable.....	347
31.1.2	udld aggressive.....	348
31.1.3	udld port.....	348
31.1.4	udld port aggressive .....	349
31.1.5	udld message.....	350
31.1.6	udld reset.....	350
31.1.7	show udld .....	351
Chapter 32	IGMP-Snooping Configuration Commands.....	353
32.1.1	igmp-snooping.....	354
32.1.2	igmp-snooping static .....	354
32.1.3	igmp-snooping immediate-leave.....	355
32.1.4	igmp-snooping mrouter .....	356
32.1.5	igmp-snooping policy .....	356
32.1.6	igmp-snooping dlf-drop.....	357
32.1.7	igmp-snooping router age.....	357
32.1.8	igmp-snooping response time.....	358
32.1.9	igmp-snooping querier .....	358
32.1.10	igmp-snooping querier querier-timer .....	359
32.1.11	igmp-snooping forward-l3-to-mrouter .....	360
32.1.12	igmp-snooping sensitive.....	360
32.1.13	igmp-snooping v3-leave-check.....	361
32.1.14	igmp-snooping forward-wrongiif-within-vlan.....	361
32.1.15	igmp-snooping policy .....	362

32.1.16	igmp-snooping limit.....	362
32.1.17	show ip igmp-snooping .....	363
32.1.18	show ip igmp-snooping timer.....	364
32.1.19	show ip igmp-snooping groups .....	365
32.1.20	show ip igmp-snooping statistics .....	365
32.1.21	debug ip igmp-snooping packet .....	366
32.1.22	debug ip igmp-snooping timer .....	366
32.1.23	debug ip igmp-snooping event.....	367
32.1.24	debug ip igmp-snooping error.....	367
Chapter 33 OAM Configuration Commands .....		368
33.1	OAM Configuration Commands OAM configuration commands include: .....	368
33.1.1	ethernet oam.....	368
33.1.2	ethernet oam {max-rate   min-rate   mode   timeout } .....	369
33.1.3	ethernet oam remote-failure {critical-event   dying-gasp   link-fault} action .....	370
33.1.4	ethernet oam link-monitor {symbol-period   frame   frame-period   frame-seconds   receive-crc} threshold high.....	371
33.1.5	ethernet oam link-monitor {symbol-period   frame   frame-period   frame-seconds   receive-crc} threshold low.....	372
33.1.6	ethernet oam link-monitor {symbol-period   frame   frame-period   frame-seconds   receive-crc} window .....	373
33.1.7	ethernet oam link-monitor high-threshold action .....	373
33.1.8	ethernet oam link-monitor negotiation-supported .....	374
33.1.9	clear ethernet oam statistics.....	375
33.1.10	show ethernet oam discovery.....	375
33.1.11	show ethernet oam statistics {pdu   link-monitor   remote-failure} .....	377
33.1.12	show ethernet oam configuration .....	378
33.1.13	show ethernet oam runtime .....	380
Chapter 34 Overview.....		381
34.1	Stipulation .....	381
34.2	Format Stipulation in the Command Line .....	381
Chapter 35 CFM.....		382
35.1	CFM Configuration Commands .....	382
35.1.1	Adding the Maintenance Domain and Entering the Maintenance Domain Mode .....	382
35.1.2	Deleting the Maintenance Domain .....	383
35.1.3	Browsing the Maintenance Domain.....	383
35.1.4	Adding a maintenance association.....	384
35.1.5	Deleting the Maintenance Association .....	384
35.1.6	Browsing the Maintenance Association .....	385



35.1.7	Adding MIP .....	386
35.1.8	Deleting MIP .....	386
35.1.9	Browsing MIP.....	386
35.1.10	Adding MEP .....	387
35.1.11	Deleting MEP .....	388
35.1.12	Browsing MEP.....	389
35.3	CFM Maintenance Commands .....	390
35.2.1	loopback .....	390
35.2.2	linktrace.....	391
35.2.3	Deleting the Linktrace Result Table.....	392
35.2.4	Setting the Size of the Linktrace Result Table .....	393
35.2.5	Setting the Number of Entries in the Linktrace Result Table .....	393
35.2.6	Setting the aging time of the linktrace result table.....	393
35.2.7	Deleting the MEP Statistics Data .....	394
35.4	CFM Control Commands .....	395
35.4.1	CFM Stack Control Command.....	395
35.4.2	CFM Interface Control Command.....	395
35.4.3	MIP Control Command .....	395
35.4	CFM Query Commands .....	396
35.4.1	Browsing the CFM Protocol Stack .....	396
35.4.2	Browsing the CFM Interface.....	396
35.4.3	Browsing the Locally Stored Information about the Remote MEP .....	397
35.4.4	Browsing the LinkTrace Result Table.....	397
35.4.5	Browsing the whole running status of CFM .....	399
Chapter 36	DHCP-relay Snooping Configuration Commands .....	399
36.1.1	ip dhcp-relay snooping .....	400
36.1.2	ip dhcp-relay snooping vlan .....	400
36.1.3	ip dhcp-relay snooping vlan vlan_id max-client.....	401
36.1.4	ip dhcp-relay snooping database-agent.....	401
36.1.5	ip dhcp-relay snooping db-file.....	402
36.1.6	ip dhcp-relay snooping write-time .....	402
36.1.7	ip dhcp-relay snooping write-immediately .....	403
36.1.8	ip dhcp-relay snooping log .....	403
36.1.9	ip dhcp-relay snooping rapid-refresh-bind.....	404
36.1.10	dhcp-relay snooping information option .....	404
36.1.11	ip verify source vlan.....	405
36.1.12	ip arp inspection vlan .....	406

36.1.13 ip source binding .....	407
36.1.14 arp inspection trust .....	407
36.1.15 dhcp snooping trust.....	408
36.1.16 dhcp snooping deny .....	408
36.1.17 dhcp snooping information circuit-id.....	409
36.1.18 dhcp snooping information remote-id string.....	409
36.1.19 dhcp snooping information vendor-specific .....	410
36.1.20 dhcp snooping information append.....	411
36.1.21 dhcp snooping information drop .....	412
36.1.22 ip-source trust .....	412
36.1.23 show ip dhcp-relay snooping.....	413
36.1.24 show ip dhcp-relay snooping binding.....	413
36.1.25 debug ip dhcp-relay snooping.....	414
36.1.26 debug ip dhcp-relay event.....	414
36.1.27 debug ip dhcp-relay binding.....	414
Chapter 37 MACFF Configuration Commands .....	415
37.1 macff enable.....	415
37.2 macff vlan vlan_id enable.....	416
37.3 macff vlan vlan_id default-ar A.B.C.D .....	416
37.4 macff vlan vlan_id other_ar A.B.C.D .....	417
37.5 macff disable .....	418
37.6 debug macff.....	418
Chapter 38 L2 Channel Configuration Commands .....	419
38.1 L2 Channel Configuration Commands.....	419
38.1.1 L2 protocol-tunnel.....	419
38.1.2 no spanning-tree .....	419
Chapter 39 Loopback Detection Configuration Commands.....	420
39.1 loopback-detection Syntax.....	420
39.2 loopback-detection enable Syntax.....	421
39.3 loopback-detection vlan-control Syntax .....	421
39.4 loopback-detection hello-time Syntax .....	422
39.5 loopback-detection recovery-time Syntax .....	422
39.6 loopback-detection control Syntax .....	423
39.7 loopback-detection dest-mac Syntax.....	424
39.8 loopback-detection existence Syntax.....	424
39.9 loopback-detection frames-threshold Syntax.....	425
39.10 loopback-detection frames-monitor Syntax .....	425

39.11	show loopback-detection Syntax .....	426
39.12	show loopback-detection Syntax .....	427
Chapter 40	QoS Configuration Commands .....	428
40.1	QoS Configuration Commands .....	428
40.1.1	cos default .....	428
40.1.2	cos map .....	429
40.1.3	dscp map .....	430
40.1.4	scheduler weight bandwidth.....	430
40.1.5	scheduler policy.....	431
40.1.6	policy-map .....	432
40.1.7	classify .....	432
40.1.8	action.....	434
40.1.9	qos policy.....	435
40.1.10	show policy-map .....	436
40.1.11	trust .....	436
Chapter 41	DoS-Attack Prevention Configuration Commands .....	437
41.1.	DoS-Attack Prevention Configuration Commands .....	437
41.1.1.	dos enable .....	437
41.1.2.	show dos.....	438
Chapter 42	Anti-Attack Configuration Commands.....	439
42.1	Anti-Attack Configuration Commands .....	439
42.1.1	filter period.....	439
42.1.2	filter threshold.....	440
42.1.3	filter block-time .....	441
42.1.4	filter polling period.....	441
42.1.5	filter polling threshold.....	442
42.1.6	filter polling auto-fit .....	442
42.1.7	filter igmp .....	443
42.1.8	filter ip source-ip .....	443
42.1.9	filter icmp .....	444
42.1.10	filter dhcp .....	444
42.1.11	filter arp.....	445
42.1.12	filter bpdu.....	445
42.1.13	filter mode.....	446
42.1.14	filter enable .....	446
42.1.15	show filter.....	447
Chapter 43	IP Address Configuration Commands.....	448

43.1	IP Address Configuration Commands.....	448
43.1.1	arp.....	448
43.1.2	arp max-gw-retries.....	449
43.1.3	arp retry-allarp.....	450
43.1.4	arp timeout.....	450
43.1.5	arp send-gratuitous.....	451
43.1.6	clear arp-cache.....	452
43.1.7	ip address.....	452
43.1.8	ip host.....	453
43.1.9	show arp.....	454
43.1.10	show hosts.....	455
43.1.11	show ip interface.....	455
	Chapter 44 DHCP Client Configuration Commands.....	457
44.1	DHCP Client Configuration Commands.....	457
44.1.1	ip address dhcp.....	457
44.1.2	ip dhcp client.....	458
44.1.3	ip dhcp-server.....	460
44.1.4	show dhcp lease.....	461
44.1.5	show dhcp server.....	462
44.1.6	debug dhcp.....	462
	Chapter 45 IPv6 Configuration Commands.....	463
45.1	IP Service Configuration Commands.....	463
45.1.1	clear tcp.....	464
45.1.2	clear tcp statistics.....	465
45.1.3	debug arp.....	466
45.1.4	debug ip icmp.....	467
45.1.5	debug ip packet.....	470
45.1.6	debug ip raw.....	475
45.1.7	debug ip tcp packet.....	476
45.1.8	debug ip tcp transactions.....	478
45.1.9	debug ip udp.....	480
45.1.10	ip mask-reply.....	481
45.1.11	ip mtu.....	481
45.1.12	ip source-route.....	482
45.1.13	ip tcp synwait-time.....	483
45.1.14	ip tcp window-size.....	483
45.1.15	ip unreachable.....	484

45.1.16 show ip sockets .....	485
45.1.17 show ip traffic.....	486
45.1.18 show tcp .....	487
45.1.19 show tcp brief.....	492
45.1.20 show tcp statistics .....	492
45.1.21 show tcp tcb .....	495
45.2 ACL Configuration Commands.....	496
45.2.1 deny.....	496
45.2.2 ip access-group.....	499
45.2.3 ip access-list.....	500
45.2.4 permit.....	501
45.2.5 show ip access-list .....	503
45.3 IP ACL based on physical port .....	504
45.3.1 deny.....	505
45.3.2 ip access-group.....	507
45.3.3 ip access-list.....	508
45.3.4 permit.....	508
45.3.5 show ip access-list .....	511
Chapter 46 IP ACL Application Configuration Commands .....	512
46.1 IP ACL Application Configuration Commands .....	512
46.1.1 ip access-group.....	512
46.1.2 ipv6 access-group .....	513
Chapter 47 IPv6 Configuration Commands.....	515
47.1 IPv6 Configuration Commands.....	515
47.1.1 ipv6 address.....	515
47.1.2 ipv6 address anycast .....	516
47.1.3 ipv6 address autoconfig .....	517
47.1.4 ipv6 address eui-64 .....	517
47.1.5 ipv6 address link-local .....	518
47.1.6 ipv6 enable .....	519
47.1.7 show ipv6 interface .....	520
Chapter 48 IPv6 Configuration Commands.....	521
48.1 IPv6 Configuration Commands.....	521
48.1.1 clear ipv6 traffic.....	521
48.1.2 debug ipv6 packet .....	523
48.1.3 ipv6 mtu.....	524
48.1.4 ipv6 redirects.....	525

48.1.5	ipv6 access-group .....	525
48.1.6	ipv6 unreachable .....	526
48.1.7	ipv6 route default.....	527
48.1.8	show ipv6 general-prefix.....	527
48.1.9	show ipv6 pmtu.....	528
48.1.10	show ipv6 traffic.....	529
48.2	Network Testing Tool Commands .....	530
48.2.1	ping6.....	530
48.2.2	traceroute6.....	532
Chapter 49 MLD Multicast Configuration Commands .....		534
49.1	ipv6 mld-snooping.....	534
49.2	ipv6 mld-snooping solicitation .....	535
49.3	ipv6 mld-snooping vlan vlan_id static X:X:X:X:X interface intf_name .....	535
49.4	ipv6 mld-snooping timer router-age timer_value.....	536
49.5	ipv6 mld-snooping timer response-time timer_value .....	536
49.6	ipv6 mld-snooping querier .....	537
49.7	ipv6 mld-snooping vlan vlan_id mrouter interface intf_name .....	537
49.8	ipv6 mld-snooping vlan vlan_id immediate-leave .....	538
49.9	show ipv6 mld-snooping .....	538
49.10	show ipv6 mld-snooping vlan vlan_id .....	540
49.11	show ipv6 mld-snooping timer.....	540
49.12	show ipv6 mld-snooping groups .....	541
49.13	show ipv6 mld-snooping statistics .....	542
49.14	show ipv6 mld-snooping mac.....	542
Chapter 50 Neighbor Detection Configuration Commands .....		544
50.1.1	debug ipv6 nd .....	544
50.1.2	show ipv6 neighbors.....	544
50.1.3	clear ipv6 neighbors .....	545
50.1.4	ipv6 neighbor.....	545
Chapter 51 NTP Configuration Commands .....		546
51.1	ntp master .....	546
51.2	ntp authentication enable.....	547
51.3	ntp authentication key .....	548
51.4	ntp authentication trusted-key .....	548
51.5	ntp server .....	549
51.6	ntp peer .....	550
51.7	show ntp.....	551

51.8	debug ntp .....	553
51.9	time-zone .....	553
Chapter 52 Power Over Ethernet Configuration Commands.....		554
Affects only for Pixietech POE-switches.....		554
52.1	POE Configuration Commands .....	554
52.1.1	show poe system .....	554
52.1.2	show poe all.....	555
52.1.3	show poe power .....	557
52.1.4	show poe interface.....	558
52.1.5	poe power-management.....	560
52.1.6	poe led-time .....	561
52.1.7	poe mib notification-stop.....	562
52.1.8	poe pse-unprotect.....	562
52.1.9	poe counter value.....	563
52.1.10	poe threshold .....	563
52.1.11	poe standard .....	564
52.1.12	poe disable .....	565
52.1.13	poe max-power .....	566
52.1.14	poe priority.....	566
52.1.15	poe PD-description.....	567
52.1.16	poe force-power.....	567
52.1.17	poe extern-power.....	568
Chapter 53 RIP Configuration Commands.....		569
53.1	RIP Configuration Commands .....	569
53.1.1	auto-summary .....	570
53.1.2	default-information originate .....	570
53.1.3	default-metric.....	571
53.1.4	ip rip authentication.....	572
53.1.5	ip rip message-digest-key.....	573
53.1.6	ip rip passive .....	573
53.1.7	ip rip password .....	574
53.1.8	ip rip receive version .....	575
53.1.9	ip rip send version .....	576
53.1.10	ip rip split-horizon .....	576
53.1.11	neighbor .....	578
53.1.12	network .....	578
53.1.13	offset .....	579

53.1.14 router rip .....	580
53.1.15 timers expire .....	581
53.1.16 timers holddown .....	581
53.1.17 timers update .....	582
53.1.18 validate-update-source .....	583
53.1.19 version .....	584
53.1.20 distance .....	585
53.1.21 filter .....	585
53.1.22 maximum-count .....	587
53.1.23 show ip rip .....	587
53.1.24 show ip rip database .....	588
53.1.25 show ip rip protocol .....	589
53.1.26 debug ip rip database.....	590
53.1.27 debug ip rip protocol.....	591
Chapter 54 BEIGRP Configuration Commands affects ONLY PXT-S2790G/2795G or higher .....	592
54.1 BEIGRP Configuration Commands.....	592
54.1.1 auto-summary .....	593
54.1.2 clear ip beigrp neighbors.....	594
54.1.3 debug ip beigrp.....	595
54.1.4 debug ip beigrp fsm.....	595
54.1.5 debug ip beigrp neighbors.....	596
54.1.6 debug ip beigrp packet.....	596
54.1.7 debug ip beigrp transmit .....	598
54.1.8 default-metric.....	599
54.1.9 distance .....	600
54.1.10 filter .....	601
54.1.11 beigrp log-neighbor-changes.....	602
54.1.12 beigrp router-id .....	602
54.1.13 ip beigrp bandwidth-percent .....	603
54.1.14 ip beigrp hello-interval .....	603
54.1.15 ip beigrp hold-time .....	604
54.1.16 ip beigrp passive .....	605
54.1.17 ip beigrp split-horizon .....	605
54.1.18 ip beigrp summary-address.....	606
54.1.19 metric weights .....	607
54.1.20 network .....	608
54.1.21 offset .....	609



54.1.22 redistribute.....	610
54.1.23 router beigrp .....	611
54.1.24 show ip beigrp interface.....	611
54.1.25 show ip beigrp neighbors .....	612
54.1.26 show ip beigrp protocol .....	613
54.1.27 show ip beigrp topology.....	614
54.1.28 show ip beigrp traffic.....	616
Chapter 55 OSPF Configuration Commands .....	617
55.1 OSPF Configuration Commands .....	617
55.1.1 area authentication .....	618
55.1.2 area default-cost .....	619
55.1.3 area range.....	620
55.1.4 area stub.....	622
55.1.5 area virtual-link.....	623
55.1.6 debug ip ospf adj .....	625
55.1.7 debug ip ospf events .....	626
55.1.8 debug ip ospf flood.....	627
55.1.9 debug ip ospf lsa-generation.....	628
55.1.10 debug ip ospf packet .....	629
55.1.11 debug ip ospf retransmission .....	630
55.1.12 debug ip ospf spf .....	630
55.1.13 debug ip ospf tree .....	632
55.1.14 default-information originate (OSPF).....	633
55.1.15 default-metric.....	634
55.1.16 distance ospf .....	635
55.1.17 filter .....	636
55.1.18 ip ospf cost .....	637
55.1.19 ip ospf dead-interval .....	638
55.1.20 ip ospf hello-interval.....	638
55.1.21 ip ospf message-digest-key .....	639
55.1.22 ip ospf network.....	640
55.1.23 ip ospf passive .....	641
55.1.24 ip ospf password.....	642
55.1.28 ip ospf priority .....	643
55.1.29 ip ospf retransmit-interval .....	643
55.1.30 neighbor .....	644
55.1.31 network area .....	646

55.1.32 redistribute.....	646
55.1.33 router ospf.....	647
55.1.34 show ip ospf .....	648
55.1.35 show ip ospf border-routers .....	649
55.1.36 show ip ospf database.....	650
55.1.37 show ip ospf interface .....	652
55.1.38 show ip ospf neighbor .....	653
55.1.39 show ip ospf virtual-link .....	654
55.1.40 summary-address.....	656
55.1.41 timers delay.....	657
55.1.42 timers hold .....	657
Chapter 56 BGP Configuration Commands affects ONLY PXT-S2790G/2795G or Higher.....	658
56.1.43 aggregate-address.....	659
56.1.44 bgp always-compare-med .....	661
56.1.45 bgp bestpath med .....	662
56.1.46 bgp client-to-client reflection.....	663
56.1.47 bgp cluster-id.....	663
56.1.48 bgp confederation identifier .....	664
56.1.49 bgp confederation peers .....	665
56.1.50 bgp dampening.....	666
56.1.51 bgp default .....	668
56.1.52 bgp deterministic-med .....	669
56.1.53 bgp redistribute-internal .....	669
56.1.54 clear ip bgp .....	670
56.1.55 debug chat.....	671
56.1.56 debug dialer.....	672
56.1.57 debug ip bgp.....	673
56.1.58 distance .....	675
56.1.59 filter .....	676
56.1.60 neighbor default-originate .....	677
56.1.61 neighbor description .....	678
56.1.62 neighbor distribute-list.....	678
56.1.63 neighbor ebgp-multihop .....	680
56.1.64 neighbor filter-list.....	680
56.1.65 neighbor maximum-prefix.....	682
56.1.66 neighbor next-hop-self.....	683
56.1.67 neighbor password.....	684

56.1.68 neighbor prefix-list .....	685
56.1.69 neighbor remote-as.....	686
56.1.70 neighbor route-map .....	687
56.1.71 neighbor route-reflector-client .....	688
56.1.72 neighbor route-refresh.....	689
56.1.73 neighbor send-community .....	690
56.1.74 neighbor shutdown .....	691
56.1.75 neighbor soft-reconfiguration .....	692
56.1.76 neighbor timers .....	693
56.1.77 neighbor update-source .....	694
56.1.78 neighbor weight .....	695
56.1.79 network (BGP) .....	696
56.1.80 redistribute(BGP).....	697
56.1.81 router bgp.....	698
56.1.82 show ip bgp .....	699
56.1.83 show ip bgp community .....	701
56.1.84 show ip bgp neighbors .....	701
56.1.85 show ip bgp paths .....	702
56.1.86 show ip bgp prefix-list .....	703
56.1.87 show ip bgp regexp .....	703
56.1.88 show ip bgp summary .....	704
56.1.89 synchronization .....	705
56.1.90 table-map .....	706
56.1.91 timers .....	706
Chapter 57 Ripng Commands.....	707
57.1 aggregate-address.....	707
57.2 debug ipv6 rip.....	708
57.3 default-information.....	709
57.4 default-metric.....	709
57.5 connect-metric .....	710
57.6 distance .....	711
57.7 filter .....	711
57.8 ipv6 rip enable.....	712
57.9 ipv6 rip passive .....	713
57.10 ipv6 rip poison-reverse.....	713
57.11 ipv6 rip split-horizon.....	714
57.12 router ripng .....	715

57.13	max-path .....	715
57.14	neighbor .....	716
57.15	offset.....	717
57.16	port.....	718
57.17	redistribute.....	718
57.18	show ipv6 rip .....	719
57.19	timers.....	720
Chapter 58 OSPFv3 Configuration Commands affects ONLY PXT-S2790G/2795G or Higher .....		721
58.1	OSPFv3 Configuration Commands .....	721
58.1.1	area default-cost .....	722
58.1.2	area nssa.....	723
58.1.3	area range.....	724
58.1.4	area stub.....	725
58.1.5	area virtual-link.....	726
58.1.6	debug ipv6 ospf .....	728
58.1.7	debug ipv6 ospf events.....	730
58.1.8	debug ipv6 ospf ifsm .....	732
58.1.9	debug ipv6 ospf lsa .....	734
58.1.10	debug ipv6 ospf nfsm .....	737
58.1.11	debug ipv6 ospf nsm .....	739
58.1.12	debug ipv6 ospf packet .....	740
58.1.13	debug ipv6 ospf route .....	743
58.1.14	default-information originate .....	745
58.1.15	default-metric.....	746
58.1.16	filter .....	746
58.1.17	ipv6 ospf area .....	747
58.1.18	ipv6 ospf cost.....	748
58.1.19	ipv6 ospf database-filter all out .....	749
58.1.20	ipv6 ospf dead-interval.....	749
58.1.21	ipv6 ospf hello-interval.....	750
58.1.22	ipv6 ospf mtu-ignore .....	751
58.1.23	ipv6 ospf neighbor.....	752
58.1.24	ipv6 ospf network.....	753
58.1.25	ipv6 ospf priority .....	754
58.1.26	ipv6 ospf retransmit-interval.....	754
58.1.27	ipv6 ospf transmit-delay.....	755
58.1.28	passive-interface .....	756

58.1.29 redistribute.....	757
58.1.30 router ospfv3.....	757
58.1.31 router-id .....	758
58.1.32 show ipv6 ospf.....	759
58.1.33 show ipv6 ospf database .....	760
58.1.34 show ipv6 ospf interface .....	762
58.1.35 show ipv6 ospf neighbor .....	763
58.1.36 show ipv6 ospf route.....	764
58.1.37 show ipv6 ospf virtual-link .....	766
58.1.38 summary-prefix .....	767
58.1.39 timers delay.....	768
58.1.40 timers hold .....	768
Chapter 59 BFD Configuration Commands affects ONLY PXT-S2790G/2795G or Higher .....	769
59.1.1 bfd init-mode.....	769
59.1.2 bfd slow-timers.....	770
59.1.3 bfd demand enable .....	771
59.1.4 bfd echo enable.....	772
59.1.5 bfd enable.....	772
59.1.6 bfd neighbor .....	773
59.1.7 bfd min_echo_rx_interval.....	774
59.1.8 bfd authentication-mode .....	775
59.1.9 show bfd.....	776
Chapter 60 IP Hardware Subnet Routing Configuration Commands .....	777
60.1 ip exf.....	777
60.2 ip exf down-up-threshold.....	777
60.3 debug ip exf.....	778
Chapter 61 IP-PBR Configuration Commands affects ONLY PXT-S2790G/2795G or Higher .....	779
61.1.1 ip pbr .....	779
61.1.2 show ip pbr.....	779
61.1.3 show ip pbr policy.....	780
61.1.4 show ip pbr exf .....	781
61.1.5 debug ip pbr .....	781
Chapter 62 VRRP Configuration Commands affects ONLY PXT-S2790G/2795G or Higher .....	782
62.1 VRRP Configuration Commands .....	782
62.1.1 vrrp associate .....	782
62.1.2 vrrp description .....	783
62.1.3 vrrp priority .....	783

62.1.4	vrrp preempt .....	784
62.1.5	vrrp track .....	785
62.1.6	vrrp authentication.....	785
62.1.7	vrrp timers .....	786
62.1.8	show vrrp.....	787
62.1.9	debug vrrp .....	788
Chapter 63 Basic Multicast Commands affects ONLY PXT-S2790G/2795G or Higher .....		788
63.1	Basic Multicast Commands .....	788
63.1.1	debug ip mpacket .....	788
63.1.2	debug ip mrouting.....	789
63.1.3	debug ip mroute-cache .....	790
63.1.4	debug ip multicast .....	791
63.1.5	ip mroute .....	792
63.1.6	ip mroute-cache .....	792
63.1.7	ip multicast-routing.....	793
63.1.8	ip multicast route-limit.....	794
63.1.9	ip multicast boundary.....	794
63.1.10	ip multicast helper-map .....	795
63.1.11	ip multicast rate-limit .....	797
63.1.12	ip multicast ttl-threshold.....	798
63.1.13	show ip mflow .....	799
63.1.14	show ip mroute-cache.....	800
63.1.15	show ip mroute mfc .....	801
Chapter 64 IGMP Configuration Commands.....		802
64.1	IGMP Configuration Commands.....	802
64.1.1	clear ip igmp group.....	802
64.1.2	debug ip igmp .....	802
64.1.3	debug ip igmp-host.....	803
64.1.4	ip igmp helper-address.....	803
64.1.5	ip igmp join-group .....	804
64.1.6	ip igmp immediate-leave group-list .....	805
64.1.7	ip igmp last-member-query-interval .....	806
64.1.8	ip igmp querier-timeout .....	806
64.1.9	ip igmp query-interval .....	807
64.1.10	ip igmp query-max-response-time .....	808
64.1.11	ip igmp static-group .....	808
64.1.12	ip igmp version .....	809

64.1.13 show ip igmp groups .....	810
64.1.14 show ip igmp interface .....	812
64.1.15 show ip igmp-host .....	813
Chapter 65 PIM-DM Configuration Commands .....	814
65.1 PIM-DM Configuration Commands .....	814
65.1.1 clear ip mroute pim-dm.....	814
65.1.2 clear ip pim-dm interface .....	815
65.1.3 debug ip pim-dm .....	815
65.1.4 ip pim-dm .....	818
65.1.5 ip pim-dm dr-priority.....	818
65.1.6 ip pim-dm hello-interval.....	819
65.1.7 ip pim-dm state-refresh origination-interval .....	820
65.1.8 ip pim-dm neighbor-filter .....	821
65.1.9 ip pim-dm state-refresh disable .....	821
65.1.10 show ip mroute pim-dm.....	822
65.1.11 show ip pim-dm neighbor .....	823
65.1.12 show ip pim-dm interface .....	825
65.1.13 show ip rpf pim-dm .....	826
Chapter 66 PIM-SM Configuration Commands.....	827
66.1 PIM-SM Configuration Commands.....	827
66.1.1 ip pim-sm.....	827
66.1.2 ip pim-sm admin-scope .....	827
66.1.3 ip pim-sm asrt-hold .....	828
66.1.4 ip pim-sm bsr-border.....	829
66.1.5 ip pim-sm dr-pri.....	829
66.1.6 ip pim-sm hello-intvl.....	830
66.1.7 ip pim-sm holdtime .....	830
66.1.8 ip pim-sm horizon-split.....	831
66.1.9 ip pim-sm jp-hold .....	832
66.1.10 ip pim-sm jp-intvl.....	833
66.1.11 ip pim-sm lan-delay .....	833
66.1.12 ip pim-sm nbma-mode .....	834
66.1.13 ip pim-sm nbr-filter .....	835
66.1.14 ip pim-sm nbr-track.....	836
66.1.15 ip pim-sm override .....	837
66.1.16 router pim-sm.....	838
66.1.17 hello-option.....	838

66.1.18 accept bsm-adv .....	840
66.1.19 accept crp-adv .....	840
66.1.20 accept rp-addr .....	841
66.1.21 accept register .....	843
66.1.22 anycast-rp .....	844
66.1.23 reg-rate-limit .....	847
66.1.24 reg-src .....	847
66.1.25 spt-threshold .....	848
66.1.26 ssm .....	849
66.1.27 c-bsr intf_type intf_name .....	851
66.1.28 c-bsr admin-scope .....	852
66.1.29 bsm-policy .....	853
66.1.30 static-rp .....	854
66.1.31 c-rp intf_type intf_name .....	855
66.1.32 intvl-time .....	857
66.1.33 holdtime .....	858
66.1.34 log .....	860
66.1.35 show running-configure .....	860
66.1.36 show ip pim-sm bsr-router .....	861
66.1.37 show ip pim-sm interface .....	862
66.1.38 show ip pim-sm neighbor .....	862
66.1.39 show ip pim-sm rp .....	863
66.1.40 show ip pim-sm rp-hash .....	864
66.1.41 show ip mroute pim-sm .....	864
66.1.42 show ip rpf pim-sm .....	866
66.1.43 debug ip pim-sm alert .....	866
66.1.44 debug ip pim-sm assert .....	867
66.1.45 debug ip pim-sm bsr .....	868
66.1.46 debug ip pim-sm rp .....	868
66.1.47 debug ip pim-sm entry .....	869
66.1.49 debug ip pim-sm hello .....	870
66.1.50 debug ip pim-sm jp .....	870
66.1.51 debug ip pim-sm nbr .....	871
66.1.52 debug ip pim-sm packet .....	871
66.1.53 debug ip pim-sm register .....	872
66.1.54 debug ip pim-sm timer .....	872
Chapter 67 Multicast VPN Settings .....	873



67.1.1	ip multicast-routing vrf vpn-instance-name.....	873
67.1.2	mdt share-group group-address binding mtunnel number .....	873
67.1.3	mdt connect-src interface .....	874
67.1.4	mdt switch-group-pool group-address group-mask threshold.....	875
67.1.5	mdt mdt switch-delay.....	875
67.1.6	mdt hold-down.....	876
67.1.7	mdt rd-list.....	876
67.1.8	show ip mroute vrf vpn-instance pim-s jointly.....	877
67.1.9	debug ip pim-s mvpn.....	878
67.1.10	debug ip multicast mvpn.....	878
Chapter 68 BVSS Configuration Commands affects ONLY PXT-S2790G/2795G or Higher .....		879
68.1.1	BVSS mode NORMAL.....	879
68.1.1	BVSS mode ENHANCED .....	880
67.1.6	BVSS stack operation commands.....	885
68.1.8	show BVSS stack .....	886

## Chapter 1 System Management Commands

### 1.1 Commands for Managing Configuration Files

Commands for managing configuration files are shown in the following:

- copy
- delete
- dir
- show configuration
- format
- more

#### 1.1.1 copy

Copy command support **tftp** or **ftp** transfer method.

To read files from the TFTP server to the switch, run copy.

```
copy tftp<:filename> {flash<:filename>|rom} [ip_addr]
```

Parameters

	Description
<b>tftp</b> <:filename>	Reads files from the TFTP server. The filename parameter shows the corresponding file name. If the filename parameter is not designated, you are prompted to enter the file name after the copy command is run.
<b>flash</b> <:filename>	Writes files into the flash of the switch. The filename parameter shows the corresponding file name. If the filename parameter is not designated, you are prompted to enter the file name after the copy command is run.
<b>rom</b>	Updates the bootrom of the switch.
<b>ip_addr</b>	Means the IP address of the TFTP server. If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.

Example

```
monitor#copy tftp:switch.bin flash:switch.bin 192.2.2.1
```

The example shows how to copy the switch.bin files from the TFTP server to the flash of the switch.

#### 1.1.2 delete

To delete a file, run **delete**.

```
delete file-name
```

## Parameters

Parameters	Description
<i>file-name</i>	Means a file name with up to 20 characters.

## Default Value

If the file name is not entered, the startup-config files will be deleted by default.

**1.1.3 dir**

To display a file and a directory, run **dir**.

**dir** *file-name*

## Parameters

Parameters	Description
<i>file-name</i>	Means a file name with up to 20 characters.

**1.1.4 show configuration**

To display the current configuration file of the system, run **show configuration** or alias **show running-config**.

The alias **show running-config** supports sub-commands, which allows you to filter the configuration output:

Switch# show running-config ?

```

interface      -- Interface current configuration range-
interface      -- Interface range current configurationnon-
interface      -- Current global configuration
routing-interface -- Routing interface current configuration
|              -- Output modifiers (support Begin/Include/Exclude/Redirect)

```

**1.1.5 format**

To format the file system, run **format** in EXEC mode.

**format**

**1.1.6 more**

To display the content of a file, run **more** in EXEC mode

(equivalent to **cat** command in Linux).

**more** *file-name*

## Parameters

Parameters	Description
<i>file-name</i>	Means a file name with up to 20 characters.

## Usage Guidelines

If all characters in the file are legible, they are displayed in the ASCII code; otherwise, it will be displayed in the binary system.

## 1.2 Basic System Management Commands

### Basic System Management Commands

- bootflash
- cd
- date
- md
- pwd
- rd
- rename
- reboot
- show break
- alias
- boot system flash
- help
- show
- history
- show alias

#### 1.2.1 boot flash

To start a device from the designated file in monitor mode, run the following command.

**boot flash** *filename*

## Parameters

Parameters	Description
<i>file-name</i>	Stands for the name of the designated file.

## Usage Guidelines

After a user enters the monitor state, you can use this command to start a device.

### Example

```
monitor#boot flash switch.bin
```

### 1.2.2 *cd*

To change the current directory, run the following command in the monitoring mode.

```
cd    directory/..
```

#### Parameters

Parameters	Description
<i>directory</i>	Means a file name with up to 20 characters.
..	Parent directory

### Example

```
monitor#cd my_dir
```

#### Related Command

```
pwd
```

### 1.2.4 *date*

To set system absolute time, run command "date".

#### Usage Guidelines

This command is used to set the absolute time for the system. For the switch with a battery-powered clock, the clock will be powered by the battery. If the clock doesn't keep good time, you need to change the battery.

For the switch without a battery-powered clock, the system date is configured to Jan 1st,1970 after the reboot of the switch, and user needs to set the current time each time when starting the switch.

### Example

```
monitor#date
```

```
The current date is 2000-7-27 21:17:24
```

```
Enter the new date(yyyy-mm-dd):2000-7-27
```

```
Enter the new time(hh:mm:ss):21:17:00
```

### 1.2.6 *md*

```
md directory
```

#### Parameters

Parameters	Description
<i>directory</i>	Means a file name with up to 20 characters.

### Usage Guidelines

The command can be used to set a directory.

#### 1.2.7 *pwd*

### Usage Guidelines

The command can be used to display the current directory.

#### 1.2.8 *rd*

**rd** *directory*

### Parameters

Parameters	Description
<i>directory</i>	Means a file name with up to 20 characters.

### Usage Guidelines

The system prompts if the directory is not empty. The system prompts if the directory doesn't exist. To delete a command, use the `rd` command.

#### 1.2.9 *rename*

To rename a file in a file system, use the `rename` command.

**rename** *old\_file\_name new\_file\_name*

### Parameters

Parameters	Description
<i>old_file_name</i>	The original filename.
<i>new_file_name</i>	The new filename.

#### 1.2.10 *reboot*

### Usage Guidelines

The command can be used to reboot the switch.

### Parameters

Parameters	Description
<i>noconfirm</i>	Reboot the switch without confirmation
<i>&lt;cr&gt;</i>	Reboot the switch with confirmation
<i>after (hour:minute)</i>	Reboot the switch after delay

### 1.2.11 *alias*

**alias** *alias\_name* *command\_line*

Parameters

Parameters	Description
<i>alias_name</i>	Name the alias name.
<i>command_line</i>	The command of naming the alias name.

#### Usage Guidelines

The command can be used to replace "command\_line" with "alias\_name". For instance, alias update1 copy tftp:MSU8508\_4.0.0B.bin flash:switch.bin 10.168.30.188. The command "copy tftp:MSU8508\_4.0.0B.bin flash:switch.bin 10.168.30.188 " will automatically run on the switch only update 1 is input.

#### Example

Replace command "copy tftp:MSU8508\_4.0.0B.bin flash:switch.bin 10.168.30.188" with "update1".

```
alias update1 copy tftp:MSU8508_4.0.0B.bin flash:switch.bin 10.168.30.188
```

### 1.2.12 *boot system flash*

To designate the systematic mirror file that will be executed when the system is started, run the following first command; to cancel this settings, run the following second command.

**boot system flash** *filename*

**no boot system flash** *filename*

Parameters

Parameters	Description
<i>filename</i>	Means a file name with up to 20 characters.

#### Usage Guidelines

If the user doesn't configure the command, the system will execute the first system mirror file of the flash file system. If the user configures with multiple commands, the system executes the mirror documents in turn. If the document doesn't exist or occurs mirror. The next file will be executed consecutively. If the file doesn't run successfully, the system enters the monitor mode.

#### Example

```
config#boot system flash switch.bin
```

### 1.2.13 help

#### Usage Guidelines

The command can be used to show the help system of the switch.

#### Example

The following example shows how to show the help system of the switch.

```
switch# help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'interface e?').

### 1.2.14 history

To show history command, run the following command. To return to the default setting, use the no form of this command.

**[no] history** [ + <count> | - <count> | clear]

#### Parameters

Parameters	Description
+ <count>	To display the count<1-20> historical command from the beginning to the end.
- <count>	To display the count<1-20> historical command from the end to the beginning.

#### Default Value

If there are no more than 20 commands executed, all historical command lines will be displayed from the beginning to the end. If there are more than 20 commands executed, all historical command lines will be displayed from the beginning to the end.

#### Command Mode

Any command mode

#### Usage Guidelines

The modularized switch can save up to 20 historical commands. You can invoke these commands with the "up" or "down" key or directly use it after edition. The command can be used to browse the history command. You can run the [no] history command to delete the history command.



## Example

The following example shows how to display the latest 5 history commands from the end to the beginning.

```
switch#history - 5 config
int e1/1 no ip addr
ip addr 192.2.2.49 255.255.255.0
exit
```

### 1.2.15 show

To display the relevant information of the system, which or specific ones of which can be filtered through the filter, run the following command:

**show <sub-command> [ | <begin | include | exclude | redirect> <WORD> [SEPARATOR WORD]]**

#### Parameters

Parameters	Description
<i>sub-command</i>	Stands for a child command.
	Uses the output filter.
<i>begin</i>	Means to show the result of the show command starting with a specific word.
<i>include</i>	Means to show the lines of the result of the show command containing a specific word.
<i>exclude</i>	Means not to show the lines of the result of the show command containing a specific word.
<i>redirect</i>	Redirects the result of the show command to the file in the designated file system.
<i>WORD</i>	Stands for a designated word, which is the designated filename as to the redirect command.
<i>SEPARATOR WORD</i>	Stands for the designated separator, which is space by default to separate the words.

#### Command Mode

The EXEC mode or the configuration mode

#### Usage Guidelines

This command can be used to filter the useless information in the result of the show command, especially when the result is too much to read. For example, if you want to browse a designated MAC address in an MAC address table, which contains a lot of MAC addresses, this command will give you convenience for you.

#### Example

The following example shows how to display the lines, in which the word “interface” is contained, in the result of show running-config.

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

```
Building configuration...
```

Current configuration:

```
!  
interface GigaEthernet0/1  
interface GigaEthernet0/2  
interface GigaEthernet0/3  
interface GigaEthernet0/4  
interface GigaEthernet0/5  
interface GigaEthernet0/6  
interface GigaEthernet0/7  
interface GigaEthernet0/8
```

### 1.2.16 show alias

To display all aliases or the designated alias, run the following command.

**show alias** [*alias name*]

#### Parameters

Parameters	Description
<i>alias name</i>	Name the alias name.

#### Default Value

Display all aliases according the format “alias name=command line”.

#### Command Mode

The EXEC mode or the configuration mode

#### Example

The following example shows how to display all aliases of the current system:

```
switch_config#show alias hualab=date router=snmp
```

#### Related Command

alias

### 1.2.17 show break

It is used to display the abnormal information of the system. The system stores all abnormal information in the latest running. The abnormal information contains the times of abnormality, the stack content and the invoked functions when abnormality occurs.

#### Command Mode

Monitoring Mode Usage

#### Guidelines

The command is only used for debugging.

## Chapter 2 Terminal Service Configuration Commands

### 2.1 Telnet Configuration Commands

The chapter describes telnet and relative commands. The telnet command is used to establish a session with the remote server. The telnet command is always working at the UNIX operating systems. Option negotiation is required. Telnet does not provide itself the login authentication. Telnet is different from Rlogin because telnet does not provide itself password check.

The telnet configuration commands include:

- telnet
- ip telnet
- where
- disconnect
- resume
- clear Telnet
- show Telnet
- debug Telnet

#### 2.1.1 telnet

To establish a telnet session, run the following command:

```
telnet server-ip-addr/server-host-name [/port port][/source-interface interface] [/local
local-ip-addr] [/debug] [/echo | /noecho] [/script scriptname]
```

Parameters

Parameters	Description
<i>server-ip-addr</i>	Dotted-decimal IP address of the remote server
<i>server-host-name</i>	Name of the remote server, which is configured by the ip hostcommand
<i>Port</i>	Telnet port of the remote server
<i>interface</i>	Local interface where the telnet connection is originated
<i>local-ip-addr</i>	Local IP address where the telnet connection is originated
<i>/debug</i>	A negotiation process for enabling the debug at the client side and printing the connection
<i>/echo</i> <i>/noecho</i>	Enable or disable the local echo. The default value is noecho.
<i>scriptname</i>	A script name used for auto login

Default Value

The default port number is 23. The interface has no default number.

## Command Mode

EXEC and global configuration mode

## Usage Guidelines

You can use one of the following command lines to establish a remote login.

```
telnet server-ip-addr/server-host-name
```

In this case, the application program directly sends the telnet login request to port 23 of the remote server. The local IP address is the IP address which is nearest to the peer and found by the routing table.

```
telnet server-ip-addr/server-host-name /port port
```

In this case, the application program sends a telnet login request to the port of the peer.

```
telnet server-ip-addr/server-host-name /source-interface interface
```

In this case, the application program uses the IP address on the interface as the local IP address.

```
telnet server-ip-addr/server-host-name /debug
```

In this case, the application program opens the debug and exports the connection at the client side.

```
telnet server-ip-addr/server-host-name echo/noecho
```

In this case, the application program enables or disables the local echo. The local echo is disabled by default. Only when the server is not in charge of echo is the local echo enabled.

```
telnet server-ip-addr/server-host-name /script scriptname
```

Before executing the automatic login command of the script, run the command `ip telnet script` to configure the script.

The previous commands can be used together.

During the session with the remote server, you can press the Q button to exit the session. If the session is not manually quit, the session will be complete after a 10-second timeout.

## Example

Suppose you want to telnet server 192.168.20.124, the telnet port of the server is port 23 and port 2323, and the local two interfaces are e1/1(192.168.20.240) and s1/0(202.96.124.240). You can run the following operations to complete the remote login.

1. `telnet 192.168.20.124 /port 2323`

In this case, the telnet connection with port 2323 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

2. `telnet 192.168.20.124 /source-interface vlan2`

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 202.96.124.240.

```
3. telnet 192.168.20.124 /local 192.168.20.240
```

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

```
4. telnet 192.168.20.124 /debug
```

In this case, the telnet connection negotiation with port 23 of the peer will be printed out.

```
5. telnet 192.168.20.124 /echo
```

In this case, the local echo is enabled. If the echo is also enabled at the server side, all input will be echoed twice.

```
6. telnet 192.168.20.124 /script s1
```

Use login script S1 for automatic login.

### 2.1.2 ip telnet

To establish a telnet session, run the following command.

```
ip telnet max-user num
```

```
ip telnet enable
```

```
ip telnet source-interface vlan value
```

```
ip telnet access-class accesslist
```

```
ip telnet listen-port start-port [end-port]
```

```
ip telnet script scriptname 'user_prompt' user_answer 'pwd_prompt' pwd_answer
```

Parameters

Parameters	Description
<i>num</i>	telnet maximum connections
<i>value</i>	Local interface where the telnet request is originated
<i>accesslist</i>	Access list name to limit the source address when the local client receives the connection
<i>start-port</i>	Starting port number designated at the listening port area
<i>end-port</i>	End port number designated at the listening port area
<i>scriptname</i>	Name of the login script
<i>user_prompt</i>	Username prompt returned by the telnet server
<i>user_answer</i>	Username response information from the client side
<i>pwd_prompt</i>	Password prompt returned by the telnet server
<i>pwd_answer</i>	Password response information submitted by the client side

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

- Run the following command to configure the local interface for originating the telnet connection:

```
ip telnet source-interface interface
```

In this case, all telnet connections originated afterwards are through the interface. The configuration command is similar to the command `telnet source-interface interface`. However, the telnet command has no interface parameters followed. When the interface is configured and the telnet command has interface parameters, the interface followed the telnet command is used.

- Run the following command to configure the name of the access list which performs limitation on local telnet connection reception.

```
ip telnet access-class accesslist
```

In this case, the access list will be checked when the server accepts all telnet connections.

- Run the following command to configure a port, except the default port 23, to receive the telnet service.

```
ip telnet listen-port start-port [end-port]
```

Note: If the end port number is not designated, the listening will be executed at a specific port. The number of the designated ports cannot be bigger than 16 and the port number ranges between 3001 and 3999.

- Run the following command to configure the telnet login script.

```
ip telnet script s1 'login:' switch 'Password:' test
```

Note: When the script is configured, the username prompt and password prompt and their answers must be correctly matched, especially the prompt information is capital sensitive and has inverted comma ("). If one of them is wrongly configured, the automatic login cannot be performed.

### Note :

You can add the **NO** prefix on the above four commands and then run them to cancel previous configuration.

### Example

1. `ip telnet source-interface vlan1`

In this case, the s1/0 interface will be adopted to originate all telnet connections afterwards.

```
2. ip telnet access-class abc
```

In this case, all the received telnet connections use access list abc to perform the access list check.

```
3. ip telnet listen-port 3001 3010
```

Except port 23, all ports from port 3001 to port 3010 can receive the telnet connection.

```
4. ip telnet script s1 'login:' switch 'Password:' test
```

The login script s1 is configured. The username prompt is login: and the answer is switch. The password prompt is Password: and the answer is test.

### 2.1.3 *ctrl-shift-6+x (the current connection is mounted)*

To mount the current telnet connection, run the following command:

**ctrl-shift-6+x**

#### Parameters

None

#### Default Value

None

#### Command Mode

Any moment in the current telnet session

#### Usage Guidelines

You can use the shortcut key to mount the current telnet connection at the client side.

#### Example

```
switchA>telnet 192.168.20.1
```

```
Welcome to Multi-Protocol 2000 Series switch
```

```
switchB>ena
```

```
switchB#(press ctrl-shift-6+x)
```

```
switchA>
```

You press **ctrl-shift-6+x** to mount the telnet connection to switch B and return to the current state of switch A.

### 2.1.4 *where*

To check the currently mounted telnet session, run the following command:

**where**

**Parameters**

None

**Default Value**

None

**Command Mode**

Global configuration mode

**Usage Guidelines**

The command can be used to check the mounted outward telnet connection at the client side. The displayed information contains the serial number, peer address, local address and local port.

**Note:**

The where command is different from the show telnet command. The former is used at the client side and the displayed information is the outward telnet connection.

**Example**

```
switchA>telnet 192.168.20.1
```

```
Welcome to Multi-Protocol 2000 Series switch
```

```
switchB>enable
```

```
switchB#(press ctrl-shift-6+x)
```

```
switchA> telnet 192.168.20.2
```

```
Welcome to Multi-Protocol 2000 Series switch
```

```
switchC>enable
```

```
switchC#(press ctrl-shift-6+x)
```

```
switchA>where
```

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.1	23	192.168.20.180	20034
2	192.168.20.2	23	192.168.20.180	20035

Enter **where** at switch A. The mounted outward connection is displayed.

**2.1.5 resume**

To resume the currently mounted outward telnet connection, run the following command:

```
resume no
```

**Parameters**



Parameters	Description
<i>no</i>	Number of the currently mounted telnet session that is checked through the where command

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

The command can be used to resume the currently mounted outward telnet connection at the client side.

### Example

```
switchA>telnet 192.168.20.1
Welcome to Multi-Protocol 2000 Series switch
switchB>ena
switchB#(press ctrl-shift-6+x)
switchA> telnet 192.168.20.2
Welcome to Multi-Protocol 2000 Series switch
switchC>ena
switchC#(press ctrl-shift-6+x)
switchA>where
NO.   Remote Addr      Remote Port      Local Addr      Local Port
1     192.168.20.1     23              192.168.20.180 20034
2     192.168.20.2     23              192.168.20.180 20035
switchA>Resume 1
[Resuming connection 1 to 192.168.20.73 . . . ] (enter)
switchB#
```

After you enter where at switch A and the mounted outward connection of switch A is displayed, enter Resume1.You will be prompted that connection 1 is resumed. The command prompts of switch B are displayed after the Enter key is pressed.

### 2.1.6 disconnect

To clear the currently mounted outward telnet session, run the following command:

**disconnect** *no*

## Parameters

Parameters	Description
<i>no</i>	Number of the currently mounted telnet session that is checked through the where command

## Default Value

None

## Command Mode

Global configuration mode

## Usage Guidelines

The command can be used to clear the currently mounted outward telnet connection at the client side.

**Note:**

The **disconnect** command is different from the **clear telnet** command. The former is used at the client side and clears the outward telnet connection. The latter is used at the server and clears the inward telnet connection.

## Example

```
switchA>telnet 192.168.20.1
Welcome to Multi-Protocol 2000 Series switch
switchB>ena
switchB#(press ctrl-shift-6+x)
switchA> telnet 192.168.20.2
Welcome to Multi-Protocol 2000 Series switch
switchC>ena
switchC#(press ctrl-shift-6+x)
switchA>where
NO.      Remote Addr      Remote Port      Local Addr      Local Port
1       192.168.20.1      23              192.168.20.180  20034
2       192.168.20.2      23              192.168.20.180  20035
switchA>disconnect 1
<Closing connection to 192.168.20.1> <y/n>y
Connection closed by remote host.
switchA>
```

After you enter where at switch A and the mounted outward connection of switch A is displayed, enter disconnect 1. You will be prompted whether the connection of switch B is closed. After you enter Y, the connection is closed.

### 2.1.7 *clear telnet*

To clear the telnet session at the server, run the following command:

```
clear telnet no
```

#### Parameters

Parameters	Description
<i>no</i>	Number of the telnet session that is displayed after the show telnet command is run

#### Default Value

None

#### Command Mode

EXEC

#### Usage Guidelines

The command can be used to clear the telnet session at the server.

#### Example

```
clear telnet 1
```

The telnet session whose sequence number is 1 is cleared at the server (192.168.20.220:1097).

### 2.1.8 *show telnet*

To display the telnet session at the server, run the following command:

```
show telnet
```

#### Parameters

None

#### Default Value

None

#### Command Mode

All command modes except the user mode

#### Usage Guidelines

The command can be used to display the telnet session at the server. The displayed information includes the sequence number, peer address, peer port, local address and local port.

### Example

```
Switch# show telnet
```

If you run the previous command, the result is shown as follows:

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.220	1097	192.168.20.240	23
2	192.168.20.180	14034	192.168.20.240	23

### 2.1.9 *debug telnet*

The following is a format of the debug command for the telnet session:

#### **debug telnet**

##### Parameters

None

##### Default Value

None

##### Command Mode

EXEC

##### Usage Guidelines

The command can be used to enable the switch of the telnet debug.

If the switch of the telnet debug is enabled, the negotiation processes of all the incoming telnet sessions are printed on the window that the debug command invokes. The debug telnet command is different from the telnet debug command. The former is to export the debug information of the telnet session connected to the server. The latter is to export the debug information of the telnet session that the client originates.

### Example

```
debug telnet
```

The debug information of the telnet session that is connected to the server is displayed.

## 2.2 **Terminal Configuration Commands**

The terminal configuration commands include:

- attach-port
- autocommand
- clear line

- connect
- disconnect
- exec-timeout
- length
- line
- location
- login authentication
- monitor
- no debug all
- password
- resume
- show debug
- show line
- terminal-type
- terminal monitor
- terminal width
- terminal length
- where
- width

### 2.2.1 *attach-port*

To bind the telnet listening port to the line vty number and enable the telnet connection at a specific port generates vty according to the designated sequence number, run the following command:

**[no] attach-port** PORT

#### Parameters

Parameters	Description
<i>Port</i>	<b>Listening port of the telnet server (3001-3999)</b>

#### Default Value

None

#### Command Mode

Line configuration mode

### Example

Bind listening port 3001 to line vty 2 3.

```
switch_config# line vty 2 3
```

```
switch_config_line#attach-port 3001
```

### 2.2.2 *autocommand*

To set the automatically-run command when user logs in to the terminal, run the following command. The connection is cut off after the command is executed.

**autocommand** *LINE*

**no autocommand**

Parameters

Parameters	Description
<i>LINE</i>	Command to be executed

### Command Mode

Line configuration mode

### Example

```
switch_conf#line vty 1
```

```
switch_conf_line#autocommand pad 123456
```

After you successfully log in, the host whose X.121 address is 123456 will be automatically padded.

### 2.2.3 *clear line*

To clear the designated line, run the following command:

```
clear line [console | vty] [number]
```

Parameters

Conform to the line command

### Command Mode

EXEC

### Example

```
switch#clear line vty 0
```

## 2.2.4 connect

To connect Telnet server, run the following command:

```
connect server-ip-addr/server-host-name {[/port port]/[/source-interface interface] [/local local-ip-addr]} [/script word]
```

### Parameters

Parameters	Description
<i>server-ip-addr/server-host-name</i>	<b>IP address or host name of the server</b>
<i>Port</i>	<b>Port number</b>
<i>interface</i>	<b>Interface name where the Telnet connection is originated</b>
<i>local-ip-addr</i>	<b>Local IP address where the telnet connection is originated</b>
<i>word</i>	<b>Name of the script</b>

### Command Mode

All Configuration Modes

### Example

```
switch# connect 192.168.20.1
```

## 2.2.5 disconnect

To delete the suspended telnet session, run the following command:

```
disconnect N
```

### Parameters

Parameters	Description
<i>N</i>	<b>number of the suspended telnet dialog</b>

### Command Mode

All Configuration Modes

### Example

```
switch#disconnect 1
```

## 2.2.6 exec-timeout

To set the max idle time of the terminal, run the following command:

```
[no] exec-timeout [time]
```

## Parameters

Parameters	Description
<i>time</i>	Idle time in seconds Value range: 0-86400

## Default Value

0 (no time-out limit)

## Command Mode

Line configuration mode

## Example

The following example shows how to set the idle time of the line to 1 hour.

```
switch_config_line#exec-timeout 3600
```

**2.2.7 length**

To set the line number on the screen of the terminal, run the following command:

```
[no] length [value]
```

## Parameters

Parameters	Description
<i>value</i>	Value range: 0 to 512. The value 0 means there is no pause.

## Default Value

24

## Command Mode

Line configuration mode

**2.2.8 line**

To enter the line configuration mode, run the following command:

```
line [console | vty] [number]
```

## Parameters

Parameters	Description
<i>console</i>	Monitoring line, which has only one number 0
<i>vty</i>	Virtual lines such as Telnet, PAD and Rlogin
<i>number</i>	Number in the line of the type



## Command Mode

Global configuration mode

### Example

The following example shows how to enter the line configuration mode of VTY 0 to 10.

```
switch_config#line vty 0 10
```

### 2.2.9 *location*

To record the description of the current line, run the following command:

**location** [*LINE*]

**no location**

Parameters

Parameters	Description
<i>LINE</i>	Description of the current line.

## Command Mode

Line configuration mode

### 2.2.10 *login authentication*

To set line login authentication, run the following command:

**[no] login authentication** [**default** | *WORD*]

Parameters

Parameters	Description
<i>default</i>	Default authentication mode
<i>WORD</i>	Name of the authentication list

## Command Mode

Line configuration mode

### Example

```
switch_conf_line#login authentication test
```

The above example shows how to set the authentication list of the line to test.

### 2.2.11 *monitor*

To export the log and debugging information to the line, run the following command:

**[no] monitor**

**Parameters**

None

**Command Mode**

Line configuration mode

**Example**

switch\_config\_line#monitor

**2.2.12 no debug all**

To shut down all debugging output of the current VTY, run the following command:

**no debug all****Parameters**

None

**Command Mode**

EXEC

**Example**

switch#no debug all

**2.2.13 password**

To set the password for the terminal, run the following command:

**password** {password | [encryption-type] encrypted-password }**no password****Parameters**

Parameters	Description
<i>password</i>	<b>Password configured on the line, which is entered in the plaintext form and whose maximum length is 30 bits.</b>
<i>[encryption-type] encrypted-password</i>	<b>encryption-type means the encryption type of the password. Currently, products only support two encryption modes: 0 and 7. The number 0 means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.</b>

For password encryption, refer to the explanation of the commands servicepassword-encryption and enable password.

## Command Mode

Line configuration mode

### Example

```
switch_conf#line vty 1 switch_conf_line#password test
```

The above example shows how to set the login password of VTY1 to test.

### 2.2.14 *resume*

To resume the mounted telnet session, run the following command:

```
resume N
```

Parameters

Parameters	Description
<i>N</i>	number of the suspended telnet dialog

## Command Mode

All Configuration Modes

### Example

```
switch#resume 1
```

### 2.2.15 *show debug*

To display all debugging information of the current VTY, run the following command:

```
show debug
```

Parameters

None

## Command Mode

EXEC or global configuration mode

### Example

```
Switch# show debug  
http authentication debug is on  
http cli debug is on  
http request debug is on  
http response debug is on  
http session debug is on  
http erro debug is on  
http file debug is on
```

TELNET:

Incoming Telnet debugging is on

### 2.2.16 show line

To display the status of the current effective line, run the following command:

```
show line {[console | vty] [number]}
```

#### Parameters

If there is no parameter followed, the status of all effective lines will be displayed. The definition of other parameters is similar to that of the line command.

#### Command Mode

Non-user mode

### 2.2.17 terminal length

To change the line number on the current terminal screen, run the following command. The parameter can be obtained by the remote host. The rlogin protocol uses the parameter to notify the remote UNIX host. Run the no terminal length command to resume the default value:

```
terminal length length
```

```
no terminal length
```

#### Parameters

Parameters	Description
<i>length</i>	Line number displayed on each screen Value range: 0-512

#### Default Value

Pause when 24 lines are displayed on the screen.

#### Command Mode

Global configuration mode

#### Usage Guidelines

This command only takes effect on the current terminal. When a session is terminated, the attributes of this terminal are also gone.

#### Example

```
switch#terminal length 40
```

#### Related Command

**line**

### 2.2.18 *terminal monitor*

To display the output debug and the system error information, run the following command. To shutdown the monitor, use the no form of this command.

**terminal monitor**

**no terminal monitor**

Parameters

None

Default Value

The system's console port is enabled by default, while other terminals are disabled by default.

Command Mode

Global configuration mode

Usage Guidelines

This command only takes effect on the current terminal. When a session is terminated, the attributes of this terminal are also gone.

Example

```
switch#terminal monitor
```

Related Command

**line**

**debug**

### 2.2.19 *terminal width*

In default settings, the switch is to export 80 characters in each line. If the default settings cannot meet your requirements, you can reset it. The parameter can be obtained by the remote host. To set the character number in each line, run the following command. To return to the default setting, use the no form of this command.

**terminal width** *number*

**no terminal width**

Parameters

Parameters	Description
<i>number</i>	Character number of each line

Default Value

80 characters in each line

## Command Mode

Global configuration mode

## Usage Guidelines

This command only takes effect on the current terminal. When a session is terminated, the attributes of this terminal are also gone.

### Example

```
switch#terminal width 40
```

### Related Command

line

## 2.2.20 terminal-type

To set the terminal type, run the following command:

```
[no] terminal-type [name]
```

### Parameters

Parameters	Description
<i>name</i>	Terminal name Terminal types currently supported are VT100, ANSI andVT100J.

### Default Value

ANSI

### Command Mode

Line configuration mode

## 2.2.21 where

To check the currently mounted telnet session, run the following command:

```
where
```

### Parameters

None

### Command Mode

All Configuration Modes

### Example

```
switch#where
```

## 2.2.22 width

To set the terminal width of the line, run the following command:

```
[no] width [value]
```

### Parameters

Parameters	Description
<i>value</i>	Value range: 0 to 256. The value 0 means no execution.

### Default Value

80

### Command Mode

Line configuration mode

## Chapter 3 Maintenance and Debugging Tool Commands

### 3.1 Network Testing Tool Commands

#### 3.1.1 ping

To test host accessibility and network connectivity, run the following command. After the ping command is run, an ICMP request message is sent to the destination host, and then the destination host returns an ICMP response message.

```
ping [-a][-d][-f] [-i {source-ip-address}] [-m {source-interface}] [-j host1 [host2 host3 ...]]
[-k host1 [host2, host3 ...]] [-l length] [-n number] [-r hops] [-s tos] [-t ttl] [-v] [-w
waittime] [-b interval] [-c] host
```

Parameters

Parameters	Description
<i>-a</i>	Sets the ping command keeping running until it is interrupted.
<i>-d</i>	Sets the direct routing to the port without checking the routing table when forwarding the packet.
<i>-f</i>	Sets the DF digit (message is not segmented). If the message required to be sent is larger than the MTU of the path, the message will be dropped by the routing switch on the path and the routing switch will then return an ICMP error message to the source host. If network performance has problems, one node in the network may be configured to a small MTU. You can use the <i>-f</i> option to decide the smallest MTU on the path. Default value: No resetting
<i>-i</i>	Sets the source IP address of the message or the IP address of an interface. Default value: Main IP address of the message-sending interface
<i>source-ip-address</i>	Source IP address adopted by the message
<i>source-interface</i>	Message takes the IP address of the source-interface interface as the source address.
<i>-j host1 [host2 host3...]</i>	Sets the relaxation source route. Default: Not set
<i>-k host1 [host2 host3...]</i>	Sets the strict source route Default: Not set
<i>-l length</i>	Sets the length of ICMP data in the message. Default: 56 bytes
<i>-n number</i>	Sets the total number of messages. Default: 5 messages
<i>-r hops</i>	Records routes. Up to hops routes are recorded. Default: not record
<i>-s tos</i>	Sets IP TOS of the message to tos. Default Value:0.
<i>-t ttl</i>	Sets IP TTL of the message to ttl. Default Value:255.
<i>-v</i>	Detailed output
<i>-w waittime</i>	Time for each message to wait for response Default Value:2seconds.
<i>-b interval</i>	Sets the time interval of sending ping packet. Unit: 10ms; Value range: 0-65535; Default Value: 0.

<code>-c</code>	<b>Simple output</b>
<code>host</code>	<b>Destination host</b>

## Command Mode

EXEC and global configuration mode

## Usage Guidelines

The command supports that the destination address is the broadcast address or the multicast address. If the destination address is the broadcast address (255.255.255.255) or the multicast address, the ICMP request message is sent on all interfaces that support broadcast or multicast. The routing switch is to export the addresses of all response hosts. By pinging multicast address 224.0.0.1, you can obtain the information about all hosts in directly-connected network segment that support multicast transmission.

Press the Q key to stop the ping command.

Simple output is adopted by default.

Parameters	Description
<code>!</code>	<b>A response message is received.</b>
<code>.</code>	<b>Response message is not received in the timeout time.</b>
<code>U</code>	<b>The message that the ICMP destination cannot be reached is received.</b>
<code>Q</code>	<b>The ICMP source control message is received.</b>
<code>R</code>	<b>The ICMP redirection message is received.</b>
<code>T</code>	<b>The ICMP timeout message is received.</b>
<code>P</code>	<b>The ICMP parameter problem message is received.</b>

The statistics information is exported:

Parameters	Description
<code>packets transmitted</code>	<b>Number of transmitted messages</b>
<code>packets received</code>	<b>Number of received response messages, excluding other ICMP messages</b>
<code>packet loss</code>	<b>Rate of messages that are not responded to</b>
<code>round-trip min/avg/max</code>	<b>Minimum/average/maximum time of a round trip (ms)</b>

## Example

```
switch#ping -l 10000 -n 30 192.168.20.125
PING 192.168.20.125 (192.168.20.125): 10000 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```



```
--- 192.168.20.125 ping statistics ---
```

```
30 packets transmitted, 30 packets received, 0% packet loss
```

```
round-trip min/avg/max = 50/64/110 ms
```

### 3.1.2 traceroute

To detect which routes have already reached the destination, run the following command.

You can transmit to the destination the UDP packets (or ICMP ECHO packets) of different TTLs to confirm which routes have come to the destination. Each router on this path has to deduct 1 from the TTL value before forwarding ICMP ECHO packets. Speaking from this aspect, TTL is an effective hop count. When the TTL value of a packet is deducted to zero, the router sends back to the source system the ICMP timeout message. Send the first response packet whose TTL is 1 and send TTL plus 1 subsequently until the target reaches to the max TTL.

By checking the ICMP timeout message sent back by inter medial routers, you can confirm the routers. At the arrival of the destination, the traceroute sends a UPD packet whose port ID is larger than 30000; the destination node hence can only transmit back a Port Unreachable ICMP message. This reception of this message means the arrival of destination.

```
traceroute [-i source-ip-address ] [-m source-interface}] [-j host1 [host2 host3 ...]]
[-k host1 [host2, host3 ...]] [-p port-number] [-q probe-count] [-r hops] [-t ttl] [-w
waittime] [-x icmp] host
```

#### Parameters

Parameters	Description
<i>-i source-ip-address</i>	<b>Sets the source IP address of packet.</b>
<i>-m source-interface</i>	<b>Sets the packet-transmitted port.</b>
<i>-j host1 [host2 host3...]</i>	<b>Sets the relaxation source route. Default: Not set</b>
<i>-k host1 [host2 host3...]</i>	<b>Sets the strict source route Default: Not set</b>
<i>-p port-number</i>	<b>Sets the ID of destination port that transmits UDP packets. Default value: 33434 Default: 33434</b>
<i>-q probe-count</i>	<b>Sets the number of packets that you detect each time. Default: 3 messages</b>
<i>-r hops</i>	<b>Records routes. Up to hops routes are recorded. Default: not record</b>
<i>-t ttl</i>	<b>Sets IP TTL of the message to ttl. Default: the minimum and maximum TTLs are 1 and 30 respectively.</b>
<i>-w waittime</i>	<b>Time for each message to wait for response Default: 3 seconds</b>
<i>-x icmp</i>	<b>Sets the detection packet to be the ICMP ECHO packet. Default: UDP packet</b>
<i>host</i>	<b>Destination host</b>

#### Command Mode

EXEC and global configuration mode

### Usage Guidelines

The UDP packet is used for detection by default, but you can run `-x icmp` to replace it with ICMP ECHO for detection.

If you want to stop traceroute, press `q` or `Q`. By default, the simple output information is as follows.

Simple output is adopted by default.

Parameters	Description
<i>!N</i>	Receives an ICMP-route unreachable packet.
<i>!H</i>	Receives an ICMP-host unreachable packet.
<i>!P</i>	Receives an ICMP-protocol unreachable packet.
<i>!F</i>	Receives an ICMP unreachable (need to be fragmented) packet.
<i>!S</i>	Receive an ICMP unreachable (failing to detect the source-station route) packet.

The statistics information is exported:

Parameters	Description
<i>hops max</i>	Means the maximum detection hops (the threshold of ICMP).
<i>byte packets</i>	Stands for the size of each detection packet.

### Example

```
switch#traceroute 90.1.1.10
traceroute to 90.1.1.10 (90.1.1.10), 30 hops max, 36 byte packets
 1 90.2.2.1  0 ms  0 ms  0 ms
 2 90.1.1.10 0 ms  0 ms  0 ms
```

## 3.2 Fault Diagnosis Commands

The chapter describes the commands used for fault diagnosis. All the following commands are used to detect the reason of the fault. You can use other commands to remove the fault, such as the debug command.

The chapter only introduces the universal diagnosis commands. For more details, please refer to the Fault Diagnosis White Paper.

The fault diagnosis commands include:

- logging
- logging buffered
- logging console

- logging facility
- logging monitor
- logging on
- logging trap
- logging command
- logging source-interface
- logging history alerts
- logging history critical
- logging history debugging
- logging history emergencies
- logging history errors
- logging history informational
- logging history notifications
- logging history warnings
- logging history rate-limit
- logging history size
- service timestamps
- clear logging
- show break
- show debug
- show logging

### 3.2.1 logging

To display the state of logging (syslog), run the following command. To return to the default setting, use the no form of this command.

**logging** A.B.C.D level

**no logging** A.B.C.D level

Parameters

Parameters	Description
<i>A.B.C.D</i>	IP address of the syslog server
<i>level</i>	Level of log information on the server Refer to table 1.

### Default value

The log information is not recorded to the server.

### Command Mode

Global configuration mode

### Usage Guidelines

The command can be used to record the log information to the designated syslog server. The command can be used for many times to designate multiple syslog servers.

### Example

```
logging 192.168.1.1 errors
```

### Related Command

```
logging trap
```

### 3.2.2 logging buffered

To record the log information to the memory of the switch, run the following command.

```
logging buffered [size | level | dump ]
```

```
no logging buffered
```

### Parameters

Parameters	Description
<i>size</i>	<b>Size of memory cache</b> <b>Value range: 4096-2147483647 Unit: byte</b>
<i>level</i>	<b>Information level of the log recorded to memory cache</b> <b>Refer to table 1.</b>
<i>dump</i>	<b>When the system has abnormality, the information in the current memory is currently recorded to the flash and the information is resumed after the system is restarted.</b>

### Default Value

The information is not recorded to the memory cache.

### Command Mode

Global configuration mode

### Usage Guidelines

The command records the log information to the memory cache of the switch. The memory cache is circularly used. After the memory cache is fully occupied, the latter information will cover the previous information.

You can use the show logging command to display the log information recorded in the memory cache of the switch.

Do not use big memory for it causes the shortage of memory.

Table 1 Level of log recording

Prompt	Level	Description	Syslog definition
<i>emergencies</i>	0	System unusable	LOG_EMERG
<i>alerts</i>	1	Immediate action needed	LOG_ALERT
<i>critical</i>	2	Critical conditions	LOG_CRIT
<i>errors</i>	3	Error conditions	LOG_ERR
<i>warnings</i>	4	Warning conditions	LOG_WARNING
<i>notifications</i>	5	Normal but significant condition	LOG_NOTICE
<i>informational</i>	6	Informational messages only	LOG_INFO
<i>debugging</i>	7	Debugging messages	LOG_DEBUG

### Related Command

**clear logging**

**show logging**

### 3.2.3 logging console

To control the information volume displayed on the console, run the following command.

To forbid the log information to be displayed on the console, use the no form of this command.

**logging console *level***

**no logging console**

### Parameters

Parameters	Description
<i>level</i>	Information level of the logs displayed on the console Refer to table 2.

### Default Value

The log level displayed on the console port is debugging by default.

### Command Mode

Global configuration mode

### Usage Guidelines

After the information level is specified, information of this level or the lower level will be displayed on the console.

Run the command `show logging` to display the currently configured level and the statistics information recorded in the log.

Table 2 Level of log recording

Prompt	Level	Description	Syslog definition
<i>emergencies</i>	<b>0</b>	<b>System unusable</b>	<b>LOG_EMERG</b>
<i>alerts</i>	<b>1</b>	<b>Immediate action needed</b>	<b>LOG_ALERT</b>
<i>critical</i>	<b>2</b>	<b>Critical conditions</b>	<b>LOG_CRIT</b>
<i>errors</i>	<b>3</b>	<b>Error conditions</b>	<b>LOG_ERR</b>
<i>warnings</i>	<b>4</b>	<b>Warning conditions</b>	<b>LOG_WARNING</b>
<i>notifications</i>	<b>5</b>	<b>Normal but significant condition</b>	<b>LOG_NOTICE</b>
<i>informational</i>	<b>6</b>	<b>Informational messages only</b>	<b>LOG_INFO</b>
<i>debugging</i>	<b>7</b>	<b>Debugging messages</b>	<b>LOG_DEBUG</b>

### Example

logging console alerts

### Related Command

**logging facility**

**show logging**

### 3.2.4 logging facility

To record specified error information, run the following command. To restore to local7, use the no form of this command.

**logging facility facility-type**

**no logging facility**

### Parameters

Parameters	Description
<i>facility-type</i>	<b>Facility type Refer to table 3.</b>

### Default Value

local7

### Command Mode

Global configuration mode

### Usage Guidelines

Table 3 Facility type

Parameters	Description
<i>auth</i>	<b>Authorization system</b>
<i>cron</i>	<b>Cron facility</b>
<i>daemon</i>	<b>System daemon</b>
<i>kern</i>	<b>Kernel</b>
<i>local0-7</i>	<b>Reserved for locally defined messages</b>
<i>lpr</i>	<b>Line printer system</b>
<i>mail</i>	<b>Mail system</b>
<i>news</i>	<b>USENET news</b>
<i>sys9</i>	<b>System use</b>
<i>sys10</i>	<b>System use</b>
<i>sys11</i>	<b>System use</b>
<i>sys12</i>	<b>System use</b>
<i>sys13</i>	<b>System use</b>
<i>sys14</i>	<b>System use</b>
<i>syslog</i>	<b>System log</b>
<i>user</i>	<b>User process</b>
<i>uucp</i>	<b>UNIX-to-UNIX copy system</b>

## Example

logging facility kern

## Related Command

**logging console**

### 3.2.5 logging monitor

To control the information volume displayed on the terminal line, run the following command.

To forbid the log information to be displayed on the terminal line, use the no form of this command.

**logging monitor level**

**no logging monitor**

Parameters

Parameters	Description
<i>level</i>	Information level of the logs displayed on the terminal line Refer to table 4.

### Default Value

debugging

### Command Mode

Global configuration mode

### Usage Guidelines

Table 4 Level of log recording

Prompt	Level	Description	Syslog definition
<i>emergencies</i>	<b>0</b>	<b>System unusable</b>	<b>LOG_EMERG</b>
<i>alerts</i>	<b>1</b>	<b>Immediate action needed</b>	<b>LOG_ALERT</b>
<i>critical</i>	<b>2</b>	<b>Critical conditions</b>	<b>LOG_CRIT</b>
<i>errors</i>	<b>3</b>	<b>Error conditions</b>	<b>LOG_ERR</b>
<i>warnings</i>	<b>4</b>	<b>Warning conditions</b>	<b>LOG_WARNING</b>
<i>notifications</i>	<b>5</b>	<b>Normal but significant condition</b>	<b>LOG_NOTICE</b>
<i>informational</i>	<b>6</b>	<b>Informational messages only</b>	<b>LOG_INFO</b>
<i>debugging</i>	<b>7</b>	<b>Debugging messages</b>	<b>LOG_DEBUG</b>

### Example

logging monitor errors

### Related Command

terminal monitor

### 3.2.6 logging on

To control the recording of error information, run the following command. To forbid all records, use the no form of this command.

logging on

no logging on

### Parameters

None

### Default Value

logging on



## Command Mode

Global configuration mode

### Example

```
switch_config# logging on
```

```
switch_config# ^Z
```

```
switch#
```

```
Configured from console 0 by DEFAULT
```

```
switch# ping 192.167.1.1
```

```
switch#ping 192.167.1.1
```

```
PING 192.167.1.1 (192.167.1.1): 56 data bytes
```

```
!!!!
```

```
--- 192.167.1.1 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0/4/10 ms
```

```
switch#IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
```

```
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
```

```
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
```

```
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
```

```
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
```

```
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
```

```
switch_config# no logging on
```

```
switch_config# ^Z switch#
```

```
switch# ping 192.167.1.1
```

```
PING 192.167.1.1 (192.167.1.1): 56 data bytes
```

```
!!!!
```

```
--- 192.167.1.1 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0/4/10 ms
```

## Related Command

**logging**

**logging buffered**

**logging monitor**

**logging console**

### 3.2.7 *logging trap*

To control the information volume recorded to the syslog server, run the following command.

To forbid the information to be recorded to the syslog server, use the no form of this command.

**logging trap *level***

**no logging trap**

## Parameters

Parameters	Description
<i>level</i>	Information level of the logs displayed on the terminal line Refer to table 5.

## Default Value

Informational

## Command Mode

Global configuration mode

## Usage Guidelines

Table 5 Level of log recording

Prompt	Level	Description	Syslog definition
<i>emergencies</i>	<b>0</b>	<b>System is unusable</b>	<b>LOG_EMERG</b>
<i>alerts</i>	<b>1</b>	<b>Immediate action needed</b>	<b>LOG_ALERT</b>
<i>critical</i>	<b>2</b>	<b>Critical conditions</b>	<b>LOG_CRIT</b>
<i>errors</i>	<b>3</b>	<b>Error conditions</b>	<b>LOG_ERR</b>
<i>warnings</i>	<b>4</b>	<b>Warning conditions</b>	<b>LOG_WARNING</b>

<i>notifications</i>	<b>5</b>	<b>Normal but significant condition</b>	<b>LOG_NOTICE</b>
<i>informational</i>	<b>6</b>	<b>Informational messages only</b>	<b>LOG_INFO</b>
<i>debugging</i>	<b>7</b>	<b>Debugging messages</b>	<b>LOG_DEBUG</b>

### Example

```
logging 192.168.1.1
```

```
logging trap notifications
```

### Related Command

```
logging
```

### 3.2.8 logging command

To enable the command execution recording, run logging command. After this function is enabled will be generated for each of all entered commands, in which the line to execute this command, the command line, the execution result, the login line and the login address will be recorded.

To disable this function, use the no form of this command.

### Parameters

None

### Default Value

```
no logging command
```

### Command Mode

Global configuration mode

### Example

```
Switch_config#logging command
```

```
Switch_config#Jul 11 15:26:56 %CMD-6-EXECUTE: `logging command` return 0, switch(vty 0, 192.168.25.42).
```

### Related Command

```
logging
```

### 3.2.9 logging source-interface

To set the source port of log exchange, run the following command. You can use no logging source-interface to disable this function.

### Parameters

None

**Default Value**

no logging source-interface

**Command Mode**

Global configuration mode

**Example**

```
Switch_config# logging source-interface vlan 1
```

**Related Command**

logging

**3.2.10 logging history alerts**

To set the level of the historical log table to alerts (need to act immediately), run the following command.

**Parameters**

None

**Default Value**

logging history warnings

**Command Mode**

Global configuration mode

**Example**

```
Switch_config#logging history alerts
```

**Related Command**

logging

**3.2.11 logging history critical**

To set the level of the historical log table to critical, run the following command.

**Parameters**

None

**Default Value**

logging history warnings

**Command Mode**

Global configuration mode

**Example**

Switch\_config#logging history critical

#### Related Command

logging

### ***3.2.12 logging history debugging***

This command is used to set the level of the historical log table to debugging

#### Parameters

None

#### Default Value

logging history warnings

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#logging history debugging
```

#### Related Command

logging

### ***3.2.13 logging history emergencies***

To set the level of the historical log table to emergencies, run the following command:

#### Parameters

None

#### Default Value

logging history warnings

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#logging history emergencies
```

#### Related Command

logging

### ***3.2.14 logging history errors***

This command is used to set the level of the historical log table to errors.

#### Parameters

None

**Default Value**

logging history warnings

**Command Mode**

Global configuration mode

**Example**

Switch\_config#logging history errors

**Related Command**

logging

**3.2.15 logging history informational**

This command is used to set the level of the historical log table to informational.

**Parameters**

None

**Default Value**

logging history warnings

**Command Mode**

Global configuration mode

**Example**

Switch\_config#logging history informational

**Related Command**

logging

**3.2.16 logging history notifications**

This command is used to set the level of the historical log table to notifications.

**Parameters**

None

**Default Value**

logging history warnings

**Command Mode**

Global configuration mode

**Example**

Switch\_config#logging history notifications

#### Related Command

logging

### 3.2.17 logging history warnings

To set the level of the historical log table to warnings, run the following command:

#### Parameters

None

#### Default Value

logging history warnings

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#logging history warnings
```

#### Related Command

logging

### 3.2.18 logging history rate-limit

To set the log output rate, run the following command.

#### Parameters

Parameters	Description
<1-512>	Stands for the number of logs which are exported each second.

#### Default Value

logging history rate-limit 0

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#logging history rate-limit 256
```

#### Related Command

logging

### 3.2.19 logging history size

To set the number of entries in the historical log table, run the following command. logging history size

## Parameters

Parameters	Description
<0-500>	Stands for the number of historical log entries.

## Default Value

logging history size 0

## Command Mode

Global configuration mode

## Example

```
Switch_config#logging history size 256
```

## Related Command

logging

**3.2.20 service timestamps**

To set configure the time stamp that is added when the system is debugged or records the log information, run the following command.

To cancel the time stamp that is added when the system is debugged or records the log information, use the no form of this command.

```
service timestamps [log|debug] [uptime|datetime]
```

```
no service timestamps [log|debug]
```

## Parameters

Parameters	Description
<i>log</i>	Adds the time stamp before the log information.
<i>debug</i>	Adds the time stamp before the debug information.
<i>uptime</i>	Duration between the startup of the switch and the current time
<i>datetime</i>	Real-time clock time

## Default Value

service timestamps log date

service timestamps debug date

## Command Mode

Global configuration mode

## Usage Guidelines



The time stamp in the uptime form is displayed like HHHH:MM:SS, meaning the duration from the start-up of the switch to the current time.

The time stamp in the date form is displayed like YEAR-MON-DAY HH:MM:SS, meaning the real-time clock time.

### Example

```
service timestamps debug uptime
```

### 3.2.21 clear logging

To clear the log information recorded in the memory cache, run the following command.

#### clear logging

##### Parameters

None

##### Command Mode

EXEC

##### Related Command

#### logging buffered

#### show logging

### 3.2.22 show break

To display the information about abnormal breakdown of the switch, run the following command.

```
show break
```

##### Parameters

None

##### Default Value

None

##### Command Mode

EXEC

##### Usage Guidelines

The command can be used to display the information about abnormal breakdown of the switch, helping to find the cause of the abnormality.

### Example

```
switch#show break
```

```
Exception Type:1400-Data TLB error BreakNum: 1 s date: 2000-1-1 time: 0:34:6
```

```
r0    r1    r2    r3    r4    r5    r6
```

```

00008538-01dbc970-0054ca18-00000003-80808080-fefefeff-01dbcca1-
r7    r8    r9    r10   r11   r12   r13
00000000-00009032-00000000-7ffffff0-00008588-44444444-0054c190-
r14   r15   r16   r17   r18   r19   r20
000083f4-000083f4-00000000-00000000-00000000-00000000-00000000-
r21   r22   r23   r24   r25   r26   r27
00000000-0000000a-00000001-00000000-00000000-004d6ce8-01dbd15c-
r28   r29   r30   r31   spr8  spr9  ip
00000002-00467078-00010300-00000300-00000310-00008588-00000370-
Variables :
00008538-44444444-01dbd15c-01dbcaac-00000002-00000000-004d6ce8-
01dbca18-
00008538 --- do_chram_mem_sys_addr---bspcfg.o
0001060c --- subcmd---cmdparse.o---libcmd.a
000083e4 --- do_chram_mem_sys---bspcfg.o
0000fb24 --- lookupcmd---cmdparse.o---libcmd.a
0000f05c --- cmdparse---cmdparse.o---libcmd.a
003e220c --- vty---vty.o---libvty.a
00499820 --- pSOS_qcv_broadcast---ksppc.o---os\libsys.a

```

The whole displayed content can be divided into six parts:

1. RROR:file function.map not found

The prompt information means that the system has not been installed the software function.map, which does not affect the system running.

If the version of the software function.map is not consistent with that of the switch, the system prompts that the version is not consistent.

2. Exception Type—Abnormal hex code plus abnormal name
3. BreakNum

It is the current abnormal number. It means the number of abnormalities that the system has since it is powered on in the latest time. It is followed by the time when the abnormality occurs.

4. Content of the register

The common content of the register is listed out.

5. Variable area

The content in the stack is listed out.

#### 6. Calling relationship of the number

If the map file is not installed on the system, only the function's address is displayed. If the map file is installed on the system, the corresponding function name, .o file name and .a file name are displayed

The calling relationship is from bottom to top.

### **3.2.23 show debug**

To display all the enabled debugging options of the switch, run the following command.

#### **show debug**

##### Parameters

None

##### Command Mode

EXEC

##### Example

```
switch# show debug
```

Crypto Subsystem:

Crypto Ipsec debugging is on

Crypto Isakmp debugging is on

Crypto Packet debugging is on

##### Related Command

**debug**

### **3.2.24 show logging**

To display the state of logging (syslog), run the following command.

#### **show logging**

##### Parameters

None

##### Command Mode

EXEC

##### Usage Guidelines

The command can be used to display the state of logging (syslog), including the login information about the console, monitor and syslog.

##### Example

```
switch# show logging
```

```
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
```

```
Console logging: level debugging, 12 messages logged
```

```
Monitor logging: level debugging, 0 messages logged
```

```
Buffer logging: level debugging, 4 messages logged
```

```
Trap logging: level informations, 0 message lines logged
```

```
Log Buffer (4096 bytes):
```

```
2000-1-4 00:30:11 Configured from console 0 by DEFAULT
```

```
2000-1-4 00:30:28 User DEFAULT enter privilege mode from console 0, level = 15
```

**Related Command**

```
clear logging
```

## Chapter 4 SSH Configuration Commands

### 4.1 SSH Configuration Commands

#### 4.1.1 *ip sshd enable*

Syntax

```
ip sshd enable
```

```
no ip sshd enable
```

Parameters

None

Default Value

Disabled

Usage Guidelines

The command can be used to generate the rsa encryption key and then monitor the connection to the ssh server. The process of generating encryption key is a process of consuming the calculation time. It takes one or two minutes.

Command Mode

Global configuration mode

Example

In the following example, the SSH service is generated.

```
switch_config#ip sshd enable
```

### 4.1.2 *ip sshd timeout*

#### Syntax

**ip sshd timeout** *time-length*

**no ip sshd timeout**

#### Parameters

Parameters	Description
<i>time-length</i>	<b>Maximum time from the establishment of connection to the authentication approval;Value range: 60-65535</b>

#### Default Value

180 seconds

#### Usage Guidelines

To prevent the illegal user from occupying the connection resources, the connections that are not approved will be shut down after the set duration is exceeded.

#### Command Mode

Global configuration mode

#### Example

In the following example, the timeout time is set to 360 seconds

```
switch_config#ip sshd timeout 360
```

### 4.1.3 *ip sshd auth-method*

#### Syntax

**ip sshd auth-method** *method*

**no ip sshd auth-method**

#### Parameters

Parameters	Description
<i>method</i>	<b>Sets authentication method list. The length of the authentication method's name is no more than 20 characters.</b>

#### Default Value

The default authentication method list is used.

#### Usage Guidelines

The ssh server uses the authentication method list of the login type.

#### Command Mode

Global configuration mode

### Example

In the following example, an auth-ssh authentication method list is configured and it is applied to the ssh server:

```
switch_config#aaa authentication login auth-ssh local switch_config#ip sshd auth-method
auth-ssh
```

#### 4.1.4 ip sshd access-class

##### Syntax

```
ip sshd access-class access-list
```

```
no ip sshd access-class
```

##### Parameters

Parameters	Description
<i>access-list</i>	<b>Standard IP access list</b> The length of the access list's name is no more than 20 characters.

##### Default Value

No access control list

##### Usage Guidelines

The command can be used to configure the access control list for the ssh server. Only the connections complying with the regulations in the access control list can be approved.

##### Command Mode

Global configuration mode

### Example

In the following example, an ssh-accesslist access control list is configured and applied in the ssh server:

```
switch_config# ip access-list standard ssh-accesslist
```

```
switch_config_std#deny 192.168.20.40
```

```
switch_config#ip sshd access-class ssh-accesslist
```

#### 4.1.5 ip sshd auth-retries

##### Syntax

```
ip sshd auth-retries times
```

```
no ip sshd auth-retries
```

##### Parameters

Parameters	Description
<i>times</i>	Maximum re-authentication times; Value range: 0-65535

### Default Value

6 times

### Usage Guidelines

The connection will be shut down when the re-authentication times exceeds the set times.

### Command Mode

Global configuration mode

### Example

In the following example, the maximum re-authentication times is set to five times:

```
switch_config#ip sshd auth-retries 5
```

#### 4.1.6 *ip sshd clear*

### Syntax

```
ip sshd clear ID
```

### Parameters

Parameters	Description
<i>ID</i>	Number of the SSH connection to the local device; Value range: 0-15

### Default Value

None

### Usage Guidelines

The command can be used to disable the incoming ssh connection with the specified number compulsorily. You can run the command `show ssh` to check the current incoming connection's number.

### Command Mode

Global configuration mode

### Example

In the following example, the No.0 incoming connection is mandatorily closed:

```
switch_config#ip sshd clear 0
```

#### 4.1.7 *ip sshd silence-period*

### Syntax

**ip sshd silence-period** *time-length*

**no ip sshd silence-period**

#### Parameters

Parameters	Description
<i>time-length</i>	Means the time of the silence, which ranges from 0 to 3600.

#### Default Value

60s

#### Usage Guidelines

The command can be used to set the login silence period. After the accumulated login failures exceed a certain threshold, the system regards that there exist attacks and disables the SSH service in a period of time, that is, the system enters the login silence period.

The silence period is set by the `ip sshd silence-period` command. The default silence period is 60 seconds. The allowable login failures are set by the `ip sshd auth-retries` command, whose default value is 6.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to set the silence period to 200 seconds.

```
switch_config#ip sshd silence-period 200
```

#### 4.1.8 ip sshd sftp

##### Syntax

**ip sshd sftp**

**no ip sshd sftp**

##### Parameters

None

##### Default Value

None

##### Usage Guidelines

The command can be used to enable the SFTP function. The SFTP function refers to the secure file transmission system based on SSH, of which the authentication procedure and data transmission are encrypted. Though it has low transmission efficiency, network security is highly improved.

##### Command Mode



Global configuration mode

### Example

The following example shows how to enable the SFTP function.

```
switch_config#ip sshd sftp
```

#### 4.1.9 *ip sshd save*

### Syntax

**ip sshd save**

**no ip sshd save**

### Parameters

None

### Default Value

None

### Usage Guidelines

The command can be used to save the initial key. When the SSH server is restarted, the key will be first read from the flash; if the key reading is successful, the recalculation of key will be avoided and the startup time will be shortened.

### Command Mode

Global configuration mode

### Example

The following example shows how to enable the key protection function.

```
switch_config#ip sshd save
```

#### 4.1.10 *ip sshd disable-aes*

### Syntax

**ip sshd disable-aes**

**no ip sshd disable-aes**

### Parameters

None

### Default Value

The AES encryption algorithm is forbidden.

### Usage Guidelines

The command can be used to decide whether to use the AES algorithm during the encryption algorithm negotiation. The AES algorithms such as aes128-cbc and aes256-cbc are not used by default.

### Command Mode

Global configuration mode

### Example

The following example shows how to disable the AES encryption algorithm.

```
switch_config#ip sshd disable-aes
```

### 4.1.11 ssh

#### Syntax

```
ssh -l userid -d destIP [-c {des|3des|blowfish}] [-o numberofpasswdprompts] [-p port] [-v {1|2}]
```

#### Parameters

Parameters	Description
<i>-l userid</i>	User account on the server
<i>-d destIP</i>	Destination IP address in the dotted decimal system
<i>-o numberofpasswdprompts</i>	Re-authentication times after the first authentication fails; Actual re-authentication times is the set value plus the smallest value set on the server. Its default value is three times. Value range: 0-65535
<i>-p port</i>	Port number that the server monitorsIts default value is 22. Value range: 0-65535
<i>-c {des 3des blowfish}</i>	Encryption algorithm used during communicationThe encryption algorithm is 3des by default.
<i>-v version</i>	Specified version number

#### Default Value

None

#### Usage Guidelines

The command can be used to create a connection with the remote ssh server.

### Command Mode

Privileged mode

### Example

The following example shows how a connection with the ssh server whose IP address is 192.168.20.41 is created. The account is z mz and the encryption algorithm is blowfish:

```
switch#ip ssh -l z mz -d 192.168.20.41 -c blowfish
```

#### 4.1.12 *show ssh*

##### Syntax

**show ssh**

##### Parameters

None

##### Default Value

None

##### Usage Guidelines

The command can be used to display the sessions on the ssh server.

##### Command Mode

Privileged mode

##### Example

The following example shows the sessions on the ssh server:

```
switch#show ssh
```

#### 4.1.13 *show ip sshd*

##### Syntax

**show ip sshd**

##### Parameters

None

##### Default Value

None

##### Usage Guidelines

The command can be used to display the current state of the ssh server.

##### Command Mode

Privileged mode

##### Example

In the following example, the current state of the ssh server is displayed:

```
switch#show ip sshd
```

## Chapter 5 Network Management Configuration

### 5.1 SNMP Commands

SNMP commands are listed below:

- snmp-server community
- snmp-server contact
- snmp-server engine ID local
- snmp-server group
- snmp-server host/hostv6
- snmp-server location
- snmp-server packet size
- snmp-server queue-length
- snmp-server trap-source
- snmp-server trap-timeout
- snmp-server user
- snmp-server view
- snmp-server source-addr
- snmp-sever udp-port
- snmp-server encryption
- Snmp-server trap-add-hostname
- snmp-server trap-logs
- snmp-server set-snmp-dos-max
- snmp-server keep-alive
- snmp-server nocode
- snmp-server event-id
- snmp-server getbulk-timeout
- snmp-server getbulk-delay
- show snmp
- debug snmp

#### 5.1.1 *snmp-server community*

Syntax

To set the community access string of the accessible SNMP protocol, run **snmp-server community** in global configuration mode. To delete the specified community character string, run the no form of this command.

```
snmp-server community [0|7] string [view view-name] [ro | rw] [word]
```

```
no snmp-server community string
```

```
no snmp-server community
```

#### Parameters

Parameters	Description
<i>0</i>	Sets the community string of the text.
<i>7</i>	Sets the encrypted public string of the text.
<i>string</i>	Means the community string of the accessible SNMP protocol, which is similar to the password.
<i>view</i> <i>view-name</i>	(optional) stands for the previously defined view's name. In this view, the MIB objects, which are effective to the community, are defined.
<i>ro</i>	(Optional) Designates the read-only permission. Those authorized workstations can only read the MIB objects.
<i>rw</i>	(Optional) Designates the read-write permission. Those authorized workstations can read and modify the MIB objects.
<i>word</i>	(optional) Specifies the name of IP ACL of the SNMP proxy, which can be accessed by the community string.

#### Default Value

By default, the SNMP community string allows the read-only permission to all objects.

#### Command Mode

Global configuration mode

#### Usage Guidelines

The following command shows how to delete a designated community.

```
no snmp-server community string
```

The following command shows how to delete all communities.

```
no snmp-server community
```

#### Example

The following example shows how to distribute the “comaccess” string to SNMP, allow the read-only access and designate IP ACL to use the community string.

```
snmp-server community comaccess ro allowed
```

The following example shows how to distribute the “mgr” string to SNMP, allow to read and write the objects in the Restricted view

```
snmp-server community mgr view restricted rw
```

The following example shows how to delete the “comaccess” community.

```
no snmp-server community comaccess
```

Related Command

```
access-list
```

```
snmp-server view
```

### 5.1.2 *snmp-server contact*

Syntax

To set the information about the contact person in a management node, run `snmp-server contact text`. To delete the contact information, use the `no` form of this command.

```
snmp-server contact text
```

```
no snmp-server contact
```

Parameters

Parameters	Description
<i>text</i>	Means the string of the information about the contact person.

Default Value

The information about contact person is not set.

Command Mode

Global configuration mode

Usage Guidelines

It corresponds to the `sysContact` of the MIB variable in the System group.

Example

The following example shows the information about the contact person in a node.

```
snmp-server contact Dial_System_Operator_at_beeper_#_27345
```

### 5.1.3 *snmp-server engineID local*

Syntax

To configure the local agent SNMP engine ID, run the following command in the global configuration mode. To return to the default setting, use the `no` form of this command.

```
snmp-server engineID local engineID
```

```
no snmp-server engineID local engineID
```

Parameters

Parameters	Description
------------	-------------

<i>engineID</i>	<b>SNMP engine ID.</b>
-----------------	------------------------

### Default Value

SNMP engine ID is not set.

### Command Mode

Global configuration mode

### Usage Guidelines

The command is used to configure the SNMP engine ID of the local agent.

### Example

```
snmp-server engineID local 8000cf80300e00f3f56e3
```

## 5.1.4 snmp-server group

### Syntax

To create or update a snmp-server group in global configuration mode, run the following first command; to cancel this SNMP group, run the following second command. Format of the command is as follows:

```
snmp-server group [groupname { v3 [auth | noauth | priv]}][read readview][write writeview] [notify notifyview] [access access-list]
```

### Parameters

Parameters	Description
<i>groupname</i>	<b>Stands for the name of the created or modified SNMP group.</b>
<i>v3</i>	<b>Means the version ID of the SNMP protocol.</b>
<i>auth noauth priv</i>	<b>Stands for the lowest security level of users in the SNMPv3 group.</b>
<i>readview</i>	<b>Means the access permission of GET operations, which is defined by the view.</b>
<i>writeview</i>	<b>Means the access permission of SET operations, which is defined by the view.</b>
<i>notifyview</i>	<b>Stands for the access permission during the transmission of Trap packets, which is defined by the view.</b>
<i>access-list</i>	<b>Allows users in the SNMP group to get through the IP access control list.</b>

### Default value

The readview allows all leaves of the Internet sub-tree to be accessed.

### Command mode:

Global configuration mode

### Usage Guidelines

The SNMP group is used to designate the access permission of the users in this group.

### Example

In the following example, an SNMP group is set and named as setter, the version ID of the SNMP protocol is 3, the security level is authentication and encryption, and the view that is accessed by the set operation is v-write.

```
snmp-server group setter v3 priv write v-write
```

### Related Command

```
snmp-server view snmp-server user
```

## 5.1.5 snmp-server [host|hostv6]

### Syntax

To specify the receiver of SNMP trap operation, run the first of the following commands in global configuration mode. To cancel this designated host, run the following second command.

```
snmp-server host|hostv6 host [udp-port port-num] [permit|deny event-id] {{version [v1 | v2c | v3] | [informs | traps] | [auth | noauth]}} community-string/user [authentication | configure | snmp]
```

```
no snmp-server host host community-string
```

### Parameters

Parameters	Description
<i>host hostv6</i>	Sets the IPv4 or IPv6 trap host.
<i>host</i>	Means the host's name or the address of the Internet. uses ipv4 address in host uses ipv6 address in hostv6
<b>[udp-port</b> <i>port-num</i> ]	(Optional) Specifies the ID of the UDP port, which transmits the traps.
<b>[permit deny</b> <i>event-id</i> ]	(Optional) Allows or blocks to transmit a designated event.
<b>{version [v1 v2c v3]}</b>	(Optional) Means the version ID of the SNMP protocol, which is used to transmit traps.
<b>[informs   traps]</b>	(Optional) Specifies the type of trap for version V2C. Informs: means the type of trap is "informs". Traps: means the type of trap is "traps".
<b>[auth   noauth]</b>	Specifies the trap authentication mode for version V3. auth: authentication noauth: non-authentication
<i>community-string/user</i>	Means a community string in version 1 and version 2c which is similar to the password and sent with the trap operations or means the username in version 3.
<b>[authentication   configure   snmp]</b>	(optional) if no trap is designated, all generated traps will be sent to the host. authentication: allows to transmit those authentication-error traps. configure: allows to transmit the SNMP-configure traps. snmp: allows to transmit the SNMP traps.



## Default Value

This command is invalid in default settings. That is to say, no trap will be sent by default. If no command with any key word is entered, all traps with v1 standard are not sent by default.

## Command Mode

Global configuration mode

## Usage Guidelines

If this command is not entered, the traps will not be sent. In order to enable a switch to send the SNMP traps,

you must run `snmp-server host`. If the keyword “trap-type” is not contained in this command, all kinds of traps of this host will be activated. If the keyword “trap-type” is contained in this command, all trap types related with this keyword are activated. You can specify multiple trap types in this command for each host.

If you designate multiple `snmp-server host` commands on the same host, the SNMP trap messages that are sent to the host will be decided by the community string and the trap type filtration in this command. (Only one trap type can be configured for a same host and a same community string).

The availability of the trap-type option depends on the switch type and the attributes of routing software, which is supported by this switch.

## Example

The following example shows how to transmit the RFC1157-defined SNMP traps to host 10.20.30.40. The community string is defined as comaccess.

```
snmp-server host 10.20.30.40 comaccess snmp
```

The following example shows that the switch uses the public community string to send all types of traps to host 10.20.30.40.

```
snmp-server host 10.20.30.40 public
```

The following example shows that only the authentication traps are effective and can be sent to host bob.

```
snmp-server host bob public authentication
```

## Related Command

**snmp-server queue-length**

**snmp-server trap-source**

**snmp-server trap-timeout**

**snmp-server event-id**

**snmp-server user**

### 5.1.6 *snmp-server location*

#### Syntax

To set the location string of a node, run the first one of the following two commands in global configuration mode. To cancel this designated host, run the following second command.

**snmp-server location text**

**no snmp-server location**

#### Parameters

Parameters	Description
<i>text</i>	The location string of a node is not set by default.

#### Default Value

The location string of a node is not set by default.

#### Command Mode

Global configuration mode

#### Usage Guidelines

It corresponds to the sysLocation of the MIB variable in the System group.

#### Example

The following example shows how to define the actual location of a switch.

```
snmp-server location Building_3/Room_214
```

#### Related Command

**snmp-server contact**

### 5.1.7 *snmp-server packetsize*

#### Syntax

To define the maximum size of the SNMP packet when the SNMP server receives requests or responds, run the following first command in global configuration mode.

**snmp-server packetsize *byte-count***

**no snmp-server packetsize**

#### Parameters

Parameters	Description
<i>byte-count</i>	Stands for the integer bytes between 484 and 17940. The default value is 3000 bytes.

#### Default Value

3000 bytes

### Command Mode

Global configuration mode

### Usage Guidelines

It corresponds to the sysLocation of the MIB variable in the System group.

### Example

The following example shows how to set up a filter to filter those packets whose maximum length is 1024 bytes.

```
snmp-server packetsize 1024
```

### Related Command

```
snmp-server queue-length
```

#### 5.1.8 *snmp-server queue-length*

### Syntax

To set the queue length for each trap host, run the following first command in global configuration mode.

```
snmp-server queue-length length
```

```
no snmp-server queue-length
```

### Parameters

Parameters	Description
<i>length</i>	<b>Stands for the number of trap events which can be saved in the queue (1-1000).</b>

### Default Value

10 trap events.

### Command Mode

Global configuration mode

### Usage Guidelines

This command is used to set the queue length for each trap host. Once the trap messages are successfully transmitted, the switch will empty the queue.

### Example

The following example shows how to set up a message queue which can capture four events.

```
snmp-server queue-length 4
```

### Related Command

**snmp-server packetsize****5.1.9 snmp-server trap-source****Syntax**

To designate an interface to be the source address of all traps, run the following first command in global configuration mode. To cancel this interface, run the following second command.

**snmp-server trap-source interface**

**no snmp-server trap-source**

**Parameters**

Parameters	Description
<i>interface</i>	<b>Stands for the interface where SNMP traps generate. The parameters include the interface type and interface ID of the syntax mode of specific platform.</b>

**Default Value**

The interface is not designated.

**Command Mode**

Global configuration mode

**Usage Guidelines**

When the SNMP server sends out a SNMP trap on whichever interface, the SNMP trap shall carry a trap address. If you want to use the trap address for tracking, you can use this command.

**Example**

The following example shows how to designate interface vlan1 as the source address of all traps.

```
snmp-server trap-source vlan1
```

**Related Command**

**snmp-server queue-length**

**snmp-server host**

**5.1.10 snmp-server trap-timeout****Syntax**

To set the timeout value of retransmitting traps, run the following first command in global configuration mode. To return to the default setting, use the no form of this command.

**snmp-server trap-timeout seconds**

**no snmp-server trap-timeout**

## Parameters

Parameters	Description
<i>seconds</i>	Means an interval for retransmitting traps, whose unit is second (1-1000).

## Default Value

30 seconds

## Command Mode

Global configuration mode

## Usage Guidelines

Before switch software tries to send traps, it is used to look for the route of destination address. If no routes exists, traps will be saved in the retransmission queue. The server trap-timeout command decides the retransmission interval.

## Example

The following example shows how to set the retransmission interval to 20 seconds:

```
snmp-server trap-timeout 20
```

## Related Command

```
snmp-server host
```

```
snmp-server queue-length
```

*5.1.11 snmp-server user*

## Syntax

To create or update an **snmp-server user** in global configuration mode, run the following first command; to cancel this SNMP user, run the following second command. If the remote parameter is designated, a remote user will be configured; when a remote user is configured, the SNMP engine ID that corresponds to the IP address of this management station must exist. Format of the command is as follows:

```
snmp-server user username groupname { v3 [ encrypted | auth ] [ md5 | sha ]  
auth-password }
```

## Parameters

Parameters	Description
<i>username</i>	Stands for the name of the created or modified SNMP user.
<i>groupname</i>	Stands for the group where the user is.
<i>v3</i>	Stands for the SNMP version.
[ <i>encrypted</i>   <i>auth</i> ]	Encryption type: <b>encrypted</b> : Encrypted: packet encryption <b>auth</b> : packet authentication

<i>[ md5   sha ]</i>	Means the method of encryption authentication.
<i>auth-password</i>	Stands for the authentication password of the user. If this password is localized, it will be used as the authentication key and the encryption key of SNMPv3.

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

This command is used to set the username and the password.

### Example

In the following example, an SNMP user is created, whose name is set-user and which belongs to setter, the version of the SNMP protocol is version 3, the security level is authentication and encryption, the password is 12345678, and MD5 is used as the hash algorithm.

```
snmp-server user set-user setter v3 encrypted auth md5 12345678
```

### Related Command

snmp-server view

snmp-server group

#### 5.1.12 snmp-server view

### Syntax

To create or update a MIB view, run the first one of the following two commands in global configuration mode. To cancel a view in the SNMP server, run the second one of the following two commands.

```
snmp-server view view-name oid-tree {included | excluded}
```

```
no snmp-server view view-name
```

### Parameters

Parameters	Description
<i>view-name</i>	Updates or creates the label of a view.
<i>oid-tree</i>	Means the object IDs of the ASN.1 sub-tree that must be contained or excepted from a view. The identifier sub-tree is used to designate a numeral-contained string, e.g., 1.3.6.2.4 or a system sub-tree. The sub-tree name can be found in all MIB trees. Means the view type. The parameter "included" or "excluded" must be specified.
<i>included   excluded</i>	Means the view type. The parameter "included" or "excluded" must be specified.

<i>[ encrypted   auth ]</i>	<b>Encryption type:</b> <b>encrypted: Encrypted: packet encryption</b> <b>auth: packet authentication</b>
<i>[ md5   sha ]</i>	<b>Means the method of encryption authentication.</b>
<i>auth-password</i>	<b>Stands for the authentication password of the user. If this password is localized, it will be used as the authentication key and the encryption key of SNMPv3.</b>

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

If other SNMP commands need a view as a parameter, you can use this command to create a view. By default, you need not define the view and you can see all the views, equivalent to Cisco-predefined everything views. The command is used to define the object the view sees.

**SNMP MIB with OID you can find on [data.itmag.uz](http://data.itmag.uz) website in Switch directory.**

### Example

The following example shows how to create the views of all objects in the MIB-II sub-tree.

```
snmp-server view mib2 mib-2 included
```

The following example shows how to create the views of all objects, including those objects in the system group.

```
snmp-server view phred system included
```

The following example shows how to create the views of all objects that includes the objects in the system groups but excludes the objects in system7(sysServices.7) and interface 1.

```
snmp-server view agon system included
```

```
snmp-server view agon system.7 excluded
```

### Related Command

```
snmp-server community
```

#### 5.1.13 *snmp-server source-addr*

### Syntax

To specify a source address for answering all SNMP requests, run the second one of the following two commands in global configuration mode. To cancel this interface, run the following second command.

```
snmp-server source-addr a.b.c.d
```

```
no snmp-server source-addr
```

## Parameters

Parameters	Description
<i>a.b.c.d</i>	Means the source address for all SNMP requests to be answered. Designate the source address of SNMP generating packets. The parameter is the IP address the device has set.

## Default Value

The default source address is the nearest routing address.

## Command Mode

Global configuration mode

## Usage Guidelines

When the SNMP server transmits an SNMP request, you can run this command to designate a special source address.

## Example

The following example shows how to designate the IP address “1.2.3.4” of the designated interface as the source address of all SNMP packets.

```
snmp-server source-addr 1.2.3.4
```

## Related Command

None

### 5.1.14 *snmp-server udp-port*

## Syntax

To specify the port number for the SNMP agent to receive packets, run the following first command in global configuration mode.

```
snmp-server udp-port portnum
```

```
no snmp-server udp-port
```

## Parameters

Parameters	Description
<i>udp-port</i>	Stands for the ID of the destination port to which SNMP traps are sent, which cannot be a command port ID.

## Default Value

It is the listening port of SNMP agent by default, that is, port 162.

## Command Mode

Global configuration mode



## Usage Guidelines

The SNMP agent will listen to this port when SNMP server transmits SNMP packets.

## Example

The following example shows how to specify the listening port of SNMP agent to port 1234.

```
snmp-server udp-port 1234
```

## Related Command

None

### *5.1.15 snmp-server encryption*

#### Syntax

To display the configured SNMP community, the SHA encryption password and the MD5 encryption password, run `snmp-server encryption` in global mode. This command is a once-for-all command, which cannot be saved or canceled by its negative form. Format of the command is as follows:

#### **snmp-server encryption**

#### Parameters

None

#### Default Value

The default settings is to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text.

#### Command Mode

Global configuration mode

#### Usage Guidelines

This command is used to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text. In this way, the security of the password is guaranteed.

#### Example

The following example shows how to show in the plain text the SNMP community, the SHA encryption password and the MD5 encryption password, which are set for host 90.0.0.3.

```
snmp-server encryption
```

#### Related Command

```
snmp-server community snmp-server user
```

### *5.1.16 snmp-server trap-add-hostname*

#### Syntax

To add the host name to the binding variable when SNMP sends traps, run the first one of the following two commands.

```
snmp-server trap-add-hostname
```

```
no snmp-server trap-add-hostname
```

#### Parameters

None

#### Default Value

The hostname is not added to the binding variable list when traps are being transmitted.

#### Command Mode

Global configuration mode

#### Usage Guidelines

This command is a great help in some cases when the NMS needs to locate which host sends these traps.

#### Example

The following example shows how to enable the trap-to-hostname binding function.

```
Router_config# snmp-server trap-add-hostname
```

### *5.1.17 snmp-server trap-logs*

#### Syntax

To write the trap transmission records into logs, run the first one of the following two commands.

```
snmp-server trap-logs
```

```
no snmp-server      trap-logs
```

#### Parameters

The command has no parameters or keywords.

#### Default Value

The transmitted traps are not recorded by default.

#### Command Mode

Global configuration mode

#### Usage Guidelines

After this function is enabled, the trap transmission records of a device can be sent to the log server and then you can know more about the running state of the device.

#### Example

The following example shows how to the trap logs function. Router\_config# snmp-server trap-logs

### 5.1.18 snmp-server set-snmp-dos-max

#### Syntax

To set the incorrect community login retry times in five minutes on the SNMP server, run the first one of the following two commands.

```
snmp-server set-snmp-dos-max retry times
```

```
no snmp-server set-snmp-dos-max
```

#### Parameters

The retry times parameter stands for the login times for a user to conduct the incorrect community login in five minutes.

#### Default Value

The incorrect community login times is not limited.

#### Command Mode

Global configuration mode

#### Usage Guidelines

This command can be used to prevent those SNMP host from guessing the device's community viciously, which lessening unnecessary CPU consumption of the device.

#### Example

The following example shows how to enable the refuse service function and set the max trying times to 10 in five minutes.

```
Router_config# snmp-server set-snmp-dos-max 10
```

### 5.1.19 snmp-server keep-alive

#### Syntax

To set the timely sending heartbeat trap, run snmp-server keep-alive in global configuration mode. The time interval is times.

```
snmp-server keep-alive times
```

```
no snmp-server keep-alive
```

#### Parameters

Parameters	Description
<i>times</i>	The time interval of heartbeat trap.

#### Default Value

The command is not configured by default.

## Command Mode

Global configuration mode

## Usage Guidelines

The command must be used with `snmp-server host`.

## Example

The following example shows how to set the device sending heartbeat trap every 3 seconds.

```
snmp-server keep-alive 3
```

## Related Command

```
snmp-server host
```

```
snmp-server hostv6
```

### 5.1.20 *snmp-server nocode*

## Syntax

To set the information about the management node (the unique identifier of the device), run `snmp-server nocode text`. To delete the identifier information, use the `no` form of this command.

```
snmp-server nocode text
```

```
no snmp-server nocode
```

## Parameters

Parameters	Description
<i>text</i>	<b>Sets the information about the management node (the unique identifier of the device).</b>

## Default Value

The node identifier is not set.

## Command Mode

Global configuration mode

## Usage Guidelines

The command is corresponding to the `snmp private` MIB variable.

## Example

The following example shows the information about the node.

```
snmp-server nocode Dial_System_Operator_at_beeper_#_27345
```

### 5.1.21 *snmp-server event-id*

## Syntax

To create and set event list, run command `snmp-server event-id` in the global configuration mode. To delete the event list, use the `no` form of this command.

**snmp-server event-id** *number* **trap-oid** *oid*

**no snmp-server event-id** *number* [**trap-oid** *oid*]

#### Parameters

Parameters	Description
<i>number</i>	<b>The only identifier of event-id.</b>
<i>oid</i>	<b>trap OID included in event-id.</b>

#### Default Value

The event list information is not set by default.

#### Command Mode

Global configuration mode

#### Usage Guidelines

The command is used in host configuration.

#### Example

The following example shows how to set trap whose trap OID is 1.2.3.4.5 to event ID 1.

```
snmp-server event-id 1 trap-oid 1.2.3.4.5
```

### 5.1.22 snmp-server getbulk-timeout

#### Syntax

To set the timeout of processing getbulk request, run command `snmp-server getbulk-timeout` in the global configuration mode. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly. To delete the configuration, use the `no` form of this command.

**snmp-server getbulk-timeout** *seconds*

**no snmp-server getbulk-timeout**

#### Parameters

Parameters	Description
<i>seconds</i>	<b>The timeout of processing getbulk request.</b>

#### Default Value

The timeout of processing getbulk request is not set by default.

#### Command Mode

Global configuration mode

### Usage Guidelines

The command is used to set the timeout of processing getbulk request. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly.

### Example

The following example shows how to set getbulk-timeout and set the timeout to 5 seconds.

```
snmp-server getbulk-timeout 5
```

### 5.1.23 snmp-server getbulk-delay

#### Syntax

To set getbulk-delay time to prevent snmp occupying excessive cpu when snmp agent processing getbulk request, run command snmp-server getbulk-delay in the global configuration mode. The unit is 0.01 seconds. To delete the configuration, use the no form of this command.

```
snmp-server getbulk-delay ticks
```

```
no snmp-server getbulk-delay
```

#### Parameters

Parameters	Description
<i>ticks</i>	<b>Sets CPU interval time in processing getbulk request. The unit is 0.01s.</b>

#### Default Value

The command is not configured when CPU is processing getbulk request in full load.

#### Command Mode

Global configuration mode

### Usage Guidelines

The command is used to set getbulk-delay time to prevent snmp from occupying excessive cpu when snmp agent processing getbulk request. The unit is 0.01s.

### Example

The following example shows how snmp agent pauses one ticks when getting one result in configuring getbulk.

```
snmp-server getbulk-delay 1
```

### 5.1.24 show snmp

#### Syntax

To monitor SNMP input and output statistics, including illegal community character strings, the number of errors and request variables, run command `show snmp`. To show SNMP engine information, run command `show snmp engineID`. To show SNMP trap host information, run command `show snmp host`. To show SNMP view information, run command **`show snmp view`**. To show snmp mibs registration information, run command **`show snmp mibs`**. To show snmp group information, run command `show snmp group`. To show SNMP user information, run command `show snmp user`.

**`show snmp [engineID | host | view | mibs | group|user]`**

#### Parameters

Parameters	Description
<i>engineID</i>	Shows SNMP engine information.
<i>host</i>	Shows SNMP trap host information.
<i>View</i>	Shows SNMP view information.
<i>mibs</i>	Shows SNMP MIB registration information.
<i>group</i>	Shows SNMP group information.
<i>user</i>	Shows SNMP user information.

#### Default Value

None

#### Command Mode

EXEC and global configuration mode

#### Usage Guidelines

The command **`show snmp`** is used to show SNMP input and output statistics.

To show SNMP engine information, run command `show snmp engine ID`.

The command **`show snmp host`** is used to show SNMP trap host information.

The command **`show snmp view`** is used to show SNMP view information.

The command **`show snmp mibs`** is used to show mib registration information.

The command **`show snmp group`** is used to show SNMP group information.

The command **`show snmp user`** is used to show SNMP user information.

#### Example

The following example shows how to list SNMP input and output statistics.

```
#show snmp
```

```
37 SNMP packets input
```

```
0 Bad SNMP version errors
```

4 Unknown community name

0 Illegal operation for community name supplied

0 Snmp encoding errors

24 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

28 Get-next PDUs

0 Set-request PDUs

78 SNMP packets output

0 Too big errors (Maximum packet size 1500) 0 No such name errors

0 Bad values errors 0 General errors

24 Get-response PDUs PDUs

13 SNMP trap PDUs

Meaning of statistics information of SNMP Agent receiving and sending packets:

Displayed Information	Meaning
Unknown community name	Unknown community name
Illegal operation for community name supplied	Illegal operation
Encoding errors	Encoding errors
Get-request PDUs	Get-request PDUs
Get-next PDUs	Get-next PDUs
Set-request PDUs	Set-request PDUs
Too big errors	The packets are too big to generate response packets.
No such name errors	No such name errors
<i>Bad values errors</i>	<b>Bad values errors</b>
<i>General errors</i>	<b>General errors</b>
<i>Get-response PDUs</i>	<b>Get-response PDUs</b>
<i>Trap PDUs</i>	<b>SNMP trap packets</b>

The following example shows how to show SNMP trap host information.

```
#show snmp host
```

```
Notification host: 192.2.2.1      udp-port: 162      type: trap user: public      security
model: v1
```

The following example shows how to show SNMP view information.



```
#show snmp view
```

```
mib2 mib-2 - included permanent active
```

### Related Command

**snmp-server host**

**snmp-server view**

### 5.1.25 debug snmp

#### Syntax

To show SNMP event, packet sending and receiving process and error information, run command **debug snmp**.

```
debug snmp [ error | event | packet ]
```

To stop showing the information, run command **no debug snmp**.

**no debug snmp**

#### Parameters

Parameters	Description
<i>error</i>	Enable the debug OLT of SNMP error information.
<i>event</i>	Enable the debug OLT of SNMP event information.
<i>packet</i>	Enable the debug OLT of SNMP input/output packets.

#### Command Mode

EXEC

#### Usage Guidelines

The command is used to enable SNMP debug information switch and output SNMP event, information of sending and receiving packets, which is helpful for SNMP fault diagnosis.

#### Example

The following example shows how to debug SNMP receiving and sending packets.

```
switch#debug snmp packet
```

```
Received 49 bytes from 192.168.0.29:1433
```

```
0000: 30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0 0...-....public.
```

```
0016: 82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00 .....}.....0..
```

```
0032: 10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 .0.....+.....
```

```
0048: 00 .
```

```
Sending 52 bytes to 192.168.0.29:1433
```

```
0000: 30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2 0..0....public.
0016: 82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00 ..!..}.....0..
0032: 13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43 .0.....+ C
0048: 03 00 F4 36 ...6
```

Received 51 bytes from 1192.168.0.29:1434

```
0000: 30 82 00 2F 02 01 00 04 06 70 75 62 6C 69 63 A0 0../ public.
0016: 82 00 20 02 02 6B 84 02 01 00 02 01 00 30 82 00 .. .k.....0..
0032: 12 30 82 00 0E 06 0A 2B 06 01 02 01 02 02 01 02 .0.....+.....
0048: 01 05 00 ...
```

Sending 62 bytes to 192.168.0.29:1434

```
0000: 30 82 00 3A 02 01 00 04 06 70 75 62 6C 69 63 A2 0...-....public.
0016: 82 00 2B 02 02 6B 84 02 01 00 02 01 00 30 82 00 ..+.k.....0..
0032: 1D 30 82 00 19 06 0A 2B 06 01 02 01 02 02 01 02 .0.....+.....
0048: 01 04 0B 45 74 68 65 72 6E 65 74 30 2F 31 ...Ethernet0/1
```

Domain	Description
<i>Received</i>	<b>Stands for SNMP receiving packets</b>
<i>192.168.0.29</i>	<b>Stands for source IP address</b>
<i>1433</i>	<b>Stands for source address port number</b>
<i>51 bytes</i>	<b>Stands for length of the receiving packets</b>
<i>30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0 82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00 10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 00</i>	<b>Stands for packets after SNMP ASN encoding</b>
<i>0...-.... public. .....}.....0.. .0.....+..... .</i>	<b>Stands for ASCII character of receiving packets. "." means not in the range of ASCII character.</b>
<i>sending</i>	<b>SNMP sending packets</b>
<i>192.168.0.29</i>	<b>Stands for the destination IP address</b>
<i>1433</i>	<b>Stands for the source address port number</b>
<i>52 bytes</i>	<b>Stands for the length of sending and receiving packets</b>
<i>30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2 82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00 13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43 03 00 F4 36</i>	<b>Stands for packets after SNMP ASN encoding</b>
<i>0..0....public. ..!..}.....0.. .0.....+....C</i>	<b>Stands for ASCII character of sending and receiving packets. "."</b>

...6	means not in the range of ASCII character.
------	--

The following example shows how to debug SNMP events.

```
switch#debug snmp event
Received SNMP packet(s) from 192.2.2.51
SNMP: GETNEXT request
-- ip.ipReasmFails.0
SNMP: Response
>> ip.ipFragOKs.0 = 1
Received SNMP packet(s) from 192.2.2.51
SNMP: GETNEXT request
-- ip.ipFragOKs.0
SNMP: Response
>> ip.ipFragFails.0 = 0
Received SNMP packet(s) from 192.2.2.51
SNMP: GETNEXT request
-- ip.ipFragFails.0
SNMP: Response
>> ip.ipFragCreates.0 = 2
```

Domain	Description
<i>SNMP</i>	Stands for the current debug SNMP protocol.
<i>GETNEXT request</i>	SNMP getnext request
<i>RESPONSE</i>	SNMP response
--	Stands for receiving packets
>>	Transmitting packets
<i>ip.ipReasmFails.0</i>	Stands for MIB OID of access request
<i>ip.ipFragOKs.0 = 1</i>	Stands for being accessed MIB OID and the return value

## 5.2 RMON Configuration Commands

RMON configuration commands include:

- rmon alarm
- rmon event

- rmon collection stat
- rmon collection history
- show rmon

### 5.2.1 rmon alarm

#### Syntax

To configure a rmon alarm entry, run the following command.

```
rmon alarm index variable interval {absolute | delta} rising-threshold value
[eventnumber] falling-threshold value [eventnumber] [repeat] [owner string]
```

#### Parameters

Parameters	Description
<i>index</i>	Stands for the index of the event table Value range: 1-65535
<i>variable</i>	Stands for the object needs to be monitored. Value range: oid of the monitored object.
<i>interval</i>	Stands for the sampling interval Value range: 1~2147483647
<i>value</i>	Stands for the alarm threshold Value range: -2147483648~ 2147483647.
<i>eventnumber</i>	Stands for the event index generated after reaching the threshold. Value range: 1~65535.
<i>repeat</i>	Stands for the repeat trigger event.
<i>string</i>	Stands for the owner description information Value range: the length of the character string is 1~31.

#### Default Value

eventnumber is not set by default.

repeat is not set by default.

#### Usage Guidelines

The command is used to monitor the value of specified object. The certain event will be triggered when the value exceeds the threshold.

#### Example

The following example shows how to set an alarm entry to monitor the object ifInOctets.2 and the sampling interval is 10. When the sampling interval increases more than 15, the event 1 will be triggered. When the sampling interval decreases more than 25, the event 2 will be triggered.

```
rmon alarm 1 1.3.6.1.2.1.2.2.1.10.2 10 absolute rising-threshold 15 1 falling-threshold 25 2
repeat owner switch
```

### 5.2.2 rmon event

#### Syntax

To configure a rmon event entry, run the following command.

```
rmon event index [description des-string] [log] [owner owner-string] [trap community]
[ifctrl interface]
```

#### Parameters

Parameters	Description
<i>index</i>	Stands for the index of the event table Value range: 1-65535
<i>des-string</i>	Stands for the event description character string. Value range: 1~127.
<i>owner-string</i>	Stands for the owner character string. Value range: 1~31.
<i>community</i>	Stands for the community name when generating trap. Value range: 1~31.
<i>interface</i>	Stands for the shutdown port that the event controls.

#### Default Value

None

#### Usage Guidelines

The command is used to set a rmon event entry. It is used for alarm.

#### Example

The following example shows to set one rmon event entry to 6 and the description character string to example; add one item in the log entry when triggering the event and generates trap with public as the community name.

```
rmon event 6 log trap public description example owner switch
```

### 5.2.3 rmon collection stats

#### Syntax

To set rmon statistics function, run the following command.

```
rmon collection stats index [owner string]
```

#### Parameters

Parameters	Description
<i>index</i>	Stands for the index of the statistics entry. Value range: 1~65535.
<i>string</i>	Stands for the owner character string. Value range: the length of the character string is 1~31.

#### Default Value

None

#### Usage Guidelines

The command must be configured in the interface mode.

### Example

The following example shows how to enable the statistics function on gigabit Ethernet interface g0/1.

```
int g0/1
rmon collection stats 2 owner switch
```

### 5.2.4 rmon collection history

#### Syntax

To configure a history control entry, run the following command.

```
rmon collection history index [buckets bucket-number] [interval second] [owner
owner-name]
```

#### Parameters

Parameters	Description
<i>index</i>	<b>index Value range: 1-65535</b>
<i>bucket-number</i>	<b>The entry of all history record control entries nearest to the bucket-number need to be reserved. Value range: 1~65535.</b>
<i>second</i>	<b>Stands for the time interval. Value range: 1~3600.</b>
<i>owner-name</i>	<b>Stands for the owner character string. Value range: the length of the character string is 1~31.</b>

#### Default Value

The default bucket-number is 50 and the default second is 1800.

#### Usage Guidelines

The command is used to configure in the interface mode. It is used for adding one entry to the history control table.

### Example

The following example shows how to add the history control entry on the gigabit Ethernet interface g0/1 and save the statistics of latest 20 time intervals.(Each time interval is 10 seconds.)

```
int g0/1
rmon collection history 2 buckets 20 interval 10 owner switch
```

### 5.2.5 show rmon

#### Syntax

To show rmon configuration, run the following command.

**show rmon [alarm] [event] [statistics] [history]**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

The command is used to show rmon configuration.

#### Example

The following example shows how to show rmon configuration, run the following command.

```
show rmon
```

## Chapter 6 AAA Configuration Commands

This Chapter describes the commands used for configuring the AAA authentication method. AAA authentication commands can be classified into authentication, authorization, accounting and local account policy configuration commands. Learn more in following sections.

### *6.1 Authentication Configuration Commands*

This section describes the commands for configuring authentication methods. Authentication defines the access right of the users before they are allowed to access the network and network services.

Please refer to “Configuring Authentication” for information on how to use the AAA method to configure the authentication. Please refer to the last part to review the examples configured by the commands in this Chapter.

Authentication Configuration Commands include:

- aaa authentication banner
- aaa authentication fail-message
- aaa authentication username-prompt
- aaa authentication password-prompt
- aaa authentication dot1x
- aaa authentication enable default
- aaa authentication login
- aaa group server
- server
- debug aaa authentication
- enable password

- enable(enter)
- service password-encryption

### 6.1.1 aaa authentication banner

#### Syntax

To configure a personal banner, run `aaa authentication banner` in global mode. To delete a personal banner, run `no aaa authentication banner`.

**aaa authentication banner** *delimiter string delimiter*

**no aaa authentication banner**

#### Parameters

Parameters	Description
<i>delimiter string</i> <i>delimiter</i>	<b>To-be-displayed text string when the user logs in; The delimiter parameter stands for the delimiter which adopts double quotation masks.</b>

#### Default Value

If you do not define the login banner, the system will display the following default banner:  
User Access Verification

#### Command Mode

Global configuration mode

#### Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the string, meaning the banner ends.

#### Example

The following example shows that the banner is modified to “Welcome to AACOM system” when logging on:

```
aaa authentication banner "Welcome to system!"
```

#### Related Command

```
aaa authentication fail-message
```

### 6.1.2 aaa authentication fail-message

#### Syntax

To configure a personal banner when login fails, run `aaa authentication fail-message` in global mode. To delete a personal banner, use the `no` form of this command.

**aaa authentication fail-message** *delimiter string delimiter*

**no aaa authentication fail-message**



## Parameters

Parameters	Description
<i>delimiter string</i> <i>delimiter</i>	<b>Text string that will be displayed when user fails to log in. The delimiter adopts double quotation marks.</b>

## Default Value

If you do not define the login banner, the system will display the following default banner:  
Authentication failed!

## Command Mode

Global configuration mode

## Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the string, meaning the banner ends.

## Example

The following example shows that user name prompt is changed to the following character string: `aaa authentication fail-message "See you later"`

## Related Command

**aaa authentication banner**

### 6.1.3 *aaa authentication username-prompt*

## Syntax

To change the text display prompting the user name input, run command `aaa authentication username-prompt` in global mode. To return to the default setting, use the `no` form of this command.

**aaa authentication username-prompt** text-string

**no aaa authentication username-prompt**

## Parameters

Parameters	Description
<i>text-string</i>	<b>It is used to prompt the user of the text to be displayed at the time of the user name input.</b>

## Default Value

When there is no user-defined text-string, the prompting character string of the user name is "Username".

## Command Mode

Global configuration mode

## Usage Guidelines

The command “aaa authentication username-prompt” is used for changing the displayed character string prompting the user name input. The “no” format of the command changes the prompt of username into default value.

Username:

Some protocols (such as TACACS+) have the capability to cover the prompting information of local username. Under such circumstances, the use of the command “aaa authentication username-prompt” will not change the prompting character string of username.

Note:

The command “aaa authentication username-prompt” does not change any prompting information provided by remote TACACS +server.

## Example

The following example shows that user name prompt is changed to the following character string: aaa authentication username-prompt “YourUsername:”

## Related Command

### aaa authentication password-prompt

#### 6.1.4 aaa authentication password-prompt

## Syntax

To change the text display prompting the user password input, run command “aaa authentication password-prompt” in global configuration mode. To return to the default setting, use the no form of this command.

**aaa authentication password-prompt** *text-string*

**no aaa authentication password-prompt**

## Parameters

Parameters	Description
<i>text-string</i>	It is used to prompt the user of the text displayed at the time of password input.

## Default Value

When the user-defined text-string is not used, the password prompt is “Password”.

## Command Mode

Global configuration mode

## Usage Guidelines

The displayed default literal information prompting the user password input can be changed by using the command “aaa authentication password-prompt”. The command not only changes the password prompt of the enable password, it also changes the password prompt

of login password. The “no” format of the command restores the password prompt to default value.

Password:

The command “aaa authentication password-prompt” does not change any prompting information provided by remote TACACS+ or RADIUS server.

### Example

The following Example will change the password prompt to “YourPassword:” aaa authentication password-prompt “YourPassword:”

### Related Command

**aaa authentication username-prompt**

**enable password**

### 6.1.5 aaa authentication dot1x

#### Syntax

To set dot1x access authentication, run command aaa authentication dot1x in global configuration mode. To disable dot1x authentication, use the no form of this command.

**aaa authentication dot1x {default | list-name} method1 [method2...]**

**no aaa authentication dot1x {default | list-name}**

#### Parameters

Parameters	Description
<i>Default</i>	<b>It uses the listed authentication method following the parameter as the default authentication method list at the time of the user’s login.</b>
<i>list-name</i>	<b>It uses the listed authentication method following the parameter as the default authentication method list at the time of the user’s login.</b>
<i>method</i>	<b>It is one of the key words described in the Form 2 at the least.</b>

#### Command Mode

Global configuration mode

#### Usage Guidelines

The default list or other naming list created by the command “aaa authentication login” will act on some specific line using the command “login authentication”.

Only when the said authentication method feeds back error, other authentication methods will be used. Should the said authentication method feedback the failure, no other authentication methods will be used.

dot1x authentication method

Keyword	Description
<i>group name</i>	Uses the server group for authentication.
<i>group radius</i>	Uses RADIUS authentication.
<i>group tacacs+</i>	Uses group tacacs+ for authentication.
<i>local</i>	Uses the local username database for authentication.
<i>local-case</i>	Uses case-sensitive local user name authentication.
<i>none</i>	Uses no authentication.

### Example

The following example creates an AAA authentication list called TEST. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication. (Now the authentication method either enable(line) or local can obtain a success or failure result. Therefore, the following command will not use the none method.

```
aaa authentication dot1x TEST group tacacs+ local none
```

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication dot1x default group tacacs+ local none
```

### Related Command

None

#### 6.1.6 *aaa authentication enable default*

##### Syntax

To enable AAA authentication to determine if a user can access the privileged command level, use the `aaa authentication enable default global configuration` command. To disable this authentication method, use the `no` form of this command.

```
aaa authentication enable default method1 [method2...]
```

```
no aaa authentication enable default
```

##### Parameters

Parameters	Description
<i>method</i>	At least one of the keywords described in Table 1.

##### Default Value

No authentication method is set. The authentication will succeed if it is the console port user. Otherwise, the authentication will fail.

## Command Mode

Global configuration mode

## Usage Guidelines

Use the `aaa authentication enable default` command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 1. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line. Only when the said authentication method feeds back error, other authentication methods will be used. Should the said authentication method feedback the failure, no other authentication methods will be used.

enable authentication method

Keyword	Description
<i>enable</i>	Uses the enable password for authentication.
<i>group name</i>	Uses the server group for authentication.
<i>group radius</i>	Uses RADIUS authentication.
<i>group tacacs+</i>	Uses tacacs+ for authentication.
<i>line</i>	Uses the line password for authentication.
<i>none</i>	Passes the authentication unconditionally.

## Example

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication. (Now the authentication method either enable (line) or local can obtain a success or failure result. Therefore, the following command will not use the none method.

```
aaa authentication enable default group tacacs+ enable none
```

## Related Command

**enable password**

### 6.1.7 aaa authentication login

#### Syntax

To set authentication, authorization, and accounting (AAA) authentication at login, use the `aaa authentication login` command in global configuration mode. To disable AAA authentication, use the `no` form of this command.

```
aaa authentication login {default | list-name} method1 [method2...]
```

```
no aaa authentication login {default | list-name}
```

## Parameters

Keyword	Description
<i>Default</i>	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.
<i>method</i>	At least one of the keywords described in Table 2.

## Default Value

No authentication method is set. The authentication will succeed if it is the console port user. Otherwise, the authentication will fail.

## Command Mode

Global configuration mode

## Usage Guidelines

The default and optional list names that you create with the `aaa authentication login` command are used with the `login authentication` command.

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

## login authentication method

Keyword	Description
<i>enable</i>	Uses the enable password for authentication.
<i>group name</i>	Uses the server group for authentication.
<i>group radius</i>	Uses RADIUS authentication.
<i>group tacacs+</i>	Uses tacacs+ for authentication.
<i>line</i>	Uses the line password for authentication.
<i>local</i>	Uses the local username database for authentication.
<i>localgroup</i>	Uses the local strategy group username database for authentication.
<i>local-case</i>	Uses case-sensitive local user name authentication.
<i>none</i>	Uses no authentication.

## Example

The following example creates an AAA authentication list called TEST. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no

enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login TEST group tacacs+ group radius none
```

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ group radius none
```

### Related Command

None

### 6.1.8 *aaa group server*

#### Syntax

To group different RADIUS server hosts into distinct lists and distinct methods, run command `aaa group server radius` in global configuration mode. To remove a group server from the configuration list, use the `no` form of this command.

```
aaa group server {radius | tacacs+} group-name
```

```
no aaa group server {radius | tacacs+} group-name
```

#### Parameters

Parameters	Description
<i>group-name</i>	Character string used to name the group of servers.

#### Default Value

No default behavior or values.

#### Command Mode

Global configuration mode

#### Usage Guidelines

The command is used to enter the configuration of the server group and add the corresponding server to it. It can establish 63 server groups in maximum.

#### Example

```
aaa group server radius radius-group
```

The example shows how to add a radius server group named radius-group.

### Related Command

server

### 6.1.9 *server*

#### Syntax

To add a server in an AAA server group, run the following command. To delete a server, use the no form of this command.

To add a server in a radius server group:

```
server {A.B.C.D | X:X:X:X::X} [key {password | {encryption-type encrypted-password}} ]
[auth-port num] [acct-port num] [retransmit value] [timeout value] [privilege pri]
```

To add a server to a tacacs+ server group:

```
server {A.B.C.D | X:X:X:X::X} [key {password | {encryption-type encrypted-password}} ]
no server A.B.C.D
```

### Parameters

Parameters	Description
<i>A.B.C.D</i>	IP address of the server
<i>X:X:X:X::X</i>	IPv6 address of the server
<i>key</i>	Key
<i>password</i>	key character string
<i>encryption-type</i>	encryption type, 0 means no encryption, and 7 means encryption.
<i>encrypted-password</i>	key character string corresponding to the encryption type
<i>auth-port</i>	authentication destination port
<i>acct-port</i>	accounting destination port
<i>num</i>	Standing for a port ID
<i>retransmit value</i>	retransmit times, the default is 2.
<i>timeout value</i>	timeout for retransmit. The default is 3 seconds.
<i>privilege pri</i>	server priority; the default is 0.

### Default Value

no server

### Command Mode

Server group configuration mode

### Usage Guidelines

You can add 63 server groups at most, 1 radius server link table and 1 tacacs+ server link table. The value of all radius server groups and servers in the server link table amounts to 64. The value of all tacacs+ server groups and servers in the server link table also amounts to 64.

### Example

The following example adds a server at 12.1.1.1 to the server group:



```
server 12.1.1.1
```

### Related Command

```
aaa group server
```

### 6.1.10 debug aaa authentication

#### Syntax

To track the user authentication process, run `debug aaa authentication`. To disable the debug information, run `no debug aaa authentication`.

#### **debug aaa authentication**

```
no debug aaa authentication
```

#### Parameters

None

#### Default Value

The debug information is disabled by default.

#### Command Mode

EXEC

#### Usage Guidelines

This command can be used to track the authentication process of each user to detect the cause of the authentication failure.

#### Example

None

#### Related Command

None

### 6.1.11 enable password

#### Syntax

To set a local password to control access to various privilege levels, use the `enable password` command. To remove the password requirement, use the `no` form of this command.

```
enable password { password | [encryption-type] encrypted-password } [level number]
```

```
no enable password [level number]
```

#### Parameters

Parameters	Description
<i>password</i>	Plain text of the password character string
<i>encryption-type</i>	Type of password encryption

<i>encrypted-password</i>	<b>Encrypted password corresponding to the set encryption type</b>
<i>level</i>	<b>Privilege level parameter</b>
<i>number</i>	<b>Value of the privilege level (1-15)</b>

### Default Value

There is no password by default.

### Command Mode

Global configuration mode

### Usage Guidelines

The passwords configured for the device do not contain space, that is, when the enable password command is used, space cannot be entered when you enter the plain text of the password. The length of the password plain-text cannot exceed 127 characters.

When the level parameter is not entered, the default level is level 15. The higher the privilege level is, the more rights the user has. If some privilege level is not configured with password, authentication will fail when the user enters the level.

Currently, our products only support two encryption modes: 0 and 7. The number 0 means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

### Example

The following example shows how to set the password of privilege level 10 to clever and encryption-type to 0.

```
enable password 0 clever level 10
```

The following example shows how to set the password of the default privilege level (15) to oscar and encryption-type to 7.

```
enable password 7 074A05190326
```

Suppose that the cipher text of oscar is 074A05190326, the value of the cipher text is obtained from the configuration files of other devices.

### Related Command

**aaa authentication enable default**

**service password-encryption**

#### 6.1.12 enable(enter)

##### Syntax

To enter the privilege mode (EXEC mode), run command enable(enter).

```
enable(enter) <1-15>
```

## Parameters

Parameters	Description
<1-15>	To be obtained privilege level

## Default Value

Do not enter the privileged level by default.

## Command Mode

User mode

## Usage Guidelines

None

## Example

```
>enable(The user level is 15 by default.)
```

```
Password: (enter the password to authenticate) #
```

```
#exi
```

```
>enable 1(To be obtained privilege level is 1)
```

```
Password: (enter the password to authenticate) #
```

## Related Command

```
aaa authentication enable default
```

```
enable password
```

*6.1.13 service password-encryption*

## Syntax

To encrypt passwords, use the service password-encryption command. To return to the default setting, use the no form of this command.

```
service password-encryption
```

```
no service password-encryption
```

## Parameters

None

## Default Value

Related passwords in the system are not encrypted.

## Command Mode

Global configuration mode

## Usage Guidelines

This command is related with three commands, `username password`, `enable password` and `password`. If this command is not configured and the previous three commands adopt the password plain-text storage mode, the configured password's plain text can be displayed after the `show running-config` command is run. If this command is configured, the passwords configured for the previous three commands will be encrypted and the configured password's plain text cannot be displayed after the `show running-config` command is run; in this case, the password plain-text display cannot be resumed even if you run `no service password-encryption`. The `no service password-encryption` command is effective only to the password which is configured by this command, while is not effective to those passwords which are encrypted before this command is used.

## Example

```
switch_config#service password-encryption
```

The example show how to encrypt the configured plain-text password and also the plain-text password after this command is used.

## Related Command

**username** username **password**

**enable password**

**password (the configuration command under vty which can be used for line authentication)**

## 6.2 Authorization Configuration Commands

This chapter describes the commands for authentication, authorization and accounting. AAA authorization can limit the effective service to a user. When the authorization result is effective, network access server configures the dialogue process of the user by using the authorization information fed back from authorization server. Then the user is available to services required. Only information included in the user profile provides such service.

Please refer to “Configuration Authorization” for information on how to configure authorization. Please refer to the last part to review the examples configured by the commands in this Chapter.

Authorization Configuration Commands include: `aaa authorization`

```
debug aaa authorization
```

### 6.2.1 *aaa authorization*

#### Syntax

The global configuration command “`aaa authorization`” is used for setting the parameter to limit the authority of the user’s access to network.

To set the parameter to limit the authority of the user’s access to network, run command “`aaa authorization`” in global configuration mode. To return to the default setting, use the `no` form of this command.

```
aaa authorization {{commands <0-15>} | network | exec} {default | list-name} method1
```

[*method2...*]

```
no aaa authorization {{commands <0-15>} | network | exec } {default | list-name}
```

```
aaa authorization config-commands
```

```
no aaa authorization config-commands
```

### Parameters

Parameters	Description
<i>commands</i>	EXEC (shell) command authorization
<0-15>	To be authorized command privilege (EXEC)
<i>network</i>	The authorization of network type service
<i>exec</i>	It adapts to the attribute related to the user EXEC terminal dialogue. It determines whether XEC shell program is allowed to register or grant the privilege level of the user entering EXEC shell.
<i>default</i>	Default authorization methods list
<i>list-name</i>	Character string which is used to name the authorization method list
<i>method</i>	At least one of the keywords listed in the form below.
<i>config-commands</i>	Configuration mode command service

### Default Value

If the user requires accounting but he does not designate the authorization method list on the corresponding path or interface, the default authorization method list will be applied. If the default method list is not defined, the authorization will not be executed.

### Command Mode

Global configuration mode

### Usage Guidelines

The command “aaa authorization” is used for enabling the authorization, creating authorization methods list and defining the authorization method that can be used when the user accesses to the designated functions. The authorization method list defines the authorization execution method and the order to execute these authorization methods. The method list is just a simple naming list, describing the authorization method (RADIUS or TACACS+). The method list can designate one or multiple authorization security protocols. Hence, it secures a standby method if all previous authorization methods fail. Under general condition, the listed first method is used at first in an attempt to authorize the user the authority to access to the designated network service. If the method does not work, the next method in the list shall be selected. The process shall be continued till the successful feedback of authorization results by using some authorization method or all the defined methods are used up.

Authorization method

Keyword	Description
<i>group name</i>	Uses the server group for authorization.
<i>group radius</i>	Uses RADIUS authorization.
<i>group tacacs+</i>	Uses tacacs+ authorization.
<i>if-authenticated</i>	If the user passes the authorization, the user is allowed to access the function required.
<i>local</i>	The local database is used for authorization.
<i>none</i>	No authorization

Once the authorization methods list is defined, the methods list shall be used on the designated line or interface before the defined method is executed. As a part of the authorization process, the authorization command sends a series of request packets of AV pairs to the program of RADIUS or TACACS+ server. The server is likely to execute one of the following actions:

- The request is accepted completely.
- The request is accepted and the attribute is added to limit the authority of user service.
- Request is refused and authorization fails.

### Example

The following Example defines the network authorization methods list named “have a try”. The methods list designates RADIUS authorization method used on the serial line employing vty. If RADIUS server makes no response, the local network authorization is executed.

```
aaa authorization exec have_a_try radius local
```

Related Command

**aaa authentication**

**aaa accounting**

### 6.2.2 *debug aaa authorization*

#### Syntax

To track the user authorization process, run `debug aaa authorization` command. To disable the debug information, run the `no` form of this command.

**debug aaa authorization**

`no debug aaa authorization`

#### Parameters

None

#### Default Value

The debug information is disabled by default.

## Command Mode

EXEC

## Usage Guidelines

This command can be used to track the authorization process of each user to detect the cause of the authorization failure.

## Example

None

## Related Command

None

## 6.3 Accounting Configuration Commands

This chapter describes the commands for accounting. The accounting function can track the services that users access, and at the same time track the service-consumed network resource number. When AAA accounting is activated, the system will report user's activities to the TACACS+ server or the RADIUS server in the accounting record method (It depends on the adopted security method). Each accounting record contains the attribute value peer which is stored on the access control server. The data is then applied to network management, client's accounting analysis or audit.

Authorization Configuration Commands include:

- `aaa accounting`
- `aaa accounting update`
- `aaa accounting suppress null-username`
- `debug aaa accounting`

### 6.3.1 *aaa accounting*

#### Syntax

To execute AAA accounting onto required services on the basis of accounting or security, run `aaa accounting` in global mode. You can run `no aaa accounting` to disable the accounting function.

```
aaa accounting {{commands <0-15>} | network | exec | connection} {default | list-name}
```

```
{{start-stop | stop-only} group {groupname | radius | tacacs+} | none }
```

```
no aaa accounting { network | exec | connection} {default | list-name}
```

#### Parameters

Parameters	Description
<i>commands</i>	Provide accounting for a priority level command
<0-15>	The priority level of the command

<i>network</i>	<b>Provides accounting information to all PPP sessions, including packets, bytes and time numbering.</b>
<i>exec</i>	<b>Provides information about EXEC terminal session (it is not supported currently).</b>
<i>connection</i>	<b>Provides information about all egress connections from related device. Currently, only the H323 session is supported.</b>
<i>default</i>	<b>Default accounting method list</b>
<i>list-name</i>	<b>Character string which is used to name the accounting method list</b>
<i>start-stop</i>	<b>accounting in beginning and end</b>
<i>stop-only</i>	<b>accounting in the end</b>
<i>none</i>	<b>no accounting</b>
<i>group groupname</i>	<b>Uses the server group for accounting</b>
<i>group radius</i>	<b>Uses RADIUS for accounting</b>
<i>group tacacs+</i>	<b>Uses tacacs+ for accounting</b>

### Default Value

If the user requires accounting but he does not designate the accounting method list on the corresponding path or interface, the default accounting method list will be applied. If the default method list is not defined, the accounting will not be executed.

### Command Mode

Global configuration mode

#### Usage Guidelines

You can use the `aaa accounting` command to enable the accounting function, create the accounting method list and define the applied accounting method when user sends the accounting record. The accounting method list defines the accounting execution method and the order to execute these accounting methods. The method list is just a simple naming list, describing the accounting method (RADIUS or TACACS+). The method list can designate one or multiple accounting security protocols. Hence, it secures a standby method if all previous accounting methods fail.

### Related Command

`aaa authentication`

**`aaa accounting`**

### 6.3.2 `aaa accounting update`

#### Syntax

To periodically transmit temporary accounting records to the accounting server, run `aaa accounting update`. You can run `no aaa accounting update` to disable temporary accounting records.



```
aaa accounting update { newinfo | periodic number}
```

```
no aaa accounting update { newinfo | periodic}
```

#### Parameters

Parameters	Description
<i>update</i>	Activates the device to transmit temporary accounting records (It needs support from the application client. It is not supported at present).
<i>newinfo</i>	Transmits temporary accounting records to the accounting server when new accounting information need be reported.
<i>periodic</i>	Periodically transmits temporary accounting records. The period is defined by the number parameter.
<i>number</i>	A parameter to define the period for temporary accounting record transmission

#### Default Value

Temporary accounting activity does not occur.

#### Command Mode

Global configuration mode

#### Usage Guidelines

The function runs with the support of the application client. It is not supported at present.

#### Related Command

```
aaa accounting
```

### 6.3.3 *aaa accounting suppress null-username*

#### Syntax

To stop generating accounting records for those non-user sessions, run `aaa accounting suppress null-username` in global mode. To return to the default setting, use the `no` form of this command.

```
aaa accounting suppress null-username
```

```
no aaa accounting suppress null-username
```

#### Parameters

None

#### Default Value

The accounting records will be generated for all sessions, no matter the sessions have username or not.

#### Command Mode

Global configuration mode

### Usage Guidelines

None

### Related Command

**aaa accounting**

#### *6.3.4 debug aaa accounting*

### Syntax

To track the user accounting process, run `debug aaa accounting` command. To disable the debug information, run the `no` form of this command.

### **debug aaa accounting**

`no debug aaa accounting`

### Parameters

None

### Default Value

The debug information is disabled by default.

### Command Mode

EXEC

### Usage Guidelines

This command can be used to track the accounting process of each user to detect the cause of the accounting failure.

### Example

None

### Related Command

None

## **6.4 Local Account Policy Configuration Commands**

This section introduces local account policy configuration commands. The local account policy is used for local authentication and local authorization.

Please refer to “local account policy configuration” for information on how to configure local account policy. Please refer to the last part to review the examples configured by the commands in this Chapter.

Local Account Policy Configuration Commands include:

`localauthen`

`localauthor`

`localpass`

```

localgroup
local authen-group
local author-group
local pass-group
local user username
show local-users
show aaa users

```

### 6.4.1 localauthen

#### Syntax

To configure local authentication policy, run the command `localauthen`. To return to the default setting, use the `no` form of this command.

```
localauthen WORD
```

```
no localauthen WORD
```

#### Parameters

Parameters	Description
<i>WORD</i>	Local authentication policy name

#### Default Value

None

#### Command Mode

Global configuration mode

#### Usage Guidelines

To enter local authentication configuration, run command `localauthen WORD`.

The max login tries within a certain time

```
login max-tries <1-9> try-duration 1d2h3m4s
```

Parameters	Description
<i>max-tries</i>	The max login tries
<i>&lt;1-9&gt;</i>	The max login tries ranges from 1 to 9
<i>try-duration</i>	Duration
<i>1d2h3m4s</i>	The format of day, hour, min and second.

#### Related Command

**login max-tries 1****ocalgroup****local authen-group****username**

## 6.4.2 localauthor

### Syntax

To configure local authentication policy, run the command `localauthen`. To return to the default setting, use the `no` form of this command.

`localauthor WORD``no localauthen WORD`

### Parameters

Parameters	Description
<i>WORD</i>	Local authorization policy name

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

The command `localauthor WORD` is used to enter the local authorization policy configuration. Use following command to configure local authorization policy.

To authorize priority for login users.

`exec privilege {default | console | ssh | telnet} <1-15>`

Parameters	Description
<i>default</i>	Default priority (Use the priority for authorization if there is no concrete login method.)
<i>console</i>	authorization priority of the login user on console port
<i>ssh</i>	authorization priority of the ssh login user on console port
<i>telnet</i>	authorization priority of the telnet login user on console port
<1-15>	Priority

### Related Command

`exec privilege`

**localgroup****local author-group****username****6.4.3 localpass****Syntax**

To configure local password policy, run the command `localpass` in global mode. To return to the default setting, use the `no` form of this command.

`localpass` **WORD**

`no localpass` **WORD**

**Parameters**

Parameters	Description
<i>WORD</i>	Local password policy name

**Default Value**

None

**Command Mode**

Global configuration mode

**Usage Guidelines**

The command `localpass WORD` is used to enter the local password policy configuration. Use following command to configure local password policy.

The password and username is different

**non-user**

History password check (When the password is different from the history one or modifying the password)

**non-history**

Set the elements of the password

**element** [*number*] [*lower-letter*] [*upper-letter*] [*special-character*]

Parameters	Description
<i>number</i>	The password must include numbers.
<i>lower-letter</i>	The password must include lower-letters.
<i>upper-letter</i>	The password must include upper-letters.
<i>special-character</i>	The password must include special characters.

The minimum length of the password

**min-length** <1-127>

Parameters	Description
<1-127>	The minimum length (ranges from 1-127)

The validity of the password

**validity** 1d2h3m4s

Parameters	Description
1d2h3m4s	The format of day, hour, min and second.

Related Command

**non-use**

**non-history**

**element**

**min-length**

**validity**

**localgroup**

**local pass-group**

**username**

#### 6.4.4 localgroup

Syntax

To configure local policy group, run command localgroup in global mode. To return to the default setting, use the no form of this command.

localgroup **WORD**

no localgroup **WORD**

Parameters

Parameters	Description
<b>WORD</b>	Local policy group name

Default Value

None

Command Mode

Global configuration mode

## Usage Guidelines

The command `localgroup WORD` is used to enter the local password policy configuration. Use following command to configure local policy group.

Stands for the local authentication configuration

### **local authen-group**

Stands for the local authorization configuration

### **local author-group**

Local password configuration

### **local pass-group**

Local account configuration

### **local user**

Configuring account

### **username**

## Related Command

**local authen-group**

**local author-group**

**local pass-group**

**local user**

**username**

**localgroup**

**local author-group**

## 6.4.5 *local authen-group*

### Syntax

To configure local authentication policy group, run command `local authen-group`. It is local policy group in global mode by default. To return to the default setting, use the `no` form of this command. `local authen-group WORD`

`no local authen-group`

### Parameters

Parameters	Description
<i>WORD</i>	Local authentication policy name

### Default Value

None

**Command Mode**

Global configuration mode, local policy group configuration mode

**Usage Guidelines**

None

**Related Command**

**localauthen**

**localgroup**

**local authen-group**

**6.4.6 local author-group****Syntax**

To configure local authentication policy group, run command `local author-group`. It is the local policy group in global mode by default. To return to the default setting, use the `no` form of this command.

`local author-group WORD`

`no local author-group`

**Parameters**

Parameters	Description
<i>WORD</i>	Local authorization policy name

**Default Value**

None

**Command Mode**

Global configuration mode, local policy group configuration mode

**Usage Guidelines**

None

**Related Command**

**localauthor**

**localgroup**

**local author-group**

**6.4.7 local pass-group****Syntax**



To configure local password policy group, run command `local pass-group`. It is the default policy group by default in global configuration mode. To return to the default setting, use the `no` form of this command.

`local pass-group` **WORD**

`no local pass-group`

#### Parameters

Parameters	Description
<i>WORD</i>	Local password policy name

#### Default Value

None

#### Command Mode

Global configuration mode, local policy group configuration mode

#### Usage Guidelines

None

#### Related Command

`localpass`

`localgroup`

`local pass-group`

### 6.4.8 local user

#### Syntax

To configure the maximum connection numbers and freezing users, run command `local user`. It is the default policy group by default in global configuration mode. To return to the default setting, use the `no` form of this command.

`local user` {`maxlinks` <1-255>} | {`freeze` **WORD** }

`no local user` {`maxlinks` | {`freeze` **WORD** }}

#### Parameters

Parameters	Description
<i>maxlinks</i>	The maximum links to the router, the same user can create at the same time.
<1-255>	The number of links created at the same time. (value range: 1-255)
<i>freeze</i>	freezing user
<i>WORD</i>	A user name

**Default Value**

None

**Command Mode**

Global configuration mode, local policy group configuration mode

**Usage Guidelines**

None

**Related Command****localgroup****6.4.9 username****Syntax**

To add users in the local user database for local authentication and authorization, run this command. The command is used in local policy group configuration mode. It is the default local policy group in global configuration mode. To return to the default setting, use the no form of this command.

```
username username [password password | {encryption-type encrypted-password}]
[maxlinks number] [authen-group WORD] [author-group WORD] [pass-group WORD]
[autocommand command] [bind-ip A.B.C.D] [bind-mac H:H:H:H:H:H] [bind-pool WORD]
[bind-port port][callback-dialstring string] [callback-line line] [callback-rotary rotary]
[nocallback-verify] [nohangup] [noescape]
```

```
no username username
```

**Parameters**

Parameters	Description
<i>username</i>	Character string of username
<i>password</i>	User password
<i>password</i>	Plain text of the password character string
<i>encryption-type</i>	Type of password encryption
<i>encrypted-password</i>	Cipher text of the password which corresponds to the limited encryption type
<i>maxlinks</i>	The maximum links to the device, the same user can create at the same time
<i>number</i>	number of links
<i>authen-group</i>	Set the local authentication policy
<i>WORD</i>	Local authentication policy name
<i>author-group</i>	Set the local authorization policy
<i>WORD</i>	Local password policy name
<i>pass-group</i>	Set the local password policy

<i>WORD</i>	Local password policy name
<i>autocommand</i>	Run the specified command when the user logs in. autocommand must run at the end of the command line.
<i>command</i>	Run the command character string automatically.
<b>The switch does not support following options.</b>	
<i>bind-ip</i>	bind user IP address (non-support)
<i>A.B.C.D</i>	IP address
<i>bind-mac</i>	bind user mac address (non-support)
<i>H:H:H:H:H:H</i>	48 byte hardware address of ARP record
<i>bind-pool</i>	bind user address pool (non-support)
<i>WORD</i>	address pool name
<i>bind-port</i>	bind user port (non-support)
<i>Port</i>	Port
<i>callback-dialstring</i>	callback dial (non-support)
<i>string</i>	telephone number character string
<i>callback-line</i>	callback line (non-support)
<i>line</i>	Stands for the ID of the line.
<i>callback-rotary</i>	callback rotary configuration (non-support)
<i>rotary</i>	rotary number;
<i>nocallback-verify</i> :	no callback verify (non-support)
<i>nohangup</i>	no hangup after the user logs in and run the command automatically (non-support)
<i>noescape</i>	no escape character after the user logs in (non-support)

### Default Value

no users

### Command Mode

Global configuration mode, local policy group configuration mode

### Usage Guidelines

The password is considered as empty character string when there is no password parameter.

user-maxlinks limits the session numbers the same account can establish. But the account will not be counts in if its session is not authenticated by local authentication. Command show aaa users can be used to check the basic information of each on-line user.

The passwords configured for the device do not contain space, that is, when the enable password command is used, space cannot be entered when you enter the plain text of the password.

Currently, our products only support two encryption modes: 0 and 7. The number 0 means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

### Example

The local user is added in the Example below. The username is someone, the password is someother.

```
username someone password someother
```

The local user is added in the Example below, the username is Oscar, the password is Joan. The encryption type applied is 7, namely the encryption method, the ciphertext of the password is needed to be entered.

```
enable password 7 1105718265
```

Given the assumption that the ciphertext of Joan is 1105718265, the value of the ciphertext is obtained from the configuration files of other routers.

### Related Command

**aaa authentication login**

#### *6.4.10 show local-users*

### Syntax

To show summary informationn of all local AAA account, run command show local-users.

**show local-users**

### Parameters

None

### Default Value

None

### Command Mode

EXEC

### Usage Guidelines

The command is used to show all AAA accounts, including following information: Local group default, links, pw\_present, login\_tries, login\_try\_time, and freezing\_cause.

### Example

```
#show local-users
```

Local group default:

username	links	pw_present	login_tries	login_try_time	freezing_cause
admin	1	0s	0	0s	
aaa	0	0s	0	0s	

Domain	Description
<i>Local group default:</i>	<b>The local policy group that the account belongs to</b>
<i>links</i>	<b>The connections that the account is using (represents how much users are using the account.)</b>
<i>pw_present</i>	<b>Password validity period</b>
<i>login_tries</i>	<b>login password failure times (sets the maximum failure times and 0 means no set)</b>
<i>login_try_time</i>	<b>login password failure time (sets the maximum failure times and 0 means no set)</b>
<i>freezing_cause</i>	<b>reason of the account being frozen</b>

## Related Command

**username**

### 6.4.11 show aaa users

## Syntax

To display the summary information about all online AAA users, run show aaa users.

**show aaa users**

## Parameters

None

## Default Value

None

## Command Mode

EXEC

## Usage Guidelines

After this command is run, the following information about online users can be displayed: port, username, service, online duration time and peer\_address.

## Example

```
#show aaa users
```

Port	User	Service	Duration	Peer Address
=====				

```
console 0      zjl      exec      04:14:03      unknown
vty 0         aaa      exec      00:12:24      172.16.20.120
```

Domain	Description
Port	ID of the interface where user lies, or index number of VTY
User	Character string of username
Service	Service applied by the user
Duration	Online duration time of the user
Peer Address	IP address of the remote host where the user lies

### Related Command

**username**

## Chapter 7 RADIUS Configuration Commands

This chapter introduces the commands for RADIUS configuration. RADIUS is a distributed client/server system capable of denying the unauthorized network access. RADIUS client is running on the router and sends the request of authentication, authorization and accounting to the central RADIUS server containing the authentication of all the user and the information of network service access.

Please refer to “RADIUS Configuration” about how to configure RADIUS information and learn more about configuration examples.

### 7.1 RADIUS Configuration Commands

RADIUS Configuration commands include:

- debug radius
- ip radius source-interface
- radius-server challenge-noecho
- radius-server acct-on
- radius-server deadtime
- radius-server host
- radius-server key
- radius-server optional-passwords
- radius-server retransmit
- radius-server timeout
- radius-server vsa send
- radius-server attribute

- radius-server directed-resquest
- radius-server attribute
- radius-server directed-resquest

### 7.1.1 *debug radius*

#### Syntax

To track RADIUS event or packet, run command `debug radius`. To disable the debug information, run the `no` form of this command.

**debug radius** {*event* | *packet*}

**no debug radius** {*event* | *packet*}

#### Parameters

Domain	Description
<i>event</i>	Tracing RADIUS event.
<i>packet</i>	Tracing RADIUS packets.

#### Default Value

None

#### Command Mode

EXEC

#### Usage Guidelines

The command can be used for network system debug and finding the reason of user authentication failure.

#### Example

The following example shows how to enable RADIUS event track:

```
debug radius event
```

### 7.1.2 *ip radius source-interface*

#### Syntax

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the `ip radius source-interface` command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the `no` form of this command.

**ip radius source-interface** *interface-name*

**no ip radius source-interface**

#### Parameters

Parameters	Description
<i>interface-name</i>	Name of the interface that RADIUS uses for all of its outgoing packets.

### Default Value

No default behavior or values

### Command Mode

Global configuration mode

### Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. This command is especially useful in cases where the device has many subinterfaces and you want to ensure that all RADIUS packets from a particular device have the same IP address.

The specified subinterface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the subinterface to the up state.

### Example

The following example shows how to configure RADIUS to use the IP address of vlan 1 for all outgoing RADIUS packets:

```
ip radius source-interface vlan 1
```

### Related Command

```
ip tacacs source-interface
```

### 7.1.3 radius-server attribute

#### Syntax

To designate some attributes to be transmitted during radius authentication and charging, run `radius-server attribute`. To disable AAA authentication, use the `no` form of this command.

```
radius-server attribute {4 | 32 | 95}
```

```
no radius-server attribute {4 | 32 | 95}
```

#### Parameters

Parameters	Description
4	Transmits the following address as attribute 4 (NAS ip address) during radius operation.
32	Transmits attribute 32 authentication or request.(NAS identifier) during radius



95

Transmits the following address as attribute 95 (NAS ipv6 address) during radius operation.
---

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

This command is used to designate a specific attribute to be transmitted during radius authentication or radius request.

The radius-server attribute 4 command is used to configure attribute 4 (NAS ip address) in radius and transmit it in the RADIUS packets.

The radius-server attribute 32 command is used to designate attribute 32 (NAS ID) to be transmitted in Radius authentication or charging.

The radius-server attribute 95 command is used to configure attribute 95 (NAS ipv6 address) in radius and transmit it in the RADIUS packets.

### Example

The radius-server attribute 4 X.X.X.X command is used when attribute 4 need be transmitted in the Radius packets and attribute 4 serves as the attribute value of X.X.X.X.

The radius-server attribute 32 in-access-req command is used when the NAS identifier need be transmitted in the authentication request.

The radius-server attribute 32 in-account-req command is used when the NAS identifier need be transmitted in the charging request.

radius-server attribute 32 identifier configuring NAS identifier

The radius-server attribute 95 X:X:X:X::X command is used when attribute 95 need be transmitted in the Radius packets and X:X:X:X::X serves as the attribute value.

### Related Command

None

#### 7.1.4 radius-server challenge-noecho

### Syntax

The command “radius-server challenge-noecho” shall be used for not showing the user data under the Access-Challenge Mode.

**radius-server challenge-noecho**

**no radius-server challenge-noecho**

### Parameters

None

### Default Value

The user data is shown under the Access-Challenge.

### Command Mode

Global configuration mode

### Usage Guidelines

None

### Example

```
radius-server challenge-noecho
```

## 7.1.5 radius-server deadtime

### Syntax

The global configuration command “radius-server dead-time” shall be used for improving the echo time of RADIUS when some servers are not workable. The command allows the system to skip the unworkable servers. The “no” format of the command can be used for setting dead-time as 0, namely, all the servers are thought to be workable.

**radius-server deadtime** *minutes*

**no radius-server deadtime**

### Parameters

Parameters	Description
<i>minutes</i>	The time length of RADIUS server thought to be unworkable, the maximum length is 1440 minutes (24 hours)

### Default Value

The unworkable time is set as 0, meaning that the server is thought to be workable all the time.

### Command Mode

Global configuration mode

### Usage Guidelines

The command is used for labeling those RADIUS servers that do not respond to the authentication request as “dead”, which avoids too long waiting for the response before using the next server. The RADIUS server labeled as “dead” is skipped by all the requests during the set minutes unless otherwise all the servers are labeled as “dead”.

### Example

The following Example designates 5-minute dead time for the RADIUS server that does not respond to the request.

```
radius-server deadtime 5
```

## Related Command

**radius-server host**

**radius-server retransmit**

**radius-server timeout**

### 7.1.6 *radius-server directed-resquest*

#### Syntax

To enable the user to set RADIUS server with the format of '@server', run command `radius-server directed-resquest` in global mode. To return to the default setting, use the `no` form of this command.

**radius-server directed-resquest [restricted]**

**no radius-server directed-resquest [restricted]**

#### Parameters

Parameters	Description
<i>restricted</i>	The user can only use the format of '@server' to set RADIUS server.

#### Default Value

It does not support using the format of '@server' to set RADIUS server.

#### Command Mode

Global configuration mode

#### Usage Guidelines

None

#### Example

```
radius-server directed-resquest
```

#### Related Command

None

### 7.1.7 *radius-server host*

#### Syntax

The global configuration command “`radius-server host`” is used for designating IP address of radius server. The “`no`” format of the command is used for deleting the designated RADIUS host.

**radius-server host** *ip-address|ipv6-address* [*auth-port port-number1*] [*acct-port port-number2*]

**no radius-server host** *ip-address|ipv6-address*

## Parameters

Parameters	Description
<i>ip-address</i>	the ip address of RADIUS server
<i>ipv6-address</i>	the IPv6 address of RADIUS server
<i>auth-port</i>	(optional item) Designating UDP destination port for authentication request.
<i>port-number1</i>	(optional item) The port number of authentication request.
<i>acct-port</i>	(optional item) Designating UDP destination port for accounting request.
<i>port-number2</i>	(optional item) The port number of accounting request.

## Default Value

Any RADIUS host is not designated.

## Command Mode

Global configuration mode

## Usage Guidelines

The command “radius server” can be used repeatedly for designating multiple servers. The polling can be made under the order of configuration when necessary.

## Example

The Example below designates RADIUS host whose IP address is 1.1.1.1. The default port is used for accounting and authentication.

```
radius-server host 1.1.1.1
```

The following Example designates Port 12 as the destination port of authentication request on the RADIUS host whose IP address is 1.2.1.2. Port 16 is used as the destination port of accounting request.

```
radius-server host 1.2.1.2 auth-port 12 acct-port 16
```

## Related Command

**aaa authentication**

**radius-server key**

**tacacs server**

**username**

## 7.1.8 radius-server key

## Syntax

The global configuration command shall be used for setting encryption key for RADIUS communication between the router and RADIUS server. The “no” format of command can be used for invalidating the encryption key.

**radius-server key *string* | {encryption-type encrypted-password}**

no radius-server key

#### Parameters

Parameters	Description
<i>string</i>	The secret key used for encrypting. The secret key shall match with the one used by RADIUS server.
<i>encryption-type</i>	encryption type, 0 means no encryption, and 7 means encryption.
<i>encrypted-password</i>	The ciphertext of the password corresponding to the encryption type limited by “encryption-type”.

#### Default Value

The key is empty character string.

#### Command Mode

Global configuration mode.

#### Usage Guidelines

The key must correspond to the key used by RADIUS server. All start empty blank will be ignored. The key cannot include the empty character.

#### Example

The following example shows how to set encryption key to “firsttime”:

```
radius-server key firsttime
```

#### Related Command

**radius-server host**

**tacacs server**

username

#### 7.1.9 radius-server optional-passwords

##### Syntax

To specify that the first RADIUS request to a RADIUS server be made without password verification, use the radius-server optional-passwords command in global configuration mode. To return the default setting, use the no form of this command.

**radius-server optional-passwords**

no radius-server optional-passwords

#### Parameters

The command has no parameters or keywords.

### Default Value

optional-password is not used by default.

### Command Mode

Global configuration mode

### Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

### Example

The following example configures the first login to not require RADIUS verification: radius-server optional-passwords

### Related Command

radius-server host

### 7.1.10 radius-server retransmit

#### Syntax

To specify the number of times the software searches the list of RADIUS server hosts before giving up, use the radius-server retransmit command in global configuration mode. To disable retransmission, use the no form of this command.

**radius-server retransmit** *retries*

no radius-server retransmit

### Parameters

Parameters	Description
<i>retries</i>	<b>Maximum number of retransmission attempts. The default is 2 attempts.</b>

### Default Value

2 attempts

### Command Mode

Global configuration mode

### Usage Guidelines

This command is generally used with the `radius-server timeout` command, indicating the interval for which a router waits for a server host to reply before timing out and the times of retry after timing out.

### Example

The following example specifies a retransmit counter value of five times:

```
radius-server retransmit 5
```

### Related Command

`radius-server timeout`

#### 7.1.11 *radius-server timeout*

### Syntax

To set the interval for which a router waits for a server host to reply, use the `radius-server timeout` command in global configuration mode. To return the default setting, use the `no` form of this command.

**radius-server timeout** *seconds*

`no radius-server timeout`

### Parameters

Parameters	Description
<i>seconds</i>	Number that specifies the timeout interval, in seconds. The default is 5 seconds.

### Default Value

3 seconds

### Command Mode

Global configuration mode

### Usage Guidelines

This command is generally used with the `radius-server retransmit` command.

### Example

The following example shows how to set the number of seconds a router waits for a server host to reply before timing out.

```
radius-server timeout 10
```

### Related Command

None

#### 7.1.12 *radius-server vsa send*

### Syntax

To configure the network access server to recognize and use vendor-specific attributes, use the command `radius-server vsa send`. To return to the default setting, use the `no` form of this command.

**radius-server vsa send [authentication]**

**no radius-server vsa send [authentication]**

Parameters

Parameters	Description
<i>authentication</i>	<b>(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.</b>

Default Value

Disabled

Command Mode

Global configuration mode

Usage Guidelines

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The `radius-server vsa send` command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the `authentication` keyword with the `radius-server vsa send` command to limit the set of recognized vendor-specific attributes to just authentication attributes.

Example

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

```
radius-server vsa send authentication
```

Related Command

```
radius-server host
```

### 7.1.13 radius-server acct-on

Syntax

To enable or disable radius accounting function, use the command **[no] radius-server acct-on enable**. To set the retransmit times of the accounting packets, use the **command [no] radius-server acct-on retransmit <1-15>**. The default times is 3.

Parameters

Parameters	Description
<i>Retransmit</i>	<b>Retransmit times of the accounting packets.</b>



### Default Value

The accounting function is disabled. The retransmit times is 3.

### Command Mode

Global configuration mode

### Usage Guidelines

None

### Example

The following example shows how to enable the accounting and set the retransmit times to 5:

```
radius-server acct-on enable
```

```
radius-server acct-on retransmit 5
```

### Related Command

None

In order to RADIUS authentication to be worked you need to execute the following commands in global configuration mode:

```
aaa authentication enable default group radius
```

```
aaa authorization exec default local group radius
```

## Chapter 8 TACACS+ Configuration Commands

This chapter describes the commands for configuring TACACS+ security protocols. TACACS+ can be used for authenticating the identity of the user, authorization of service authority and the accounting of the execution process of user service.

Please refer to “TACACS+ Configuration” about how to configure TACACS+ information and learn more about configuration examples.

### 8.1 TACACS+ Configuration Commands

TACACS+ configuration commands include:

- `debug tacacs`
- `ip tacacs source-interface`
- `tacacs-server host`
- `tacacs-server key`
- `tacacs-server timeout`

#### 8.1.1 `debug tacacs`

##### Syntax

To trace TACACS+ protocol event or checking the packets received or sent, run command “`debug tacacs`”. To return to the default setting, use the `no` form of this command.

**`debug tacacs {event | packet}`**

**`no debug tacacs {event | packet}`**

##### Parameters

Parameters	Description
<i>event</i>	Tracing TACACS+ event
<i>packet</i>	Tracing TACACS+ packet

##### Default Value

The debug information is disabled by default.

##### Command Mode

EXEC

##### Usage Guidelines

The command is only used for the debugging of the network to find out the cause of failure of AAA service.

##### Example

The following example shows how the debugging of the network to find out the cause of failure of AAA service.

```
debug tacacs event
```

### Related Command

None

### 8.1.2 *ip tacacs source-interface*

#### Syntax

To apply IP address of the designated interface to all the TACACS+ packets, run command “ip tacacs source-interface” in global mode. To return to the default setting, use the no form of this command.

```
ip tacacs source-interface subinterface-name
```

```
no ip tacacs source-interface
```

#### Parameters

Parameters	Description
<i>subinterface-name</i>	<b>Interface name corresponding to the source IP address of all TACACS+ packets.</b>

#### Default Value

None

#### Command Mode

Global configuration mode

#### Usage Guidelines

The command can be used to set source IP address for all TACACS+ packets by designating the source interface. So long as the interface is under “up” state, all TACACS+ packets will use IP address of the interface as the source address, thus ensuring that TACACS+ packet of each router will have the same source IP address. So TACACS+ server will not need to maintain the address list containing the IP address. That is to say, in order to ensure all TACACS+ packets coming from the specific router to have the same source IP address, the command will work when the router has many interfaces.

The designated interface shall have the IP address linked to the interface. If the designated interface has no IP address or is under a “down” state, the default value will be restored, namely the source IP address shall be determined on the real condition. In order to avoid the case, the IP address shall be added to the interface and the interface shall be ensured under the “up” state.

#### Example

The following Example will use IP address of the interface vlan1 as source IP address of all TACACS+ packets.

```
ip tacacs source-interface vlan1
```

#### Related Command

```
ip radius source-interface
```

### 8.1.3 tacacs-server host

#### Syntax

To designate TACACS+ server in global configuration mode, run command “tacacs server host”. To return to the default setting, use the no form of this command.

```
tacacs-server host ip-address [single-connection | multi-connection] [port integer1]
[timeout integer2] [key string]
```

```
no tacacs-serve ip-address
```

#### Parameters

Parameters	Description
<i>ip-address</i>	IP address of the server
<i>single-connection</i>	(optional) Designating router to maintain the single and open TCP connection for the confirmation from AAA/TACACS+ server.
<i>multi-connection</i>	(Optional) Designating router to maintain the different TCP connection for the different confirmation from AAA/TACACS+ server
<i>Port</i>	(optional) Designating port number of server. The option covers the default port number 49.
<i>integer1</i>	(optional) The port number of server. The range of valid port number is 1 to 65536.
<i>timeout</i>	(optional) Designating the timeout of waiting for server response. It will cover the global timeout set for the server by using the command “tacacs timeout”
<i>integer2</i>	(optional) Setting the value of timeout timer. It is calculated on second.
<i>key</i>	(optional) Designating authentication and encryption key. The secret key shall match with the one used by the program of TACACS+ server. Designating this. It will cover all keys set for the server by command "tacacs key".
<i>string</i>	(optional) Specifying the encrypted key.

#### Default Value

Disabled

#### Command Mode

Global configuration mode

#### Usage Guidelines

The command can be used to search a host according to the specified order by command tacacs-server plus host. As some parameters of tacacs-server host will cover all configurations of commands "tacacs-server timeout" and "tacacs-server key" in global mode, the command can set the communication attribute of each TACACS+ server exclusively. Thus, the security of the network enhanced.

## Example

The following example shows how the designated server negotiates with TACACS+ server whose IP address is 1.1.1.1 and carries out AAA authentication. The command can also designate the TCP port number of the server to 51, the timeout is 3 seconds and the encryption key is tacacs-server key.

```
tacacs -server host 1.1.1.1 single-connection port 51 timeout 3 key a_secret
```

### 8.1.4 tacacs-server key

#### Syntax

To set the encryption key of the communication process between the device and TACACS+ server, run command `tacacs-server key` in global mode. To return to the default setting, use the `no` form of this command.

**tacacs-server key**

**no tacacs-server key**

#### Parameters

Parameters	Description
<i>key</i>	Uses for setting encryption key. The secret key shall match with the one used by the program of TACACS+ server.

#### Command Mode

Global configuration mode

#### Usage Guidelines

You must set the encryption key by command `tacacs-server key` before running TACACS+ protocol. The key must correspond to the key used by TACACS+ server program. All sentence-initial spaces will be ignored and there cannot be any space in the middle of the key.

#### Example

The following example shows how to set the encryption key as testkey.

```
tacacs-server key testkey
```

### 8.1.5 tacacs-server timeout

#### Syntax

To set the timeout of TACACS+ waiting for a server reply, run command `tacacs-server timeout` in global configuration mode. To return to the default setting, use the `no` form of this command.

**tacacs-server timeout *seconds***

**no tacacs-server timeout**

## Parameters

Parameters	Description
<i>seconds</i>	<b>The timeout in seconds (ranges from 1 to 600) The default value is 5 seconds.</b>

## Default Value

5 seconds

## Command Mode

Global configuration mode

## Usage Guidelines

If the command `tacacs-server` sets timeout, it will cover the global timeout set by the command before.

## Example

The following example shows how to change the timeout to 10 seconds:

```
tacacs-server timeout 10
```

**In order to TACACS+ authentication to be worked you need to execute the following commands in global configuration mode:**

```
aaa authentication enable default group tacacs+
```

```
aaa authorization exec default local group tacacs+
```

## Chapter 9 HTTP Configuration Commands

### 9.1 *ip http language*

#### Syntax

To set the prompt language when a command is configured, run the following command.

```
[no] ip http language { english }
```

#### Parameters

Parameters	Description
<i>english</i>	<b>Sets the language to English.</b>

#### Default Value

None

#### Usage Guidelines

This command is configured in global configuration mode.

#### Example

The following example shows how to set the language to English.

```
Switch_config#ip http language english
```

### 9.2 *ip http port*

#### Syntax

To set the HTTP port, run the following command. To return to the default setting, use the no form of this command.

```
ip http port { portNumber }
```

```
no ip http port
```

#### Parameters

Parameters	Description
<i>portNumber</i>	<b>Means the HTTP port's valid range is from 1 to 65535.</b>

#### Default Value

80

#### Usage Guidelines

This command is configured in global configuration mode.

#### Example

The following example shows how to set the HTTP port to 1234.

```
Switch_config#ip http port 1234
```

### **9.3 ip http secure-port**

#### Syntax

To set the HTTPS port, run this command. To return to the default setting, use the no form of this command.

```
ip http secure-port {portNumber}
```

```
no ip http secure-port
```

#### Parameters

Parameters	Description
<i>portNumber</i>	Means the HTTPS port's valid range is from 1 to 65535.

#### Default Value

443

#### Usage Guidelines

This command is configured in global configuration mode.

#### Example

The following example shows how to set the HTTPS port to 1234.

```
Switch_config# ip http secure-port 1234
```

### **9.4 ip http server**

#### Syntax

To set the HTTP service, run this command.

```
[no] ip http server
```

#### Usage Guidelines

This command is set in global configuration mode.

#### Example

The following example shows how to set the HTTP service.

```
Switch_config# ip http server
```

### **9.5 ip http http-access enable**

#### Syntax

```
[no] ip http http-access enable
```

To set the HTTP access mode, run this command.

#### Usage Guidelines



This command is set in global configuration mode and used to access the website, which starts with `http://`.

### Example

The following example shows how to set the HTTP access mode.

```
Switch_config# ip http http-access enable
```

## **9.6 ip http ssl-access enable**

### Syntax

```
[no] ip http ssl-access enable
```

To set the HTTPS access mode, run this command.

### Usage Guidelines

This command is set in global configuration mode and used to access the website, which starts with `https://`.

### Example

The following example shows how to set the HTTPS access mode.

```
Switch_config# ip http ssl-access enable
```

## **9.7 ip http web use-footer**

### Syntax

```
ip http web use-footer
```

To configure “About” option on the Web page, run the command.

```
no ip http web use-footer
```

To remove “About” option on the Web page, run the command.

### Usage Guidelines

This command is set in global configuration mode.

### Example

The following example shows how to hide “About” option on the Web page.

```
Switch_config# no ip http web use-footer
```

## **9.8 ip http web max-vlan**

### Syntax

```
ip http web max-vlan { max-vlan }
```

To set the maximum number of VLAN entries displayed in a web page, run this command.

```
no ip http web max-vlan
```

To resume the default maximum number of VLAN entries to 100, run this command.

## Parameters

Parameters	Description
<i>max-vlan</i>	Means the maximum number of vlan entries in the web page, which ranges from 1 to 4094.

## Default Value

100

## Usage Guidelines

This command is configured in global configuration mode.

## Example

The following example shows how to set the maximum number of VLAN entries displayed in a web page to 123.

```
Switch_config# ip http web max-vlan 123
```

**9.9 ip http web max-macaddr-table**

## Syntax

```
ip http web max-macaddr-table { max-macaddr-table }
```

To configure the max number of MAC address item shown on the Web page, run the command.

```
no ip http web max-macaddr-table
```

To return the max number of MAC address item shown on the Web page to 100, run the command.

## Parameters

Parameters	Description
<i>max-macaddr-table</i>	The max number of MAC address items shown on the Web page, the valid range is 1 to 500.

## Default Value

100

## Usage Guidelines

This command is set in global configuration mode.

## Example

The following example shows how to set the max number of MAC address items on the Web page.

```
Switch_config# ip http web max-macaddr-table 123
```

### 9.10 *ip http web igmp-groups*

#### Syntax

```
ip http web igmp-groups { igmp-groups }
```

To set the maximum number of multicast entries displayed in a web page, run this command.

```
no ip http web igmp-groups
```

To resume the default maximum number of multicast entries to 15, run this command.

#### Parameters

Parameters	Notes:
<i>igmp-groups</i>	Means the maximum number of multicast entries in the web page, which ranges from 1 to 100.

#### Default Value

15

#### Usage Guidelines

This command is configured in global configuration mode.

#### Example

The following example shows how to set the maximum number of multicast entries displayed in a web page to 12.

```
Switch_config#ip http web igmp-groups 12
```

### 9.11 *ip http web portpanel update-interval*

#### Syntax

```
ip http web portpanel update-interval { update-interval }
```

To configure the update interval of the web port panel, run the command.

```
no ip http web portpanel update-interval
```

To return the update interval of the web port panel to 1 minute, run the command.

#### Parameters

Parameters	Notes:
<i>update-interval</i>	The update interval of the web port panel. The valid range is 1 to 5.

#### Default Value

1

#### Usage Guidelines

This command is set in global configuration mode.

### Example

The following example shows how to set the update interval of the web port panel to 3 minutes.

```
Switch_config#ip http web portpanel update-interval 3
```

## 9.12 ip http web portpanel visible

### Syntax

```
ip http web portpanel visible
```

To enable the port panel of the web page visible, run the command.

```
no ip http web portpanel visible
```

To disable the port panel of the web page visible, run the command.

### Usage Guidelines

This command is set in global configuration mode.

### Example

The following example shows how to disable the port panel of the web page.

```
Switch_config#no ip http web portpanel visible
```

## 9.13 ip http web max-syslogs

### Syntax

```
ip http web max-syslogs { max-syslogs }
```

To configure the max number of system logs shown on the Web page, run the command.

```
no ip http web max-syslogs
```

To return the max number of system logs shown on the Web page to 128, run the command.

### Parameters

Parameters	Notes:
<i>max-syslogs</i>	The max number of system logs. The valid range is 100 to 500.

### Default Value

128

### Usage Guidelines

This command is set in global configuration mode.

### Example

The following example shows how to set the max number of system logs to 200.

```
Switch_config#ip http web max-syslogs 200
```

### **9.14 show ip http**

#### Syntax

```
show ip http
```

#### Usage Guidelines

The command is used to browse whether the HTTP server is enabled.

#### Example

```
Switch_config#show ip http
```

```
Http server is running
```

## **Chapter 10 Interface Configuration Commands**

### **10.1 Interface Configuration Commands**

The interface configuration commands include:

- interface
- description
- bandwidth
- delay
- shutdown
- show interface
- show running-config interface

#### **10.1.1 interface**

##### Syntax

To enter the interface configuration mode, run this command. If the logical port is inexistent, you have to create this port first and then enter the port mode. If the physical port is inexistent, the command will fail to be executed. The negative form of this command has different functions for the physical port and the logical port.

##### **[no] interface *port***

To return to the default settings of the physical port, run this command.

```
no interface physical-port
```

To delete the logic interface, run this command.

```
no interface logical-port
```

##### Parameters

Parameters	Notes:
------------	--------

<i>Port</i>	<b>Stands for the existent physical or logical port.</b>
-------------	--

### Default Value

The default mode is not the port mode.

### Usage Guidelines

When you execute this command in configuration mode, you have to enable this command to be in port configuration mode first. When the port command is configured, you shall use the exit command to exit from the port mode.

### Example

The following example shows how to enter the port mode of port g0/1.

```
Switch_config#
Switch_config#interface gigaEthernet0/1
Switch_config_g0/1#exit
Switch_config#
```

## 10.1.2 Description

### Syntax

To set the description information of a port, run the following command.

**[no] description *line***

### Parameters

Parameters	Notes:
<i>line</i>	<b>Stands for the character string of the description information, among which space may exist.</b>

### Default Value

There is no description information by default.

### Usage Guidelines

The command must be configured in port configuration mode.

### Example

The following example shows how to set the description information of port g01/1 to up link.

```
Switch_config# interface gigaEthernet0/1
Switch_config_g0/1# description uplink
```

### 10.1.3 bandwidth

#### Syntax

To set the bandwidth of an interface, run the following command.

**[no] bandwidth** *kilobps*

#### Parameters

Parameters	Notes:
<i>kilobps</i>	port bandwidth, the value ranges from 1 to 10000000(kbps).

#### Default Value

The default value of the 100M port is 100000 and the default value of gigabit port is 1000000.

#### Usage Guidelines

The command must be configured in port configuration mode.

#### Note:

The configured bandwidth does not mean the actual bandwidth of a port, but is used by some protocol to calculate the port cost.

#### Example

The following example shows how to set port g0/1 to 10000000.

```
Switch_config # interface gigaEthernet0/1
```

```
Switch_config_g0/1# bandwidth 10000000
```

### 10.1.4 delay

#### Syntax

To set the delay of an interface, run the following command.

**[no] delay** *tensofmicroseconds*

#### Parameters

Parameters	Notes:
<i>tensofmicroseconds</i>	port delay, the valuen ranges from 1 to 10000000 (10 microseconds)

#### Default Value

The default value of the delay is 1.

#### Usage Guidelines

This command is configured in port configuration mode.

### Example

The following example shows how to set the delay of an interface to 10.

```
Switch_config_g0/1# delay 10
```

### 10.1.5 shutdown

#### Syntax

To enable the port, run this command.

```
[no] shutdown
```

#### Parameters

None

#### Default Value

The physical port is in enabled shutdown status by default.

#### Usage Guidelines

This command can be used in port mode to enable or disable port.

### Example

The following example shows how to enable port g0/1.

```
Switch_config_g0/1#  
Switch_config_g0/1#  
no shutdown Switch_config_g0/1#
```

### 10.1.6 show interface

#### Syntax

To browse the state of an interface, run the following command.

```
show interface <port>
```

#### Parameters

Parameters	Notes:
<i>Port</i>	<b>Name of an interface</b> If a specific port is not in the command, the system will show the statuses of all ports.

#### Default Value

None

#### Usage Guidelines

This command can be used in EXEC and configuration modes to show the physical status and packet reception statistics of a port.



## Example

The following example shows the information about port g0/1:

```
Switch_config# show interface gigaEthernet 0/1:
```

```
GigaEthernet0/1 is administratively down, line protocol is down
```

```
Hardware is Giga-Combo-FX, address is 00e0.0fe4.d083 (bia 00e0.0fe4.d083)
```

```
MTU 1500 bytes, BW 1000000 kbit, DLY 10 usec
```

```
Encapsulation ARPA
```

```
Auto-duplex, Auto-speed
```

```
flow-control off
```

```
5 minutes input rate 0 bits/sec, 0 packets/sec
```

```
5 minutes output rate 0 bits/sec, 0 packets/sec
```

```
Received 0 packets, 0 bytes
```

```
0 broadcasts, 0 multicasts
```

```
0 discard, 0 error, 0 PAUSE
```

```
0 align, 0 FCS, 0 symbol
```

```
0 jabber, 0 oversize, 0 undersize
```

```
0 carriersense, 0 collision, 0 fragment
```

```
0 L3 packets, 0 discards, 0 Header errors
```

```
Transmitted 0 packets, 0 bytes
```

```
0 broadcasts, 0 multicasts
```

```
0 discard, 0 error, 0 PAUSE
```

```
0 sqetest, 0 deferred
```

```
0 single, 0 multiple, 0 excessive, 0 late
```

```
0 L3 forwards
```

### 10.1.7 show running-config interface

#### Syntax

To display the settings of a port, run the following command.

```
show running-config interface port
```

#### Parameters

Parameters	Notes:
<i>Port</i>	Stands for the existent port.

**Default Value**

None

**Usage Guidelines**

This command can be executed in EXEC or configuration mode to browse the settings of a port.

**Example**

The following example shows the settings of port g0/1:

```
Switch_config#show running-config interface g0/1
```

```
Building configuration...
```

```
Current configuration:
```

```
!
```

```
interface GigaEthernet0/1
```

```
shutdown
```

```
description uplink
```

```
bandwidth 10000000
```

```
delay 10
```

```
Switch_config#
```

**10.2 Configuration Example**

The following example shows how to create a VLAN port, set its description information and IP address and browse the status and settings of this port. To browse the port status and configuration, run show command.

```
Switch_config#
```

```
Switch_config# interface vlan1
```

```
Switch_config_v1# description uplink
```

```
Switch_config_v1#
```

```
Switch_config_v1# ip address 192.168.1.1 255.255.255.0
```

```
Switch_config_v1# exit
```

```
Switch_config#
```

```
Switch_config# show running-config interface vlan1
```

```
Building configuration...
```

```
Current configuration:
```

```
!
```

```
interface VLAN1
```

```
description uplink
ip address 192.168.1.1 255.255.255.0
Switch_config# show interface vlan1
VLAN1 is up, line protocol is down
Description: uplink
Hardware is EtherSVI, Address is 00e0.0fe4.d06a(00e0.0fe4.d06a)
Interface address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 kbit, DLY 2000 usec
Encapsulation ARPA
ARP type: ARPA, ARP timeout 04:00:00
Peak input rate 0 pps, output 0 pps
0 packets input, 0 bytes
Received 0 broadcasts, 0 multicasts
0 mpls unicasts, 0 mpls multicasts, 0 mpls input discards 0 input errors, 0 input discards
0 packets output, 0 bytes
Transmitted 0 broadcasts, 0 multicasts
0 mpls unicasts, 0 mpls multicasts, 0 mpls output discards
0 output errors, 0 discards
Switch_config#
```

## Chapter 11 Interface Range Commands

### 11.1 Interface Range

#### Syntax

```
interface range slot/<port1-port2 | port3>[, <port1-port2|port3>]
```

#### Parameters

Name	Usage Guidelines	Value Range
<i>type</i>	Port type	All reasonable port types, except the manager port on the main control board of the cabinet-like switch
<i>slot</i>	Slot number	All legal slot numbers
<i>port1</i>	Starting value of the port numbers	All legal port numbers on a slot
<i>port2</i>	Ending value of the port numbers	All legal port numbers on a slot which are no smaller than port 1
<i>port3</i>	An independent port	All legal port numbers on a slot

#### Default Value

None

#### Usage Guidelines

The command can be used to enter the interface range mode.

#### Example

The following example shows how to enter the port configuration mode of gigabit Ethernet port 1, 2, 3 or 4 on slot 0.

```
switch_config# interface range gigaEthernet 0/1-4
switch_config_if_range#
```

Note:

There is no space at the neither side of the symbol “\_” and the symbol “,”.

## Chapter 12 Port Physical Characteristic Configuration Commands

### 12.1 Port Physical Characteristic Configuration Commands

Configuration commands are shown as follows:

- speed
- duplex
- flow-control

#### 12.1.1 speed

##### Syntax

To set the speed of the interface, ran speed {10 | 100 | 1000 | auto}.

**speed** {10 | 100 | auto} (TX port)

**speed** {100 | 1000 | auto} (Optical port)

**no speed**

##### Parameters

Parameters	Notes:
10, 100,1000	Sets the speed of an interface to 10M, 100M or 1000M.
auto	Sets the speed of the interface to auto.

##### Default Value

The speed of the electrical interface is auto, the speed of the 100M optical interface is 100M and the speed of the 1000M optical interface is 1000M.

##### Usage Guidelines

This command is configured in layer-2 interface configuration mode.

##### Note:

The optical interface speed is fixed. The gigabit optical interface enables auto-negotiation function by default. The optical/electric port cannot support the gigabit and full-duplex at the same time. The ordinary TX port does not support speed 1000.

##### Example

The following example shows how to set the speed of interface g0/1 to 100M.

```
Switch_config# interface g0/1
```

```
Switch_config_g0/1# speed 100
```

#### 12.1.2 duplex

##### Syntax

To set the duplex mode of an interface, run `duplex {auto | full | half}`.

**duplex** {*auto* | *full* | *half*}

**no duplex**

Parameters

Parameters	Description
<i>auto</i>	<b>Automatic negotiation</b>
<i>full</i>	<b>Full duplex</b>
<i>half</i>	<b>Half duplex</b>

Default Value

The electrical interface is in automatic negotiation mode, while the optical interface is in full duplex mode.

Usage Guidelines

This command is configured in layer-2 interface configuration mode.

**Note:**

The duplex mode of the optical interface is fixed, that is, the duplex mode of all optical interfaces is the full duplex mode. The optical/electric port cannot support the gigabit and full-duplex at the same time. There is backpressure in half-duplex mode.

Example

The following example shows how to set the interface g0/1 to the full duplex mode.

```
Switch_config# interface g0/1
```

```
Switch_config_g0/1# duplex full
```

### 12.1.3 flow-control

Syntax

To configure flow control for an interface, run the following command.

**flow-control** { *on* | *off* | *auto* }

Parameters

Parameters	Description
<i>on</i>	<b>Enables the flow control.</b>
<i>off</i>	<b>Disables the flow control.</b>
<i>auto</i>	<b>Auto-negotiation Mode</b>

Default Value

The flow control function is disabled by default.

### Usage Guidelines

The command must be configured in L2 port configuration mode.

### Note:

The difference between “flow-control auto” and “flow-control on” is in the “auto” mode the device sends flow control frame only when it negotiates successfully with the opposite end as the system is compelled to receive flow control frame in both modes.

### Example

The following example shows how to enable the flow control function for port g0/1.

```
Switch_config#int g0/1
```

```
Switch_config_g0/1#flow-control on
```

## Chapter 13 Port Additional Characteristics Configuration Commands

### 13.1 Configuring Port Isolation (Private VLAN-EDGE)

#### 13.1.1 port-protected

##### Syntax

To configure a port isolation group, run the following command. To return to the default setting, use the no form of this command.

**port-protected** *group-id*

**[no]** port-protected *group-id*

##### Parameters

Parameters	Description
<i>group-id</i>	Configures port isolation group 1 to 28.

##### Default Value

None

##### Usage Guidelines

The command can be used to configure the group isolation in global configuration mode.

##### Example

The following example shows how to set ID of the isolation group to 1.

```
Switch_config#port-protected 1
```

### 13.1.2 Description

#### Syntax

To set the port isolation group description, run the following command. To delete the description, use the no form of this command.

**description** *word*

**no description**

#### Parameters

Parameters	Description
<i>Word</i>	<b>Sets the port isolation description. The description covers 31 characters at most.</b>

#### Default Value

None

#### Usage Guidelines

The command can be used to describe the group in global configuration mode.

#### Example

The following example shows how to set ID of the isolation group g1 to 1.

```
Switch-config-p1#description g1
```

### 13.1.3 switchport protected

#### Syntax

To set port isolation, run the following command. To return to the default setting, use the no form of this command.

**switchport protected** *<group-id>*

**no switchport protected**

#### Parameters

Parameters	Description
<i>group-id</i>	<b>Selects the port isolation group 1 to 28.</b>

#### Default Value

None

#### Usage Guidelines

The command must be configured in layer-2 port configuration mode. The system configures isolation not based on groups by default and group-id doesn't need to configure at the end. If configures isolation based on groups, it should be configured in global mode. Only



deleting the isolation on all ports can you reselect isolation based on groups or not based on groups.

### Example

The following example shows how to set isolation of port g0/1 not based on groups. Port isolation will work ONLY within one port-protected group.

```
Switch_config_g0/1#switchport protected 1
```

```
!
```

```
Switch_config_g0/2#switchport protected 1
```

## 13.2 Configuring the Storm Control Command

### Syntax

To configure the storm control function of the port, run the following command. To return to the default setting, use the no form of this command.

```
storm-control {broadcast | multicast | unicast} threshold count
```

```
no storm-control {broadcast | multicast | unicast} threshold
```

### Parameters

Parameters	Description
<i>broadcast</i>   <i>multicast</i>   <i>unicast</i>	<b>Defines broadcast/multicast/unicast storm control.</b>
<i>count</i>	<b>Defines the threshold flux of the storm. 1-65535</b>

### Default Value

The storm control function is disabled by default.

### Usage Guidelines

The command must be configured in L2 port configuration mode.

### Example

The following example shows how to set the unknown unicast-frame storm to 20pps on port g0/1.

```
Switch_config#interface g0/1
```

```
Switch_config_g0/1#storm-control unicast threshold 20
```

## 13.3 Configuring Switchport Rate Limit

### Syntax

To configure the rate limit for a port, run this command. To return to the default setting, use the no form of this command.

```
switchport rate-limit {band | bandwidth percent} {ingress|egress}
```

**no switchport rate-limit{ ingress|egress}**

## Parameters

Parameters	Description
<i>Band</i>	Means the rate of the flow. The step length is 64Kbps.
<i>percent</i>	Means the percentage of the flow. unit 1%
<i>ingress</i>	Functions on the ingress port.
<i>egress</i>	Functions on the egress port.

## Default Value

The rate of the port is not limited by default.

## Usage Guidelines

Layer-2 port configuration mode

## Example

The following example shows how to set the incoming flow rate to 1M on port g0/1.

```
Switch_config#interface g0/1
```

```
Switch_config_g0/1#switchport rate-limit 16 ingress
```

**13.4 Configuring Port Loop Check**

## Syntax

To configure the interval for a port to transmit the loop check packets, run `keepalive second`. To return to the default setting, use the `no` form of this command.

**keepalive** *second*

**[no]** **keepalive** *second*

## Parameters

Parameters	Description
<i>Second</i>	Interval, unit: second.

## Default Value

12 seconds

## Usage Guidelines

The command must be configured in physical interface configuration mode.

## Example

The following example shows how to set the transmission interval to 10 seconds on interface g0/1.

```
Switch_config#interface g0/1
```

```
Switch_config_g0/1#keepalive 10
```

### **13.5 Configuring MAC Address Learning**

#### **Syntax**

To configure the MAC address learning for a port, run `switchport disable-learning`. To return to the default setting, use the `no` form of this command.

**switchport disable-learning**

**[no] switchport disable-learning**

#### **Parameters**

None

#### **Default Value**

The MAC address learning is enabled by default.

#### **Usage Guidelines**

The command must be configured in physical interface configuration mode.

#### **Example**

The following example shows how to disable the MAC address learning on interface `g0/1`.

```
Switch_config#interface g0/1
```

```
Switch_config_g0/1#switchport disable-learning
```

### **13.6 Configuring Port Security**

The port security configuration commands include:

- **switchport port-security mode**
- **switchport port-security dynamic**
- **switchport port-security static**
- **switchport port-security sticky**

#### **13.6.1 switchport port-security mode**

##### **Syntax**

To set the interface security mode, run the following command. To return to the default setting, use the `no` form of this command.

**switchport port-security mode {dynamic | static *accept/reject* | sticky}**

**[no] switchport port-security mode**

##### **Parameters**

None

### Default Value

The port security is disabled by default.

### Usage Guidelines

The command must be configured in physical interface configuration mode.

### Example

The following example shows how to set interface g0/1 to the dynamic port security mode.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1#switchport port-security mode dynamic
```

### 13.6.2 *switchport port-security dynamic*

#### Syntax

To configure the maximum number of MAC addresses when the port is in dynamic security mode, run `switchport port-security dynamic maximum`. To return to the default setting, use the `no` form of this command.

**switchport port-security dynamic maximum** *dynamic\_number*

**[no] switchport port-security dynamic maximum**

#### Parameters

Parameters	Description	Value Range
<i>dynamic_number</i>	The maximum address number that can be learned	1-2048

### Default Value

The number of MAC addresses that can be learned is 1- the maximum number of items in the MAC address table.

### Usage Guidelines

The command must be configured in physical interface configuration mode.

### Example

The following example shows how to set the number of that can be learned MAC addresses of port g0/1 to 10.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1# switchport port-security dynamic maximum 10
```

### 13.6.3 *switchport port-security static mac-address*

#### Syntax

To configure a static security MAC address, run `switchport port-security static mac-address H.H.H`. To return to the default setting, use the `no` form of this command.

**switchport port-security static mac-address H.H.H**

**[no] switchport port-security static mac-address H.H.H**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

The command must be configured in physical interface configuration mode.

#### Example

The following example shows how to set MAC address 0001.0002.0003 to a static security MAC address.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1# switchport port-security static mac-address 1.2.3
```

### 13.6.4 switchport port-security sticky

#### Syntax

To configure the sticky characteristic of MAC address, run the following command. To return to the default setting, use the no form of this command.

**switchport port-security sticky {maximum sticky\_number | mac-address H.H.H | aging-time aging\_time}**

**[no] switchport port-security sticky {maximum | mac-address H.H.H | aging-time}**

#### Parameters

Parameters	Description
<i>sticky_number</i>	<b>The maximum address number that can be learned. The default is 100 and the value range is from 1 to 2048.</b>
<i>H.H.H</i>	<b>Mac Address</b>
<i>aging_time</i>	<b>aging time Unit: minute, the default value is 0 and the value range is 0 to 100.</b>

#### Default Value

There is no sticky of mac address by default.

#### Usage Guidelines

The command must be configured in physical interface configuration mode.

#### Example

The following example shows how to set mac: 4433.0002.0021 to the sticky mac manually.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1# switchport port-security sticky mac-address 4433.0002.0021
```

### 13.7 Configuring Port Binding

#### Syntax

To bind a MAC address to a IP address, run `switchport port-security bind|block`

```
{ip|arp|both-arp-ip ip-addr | ipv6 ipv6-addr | mac mac-addr }.
```

To cancel the address binding one by one or to exit the port binding state by cancelling all addresses on the port, run `no switchport port-security bind|block`

```
{ip|arp| both-arp-ip ip-addr | ipv6 ipv6-addr | mac mac-addr}.
```

```
switchport port-security bind|block {ip|arp|both-arp-ip ip-addr| ipv6 ipv6-addr | mac mac-addr}
```

```
no switchport port-security bind|block {ip|arp| both-arp-ip ip-addr | ipv6 ipv6-addr | mac mac-addr}
```

#### Parameters

Parameters	Description	Value Range
<i>ip-addr</i>	IP address	A.B.C.D
<i>Mac-addr</i>	Stands for the MAC address.	H.H.H

#### Default Value

None

#### Usage Guidelines

It works in layer-2 port configuration mode.

The port binding function is forbidden by default. However, if one address is bound, the port is then in binding state unless you use the negative form of this command to clear all bound address items.

#### Example

The following example shows how to bind IP address 1.2.3.4 to MAC address 0001.0001.1111 on interface g0/1 to decline the IP packets and ARP packets from the bound address.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1# switchport port-security block both-arp-ip 1.2.3.4 mac 0001.0001.1111
```

### 13.8 SVL/IVL

#### Syntax

To set SVL, run the following command.

**[no]vlan shared-learning**

Parameters

None

Default Value

VLAN IVL on the port

Usage Guidelines

This command is run in global configuration mode.

Example

The following example shows how to set SVL.

```
Switch_config#vlan shared-learning
```

### 13.9 Configuring Link Scan Commands

Syntax

To set the scan interval of an interface, run the following command.

**[no] Link scan [normal | fast] interval**

Parameters

Parameters	Description
<i>[normal   fast]</i>	<b>Normal means standard link scan mode. Fast means fast link scan mode.</b>
<i>interval</i>	<b>scan interval, unit 1ms, 10-1000.</b>
<i>aging_time</i>	<b>aging time Unit: minute, the default value is 0 and the value range is 0 to 100.</b>

Default Value

The scan interval is 500ms in standard mode by default. Fast mode, the default interval is 10ms.

Usage Guidelines

This command is configured in global configuration mode. The Fast mode is mainly used for cooperating with the protocol, for instance, RSTP. The Normal mode is mainly used for finding up/down.

Example

The following example shows how to set the scan interval of a switch to 20ms.

```
Link scan normal 20
```

### 13.10 Configuring the Enhanced Link State Detection Command

#### Syntax

To enable/disable the enhanced link state detection command, run the following command.

**[no] switchport enhanced-link**

#### Parameters

None

#### Default Value

Disabled.

#### Usage Guidelines

The command must be configured in port configuration mode.

#### Example

The following example shows how to enable the enhanced link state detection on interface g0/1:

```
Switch_config#interface g0/1
Switch_config_g0/1#switchport enhanced-link
```

### 13.11 Configuring System MTU

#### Syntax

To configure the value of system mtu, run the following command.

**[no] system mtu *mtu***

#### Parameters

Parameters	Description
<i>mtu</i>	Sets the value of system mtu, 1500-9216.

#### Default Value

The default mtu is 1500 bytes.

#### Usage Guidelines

This command is configured in global configuration mode.

#### Example

The following example shows how to set system mtu to 2000 bytes.

```
Switch#config
Switch_config#system mtu 2000
```



## NOTICE

When inter-connecting with other-brand switches (for example Cisco IOS-XE), it's recommended to change the default MTU size from 1500 to 2000.

## Chapter 14 Port Mirroring Configuration Commands

### 14.1 Port Mirroring Configuration Commands

Port mirroring configuration commands include:

- mirror
- show mirror

#### 14.1.1 mirror

##### Syntax

To set port mirror, run this command.

```
[no] mirror session session_number {destination {interface interface-id}
{rspan vid tpid} | source {interface interface-id [, | -] [rx | tx | both]}
```

##### Parameters

Parameters	Description
<i>session_number</i>	Number of port mirroring Value range: 1-4
<i>destination</i>	Information about destination port mirroring
<i>vid</i>	VID of the tag of remote mirroring
<i>TPID</i>	TPID of the tag of remote mirroring
<i>source</i>	Information about the mirrored port
<i>rx   tx   both</i>	Data flow that will be mirrored Rx means that only the input data is mirrored; tx means that only the output data is mirrored; both means both the input data and the output data are mirrored.

##### Default Value

None

##### Usage Guidelines

This command is configured in global configuration mode.

##### Note:

The unknown unicast packets including the unknown unicast and the broadcast take the source whose mirroring number is 1 as the source port in output mirroring.

##### Example

Local mirroring: The following example shows how to set interface g0/2 as the output mirroring of interface g0/1.

```
Switch_config# mirror session 1 destination interface g0/2
```

```
Switch_config# mirror session 1 source interface g0/1
```

Remote mirroring: The following example shows how to set interface g0/2 as the local output mirroring of interface g0/1. The VLAN of remote mirroring is 100. TPID is 0x8100.

```
Switch_config# mirror session 1 destination interface g0/2 rspan 100 0x8100
```

```
Switch_config# mirror session 1 source interface g0/1
```

### 14.1.2 show mirror

#### Syntax

To display the configuration information about port mirroring, run the following command.

```
show mirror [session session_number]
```

#### Parameters

Parameters	Description
<i>session_number</i>	<b>Number of port mirroring Value range: 1-4</b>

#### Default Value

None

#### Usage Guidelines

This command can be used to display the information about port mirroring.

#### Example

The following example shows how to display the information of port mirroring on port 1.

```
Switch_config#show mirror session 1
```

```
Session 1
```

```
-----
```

```
Destination Ports: g0/3 Source Ports:
```

```
RX Only:      None
```

```
TX Only:      None
```

```
Both:         g0/2
```

## Chapter 15 MAC Address Configuration Commands

### 15.1 MAC Address Configuration Commands

#### 15.1.1 mac address-table static

##### Syntax

To add a static MAC address, run `mac address-table static mac-addr vlan vlan-id interface interface-id`. To cancel the static MAC address, run `no mac address-table static mac-addr vlan vlan-id interface interface-id`.

`mac address-table static mac-addr vlan vlan-id interface interface-id`

**[no] mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

##### Parameters

Parameters	Description
<i>mac-addr</i>	<b>MAC address Value range: H.H.H</b>
<i>vlan-id</i>	<b>A VLAN that the MAC address belongs to Value range: 1-4094</b>
<i>interface-id</i>	<b>Physical port that the MAC address belongs to.</b>

##### Default Value

None

##### Usage Guidelines

This command is configured in global configuration mode.

##### Example

The following example shows how to bind MAC address 0004.5600.67ab to port g0/2 of VLAN1.

```
Switch_config# mac address-table static 0004.5600.67ab vlan 1 interface g0/2
```

#### 15.1.2 mac address-table aging-time

##### Syntax

To configure the aging time of the MAC address table, run the following command.

**mac address-table aging-time** [0 | 10-1000000]

##### Parameters

Parameters	Description
0	<b>Means that the MAC address never ages.</b>
10-1000000	<b>Aging time of the MAC address whose unit is second</b>

### Default Value

300s

### Usage Guidelines

This command is configured in global configuration mode.

### Example

The following example shows how to set the aging time of the MAC address to 100 seconds.

```
Switch_config# mac address-table aging-time 100
```

### 15.1.3 mac address-table blackhole

#### Syntax

To add or delete a black hole MAC address, run the following command.

```
[no] mac address-table blackhole mac-addr vlan vlan-id
```

#### Parameters

Parameters	Description
<i>mac-addr</i>	MAC address Value range: H.H.H
<i>vlan-id</i>	A VLAN that the MAC address belongs to Value range: 1-4094

### Default Value

None

### Usage Guidelines

This command is configured in global configuration mode.

### Example

The following example shows how to configure the address 0004.5600.67ab to the black hole mac on VLAN1.

```
Switch_config# mac address-table blackhole 0004.5600.67ab vlan 1
```

### 15.1.4 show mac address-table

#### Syntax

To display the MAC address table of the switch, run the following command.

```
show mac address-table [dynamic [interface interface-id | vlan vlan-id] | static | brief | multicast | interface interface-id | vlan vlan-id | H.H.H | blackhole]
```

#### Parameters

Parameters	Description
<i>dynamic</i>	Dynamically-learned MAC address table

<i>interface-id</i>	<b>Name of an interface</b>
<i>vlan-id</i>	<b>VLAN ID Value range: 1-4094</b>
<i>static</i>	<b>Static MAC address table</b>
<i>brief</i>	<b>Brief information about the MAC address</b>
<i>multicast</i>	<b>Multicast MAC address table</b>
<i>Interface</i>	<b>Interface's MAC address table</b>
<i>Vlan</i>	<b>Vlan mac address table</b>
<i>H.H.H</i>	<b>Specific address</b>
<i>Blackhole</i>	<b>Blackhole MAC address;</b>

### Default Value

None

### Usage Guidelines

This command is used to display the MAC address table.

### Example

The following example shows how to display all dynamic MAC address tables.

```
Switch_config#show mac address-table
```

Mac Address Table (Total 2)

```

-----
Vlan          Mac Address          Type          Ports
-----
1             0026.5a7c.fad3      DYNAMIC      g0/2
1             0000.0000.0004      DYNAMIC      g0/2

```

### 15.1.5 clear mac address-table

#### Syntax

To delete the dynamic MAC address, run the following command.

```
clear mac address-table dynamic [address mac-addr | interface interface-id | vlan vlan-id]
```

#### Parameters

Parameters	Description
<i>mac-addr</i>	<b>MAC address Value range: H.H.H</b>
<i>interface-id</i>	<b>Means a name of a L2 interface.</b>
<i>vlan-id</i>	<b>VLAN ID Value range: 1-4094</b>

### Default Value

None

### Usage Guidelines

This command is used in EXEC mode.

### Example

The following example shows how to clear all dynamically-learned MAC addresses on interface g0/2.

```
Switch# clear mac address-table dynamic interface g0/2
```

## Chapter 16 MAC Access List Configuration Commands

### 16.1 MAC Access List Configuration Commands

The MAC access list configuration commands include:

- mac access-list
- permit
- deny
- mac access-group

#### 16.1.1 mac access-list

### Syntax

To add or cancel a MAC access list, run the following command.

```
[no] mac access-list name
```

### Parameters

Parameters	Description
<i>name</i>	MAC: Name of the MAC access list

### Default Value

When there is a rule in the access list, an item- deny any any- will be added to the end by default and the item will not show.

### Usage Guidelines

This command is run in global configuration mode.

### Example

The following example shows how to configure a mac-acl MAC access list.

```
Switch-config# mac access-list mac-acl
```

Switch-config-macl#

### 16.1.2 permit

#### Syntax

To add or cancel an item to or from the MAC access list, run the following command.

```
[no] permit {any | host src-mac-addr | src-mac-addr src-mac-mask} {any | host dst-mac-addr | dst-mac-addr dst-mac-mask} [arp [{any | src-ip-addr} {any | dst-ip-addr}] | ethertype]
```

#### Parameters

Parameters	Description	Value Range
<i>any</i>	Any value	—
<i>host</i>	Chassis	—
<i>src-mac-addr</i>	Stands for source MAC address	H.H.H
<i>src-mac-mask</i>	Stands for source mac mask	H.H.H
<i>dst-mac-addr</i>	Stands for destination MAC address	H.H.H
<i>dst-mac-mask</i>	Stands for destination mac mask	H.H.H
<i>arp</i>	Stands for matched arp packets	—
<i>src-ip-addr</i>	Stands for source IP address	A.B.C.D
<i>dst-ip-addr</i>	Stands for the destination IP address	A.B.C.D
<i>ethertype</i>	Type of the matched Ethernet packet	0x0600-0xFFFF

#### Default Value

All items are rejected.

#### Usage Guidelines

This command is running in MAC access list configuration mode.

#### Example

The following example shows how to set the MAC address of a host to 1234.5678.abcd.

```
Switch-config-macl#permit host 1234.5678.abcd any
```

### 16.1.3 deny

#### Syntax

To add or cancel an item rejected by the MAC access list, run the following command.

```
[no] deny {any | host src-mac-addr | src-mac-addr src-mac-mask} {any | host dst-mac-addr | dst-mac-addr dst-mac-mask}[ arp [{any | src-ip-addr} {any | dst-ip-addr}] | ethertype]
```

## Parameters

Parameters	Description	Value Range
<i>any</i>	Any value	—
<i>host</i>	Chassis	—
<i>src-mac-addr</i>	Stands for source MAC address	H.H.H
<i>src-mac-mask</i>	Stands for source mac mask	H.H.H
<i>dst-mac-addr</i>	Stands for destination MAC address	H.H.H
<i>dst-mac-mask</i>	Stands for destination mac mask	H.H.H
<i>arp</i>	Stands for matched arp packets	—
<i>src-ip-addr</i>	Stands for source IP address	A.B.C.D
<i>dst-ip-addr</i>	Stands for the destination IP address	A.B.C.D
<i>ethertype</i>	Type of the matched Ethernet packet	0x0600-0xFFFF

## Default Value

All items are rejected.

## Usage Guidelines

This command is running in MAC access list configuration mode.

## Example

The following example shows how to reject a host whose MAC address is 1234.5678.abcd.

```
Switch-config-macl#deny host 1234.5678.abcd any
```

**16.1.4 mac access-group**

## Syntax

Global :

To apply the established MAC access list to an interface or in the global mode or cancel a MAC access list which is already applied to an interface or in the global mode, run the following command.

```
mac access-group name [vlan {word | add word | remove word}]
```

```
[no] mac access-group name [vlan]
```

## Port

```
[no] mac access-group name
```

## Parameters



Parameters	Description
<i>name</i>	<b>MAC: Name of the MAC access list</b>
<i>Vlan</i>	<b>THE ACCESS LIST IS APPLIED IN INGRESS.</b>
<i>Word</i>	<b>VLAN RANGE TABLE</b>
<i>add</i>	<b>ADD VLAN RANGE TABLE</b>
<i>remove</i>	<b>DELETE VLAN RANGE TABLE</b>

### Default Value

No MAC access list is applied to an interface.

### Usage Guidelines

This command is configured in layer-2 interface configuration mode or the interface configuration mode. If there is no access list, an access list with the empty rule will be created.

### Example

The following example shows how to configure the macacl MAC access list on interface g0/1.

```
Switch_config_g0/1#mac access-group macacl
```

## Chapter 17 802.1x Configuration Commands

### 17.1 802.1x Configuration Commands

802.1x configuration commands include:

- dot1x enable
- dot1x port-control
- dot1x authentication multiple-hosts
- dot1x authentication multiple-auth
- dot1x default
- dot1x reauth-max
- dot1x re-authentication
- dot1x timeout quiet-period
- dot1x timeout re-authperiod
- dot1x timeout tx-period
- dot1x mab
- dot1x mabformat
- dot1x user-permit

- dot1x authentication method
- dot1x accounting enable
- dot1x accounting method
- dot1x authen-type, dot1x authentication type
- dot1x guest-vlan
- dot1x guest-vlan id
- dot1x forbid multi-network-adapter
- dot1x keepalive
- aaa authentication dot1x
- debug dot1x error
- debug dot1x state
- debug dot1x packet
- show dot1x

### ***17.1.1 dot1x enable***

#### **Syntax**

**dot1x enable**

**no dot1x enable**

#### **Parameters**

None

#### **Default Value**

None

#### **Usage Guidelines**

If the 802.1x function is not enabled, you cannot start it on an interface. If the 802.1x function is forbidden, all interfaces have no the 802.1x function, and at the same time, all 802.1x packets will not be received by CPU but can be forwarded in VLAN like normal multicast packets.

#### **Command Mode**

Global configuration mode

#### **Example**

The following example shows how to enable dot1x.

```
Switch_config#dot1x enable Switch_config #
```

### 17.1.2 dot1x port-control

#### Syntax

**dot1x port-control {auto|force-authorized|force-unauthorized|misc-mab}**

**no dot1x port-control**

#### Parameters

Parameters	Description
<i>auto</i>	Enables the 802.1x authentication mode.
<i>force-authorized</i>	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required.
<i>force-unauthorized</i>	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.
<i>Misc-mab</i>	The hybrid mode of multi-user and mab authentication

#### Default Value

force-authorized

#### Usage Guidelines

The 802.1x protocol is an interface-based two-layer authentication mode. You can run the auto command to enable the authentication mode. This authentication mode can be configured only on the physical interface and the interface's attributes cannot include VLAN backbone, dynamical access, security port or listening port.

#### Command Mode

Port configuration mode

#### Example

The following example shows how to enable 802.1x on interface g0/1.

```
Switch_config_g0/1# dot1x port-control auto
```

```
Switch_config_g0/1#
```

The following example shows how to firstly set interface g0/1 to the VLAN backbone and then enable 802.1x.

```
Switch_config_g0/1#switchport mode trunk
```

```
Switch_config_g0/1#dot1x port-control auto
```

```
802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(g0/1)
```

```
Switch_config_g0/1#
```

### 17.1.3 dot1x authentication multiple-hosts

#### Syntax

**dot1x authentication multiple-hosts****no dot1x authentication multiple-hosts****Parameters**

None

**Default Value**

Disabled

**Usage Guidelines**

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. When one user passes the authentication, the port sets to the “up” state. Other users can access the port without authentication.

Note: After modifying the multi-host authentication mode, all users of the port will be authenticated again.

**Command Mode**

Port configuration mode

**Example**

The following example shows how to enable multi-hosts authentication on interface g0/1.

```
Switch_config_g0/1# dot1x authentication multiple-hosts
```

```
Switch_config_g0/1#
```

**17.1.4 dot1x authentication multiple-auth****Syntax****dot1x authentication multiple-auth****no dot1x authentication multiple-auth****Parameters**

None

**Default Value**

Disabled

**Usage Guidelines**

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. When only one user passes its authentication, the interface will be up; only when all users fail in their authentication, in another word, only when no successfully authenticated user exist on the interface, the interface will be down. This mechanism gives guarantee to respective authentication for each user and if a user fails in its authentication, other users still have the normal access rights.

Note: The multi-auth mode cannot coexist with guest vlan or mab. If an interface is in multi-authen mode, all users on the interface will be authenticated again.

## Command Mode

Port configuration mode

## Example

The following example shows how to enable multi-auth authentication on interface g0/1.

```
Switch_config_g0/1# dot1x authentication multiple-auth
```

```
Switch_config_g0/1#
```

### 17.1.5 dot1x default

#### Syntax

**dot1x default**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to resume all global configurations to the default settings.

## Command Mode

Global configuration mode

## Example

The following example shows how to resume all dot1x configuration parameters to their default values.

```
Switch_config #dot1x default
```

```
Switch_config #
```

### 17.1.6 dot1x reauth-max

#### Syntax

**dot1x reauth-max** *count*

**no dot1x reauth-max**

#### Parameters

Parameters	Description
<i>count</i>	Maximum authentication re-try times, ranging between 1 and 10

#### Default Value

---

5

### Usage Guidelines

This command is used to set the authentication retry times. If the retry times exceeds the maximum retry times and the client has no response, the authentication is mounted.

### Command Mode

Global configuration mode

### Example

The following example shows how to configure the maximum times of dot1x identity authentication request to 4.

```
Switch_config #dot1x reauth-max 4
```

```
Switch_config #
```

### *17.1.7 dot1x re-authentication*

#### Syntax

**dot1x re-authentication**

**no dot1x re-authentication**

#### Parameters

None

#### Default Value

None

### Usage Guidelines

After an interface passes authentication, the interface will still perform authentication to hosts in a certain period. You can run `dot1x timeout re-auth period` to configure the period.

### Command Mode

Global configuration mode

### Example

The following example shows how to enable the re-authentication function.

```
Switch_config #dot1x re-authentication
```

```
Switch_config #
```

### *17.1.8 dot1x timeout quiet-period*

#### Syntax

**dot1x timeout quiet-period time**

**no dot1x timeout quiet-period**

## Parameters

Parameters	Description
<i>time</i>	Period for restarting dot1x authentication, ranging between 0 and 65535 seconds

## Default Value

60s

## Usage Guidelines

There is a certain period when the switch cannot perform any authentication after the previous authentication fails.

## Command Mode

Global configuration mode

## Example

The following example shows how to set the value of quiet-period to 40.

```
Switch_config #dot1x timeout quiet-period 40
```

```
Switch_config #
```

**17.1.9 dot1x timeout re-authperiod**

## Syntax

```
dot1x timeout re-authperiod time
```

```
no dot1x timeout re-authperiod
```

## Parameters

Parameters	Description
<i>time</i>	dot1x re-authentication period, ranging between 1 and 4294967295s

## Default Value

3600s

## Usage Guidelines

This command validates only when the re-authentication function is enabled.

## Command Mode

Global configuration mode

## Example

The following example shows how to set the dot1x re-authentication period to 7200 seconds.

```
Switch_config # dot1x timeout re-authperiod 7200
```

```
Switch_config #
```

### 17.1.10 *dot1x timeout tx-period*

#### Syntax

**dot1x timeout tx-period time**

**no dot1x timeout tx-period**

#### Parameters

Parameters	Description
<i>time</i>	Time which ranges between 1 and 65535 seconds

#### Default Value

30s

#### Usage Guidelines

This command is used to set the client's authentication request response interval. If the interval is exceeded, the switch would retransmit the authentication request.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to set the transmission frequency to 24.

```
Switch_config # dot1x timeout tx-period 24
```

```
Switch_config #
```

### 17.1.11 *dot1x mab*

#### Syntax

**dot1x mab**

**no dot1x mab**

#### Parameters

None

#### Default Value

The debugging switch is disabled.

#### Usage Guidelines



When a peer device cannot run the 802.1x client software, the switch will adopt the MAB authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication.

When the MAB authentication is enabled and the peer device, however, neither sends the eapol\_start packet nor responds to the request\_identity packet and exceeds the timeout threshold, the switch regards this case as the evidence of not support the 802.1x authentication client on the peer device and then turns to the MAB authentication. When the switch sends the gained MAC address as the username and password to the Radius server for authentication, the authentication will still not succeed until the Radius server has authorized this MAC address.

**Note:** The MAB authentication mode cannot coexist with the multi-auth mode.

## Command Mode

Port configuration mode

## Example

The following example shows how to enable mab authentication on port g0/1.

```
Switch_config_g0/1# dot1x mab
```

```
Switch_config_g0/1#
```

### 17.1.12 dot1x mabformat

#### Syntax

**dot1x mabformat {1|2|3|4|5|6}**

**no dot1x mabformat**

#### Parameters

Parameters	Description
1	Format of the MAC address: aa:bb:cc:dd:ee:ff
2	Format of the MAC address: aa:bb:cc:dd:ee:ff
3	Format of the MAC address: aabbccddeeff
4	Format of the MAC address: AABBCCDDEEFF
5	Format of the MAC address: aa-bb-cc-dd-ee-ff
6	Format of the MAC address: AA-BB-CC-DD-EE-FF

#### Default Value

The default is 1.

#### Usage Guidelines

When the MAB authentication is enabled, you can set the format of the MAC address to the Radius server through this command.

## Command Mode

Global configuration mode

## Example

The following example shows how to set the format of MAC to 3.

```
Switch_config # dot1x mabformat 3
```

```
Switch_config #
```

### *17.1.13 dot1x user-permit*

## Syntax

```
dot1x user-permit xxx yyy zzz
```

```
no dot1x user-permit
```

## Parameters

Parameters	Description
xxx	A user name
yyy	A user name
zzz	A user name

## Default Value

No user is bound and all users would pass.

## Usage Guidelines

This command can be used to bind users on an interface. Each interface can be bound to up to eight users. When the 802.1x authentication is enabled, the authentication is performed only to those bound users. However, to those unbound users, the authentication must fail.

## Command Mode

Port configuration mode

## Example

The following example shows how to bind users a, b, c and d on interface g0/1.

```
Switch_config _g0/1# dot1x user-permit a b c d
```

```
Switch_config _g0/1#
```

### *17.1.14 dot1x authentication method*

## Syntax

```
dot1x authentication method xxx
```

```
no dot1x authentication method
```

## Parameters

Parameters	Description
xxx	Method name

## Default Value

Default method

## Usage Guidelines

This command is used to configure the authentication method which must be one of authentication methods provided by AAA. One interface only uses one authentication method. When AAA performs authentication to the 802.1x user, AAA would select the configured authentication method to perform the authentication.

## Command Mode

Port configuration mode

## Example

The following example shows how to set the authentication method on interface g0/1 to abcd which applies the local username for authentication and that on interface g0/2 to efgh which applies the remote radius authentication.

```
Switch_config #aaa authentication dot1x abcd local
```

```
Switch_config #aaa authentication dot1x efgh group radius
```

```
Switch_config #int g0/1
```

```
Switch_config _g0/1# dot1x authentication method abcd
```

```
Switch_config _g0/1# int g0/2
```

```
Switch_config _g0/2# dot1x authentication method efgh
```

### *17.1.15 dot1x accounting enable*

## Syntax

**dot1x accounting enable**

**no dot1x accounting enable**

## Parameters

None

## Default Value

The accounting service is disabled by default.

## Usage Guidelines

This command is used to enable the accounting function on a port which runs with the authentication function. You'd better enable the dot1x re-authentication function when the accounting function is running.

### Command Mode

Port configuration mode

### Example

The following example shows how to configure the dot1x authentication function on interface g0/1 and enable the accounting function.

```
Switch_config #dot1x enable
Switch_config #int g0/1
Switch_config _g0/1# dot1x port auto
Switch_config _g0/1# dot1x accounting enable
```

#### 17.1.16 dot1x accounting method

### Syntax

**dot1x accounting method** xxx

**no dot1x accounting method**

### Parameters

Parameters	Description
xxx	Name of the accounting method

### Default Value

Default method

### Usage Guidelines

This command is used to configure an accounting method on a port. This method must be one of the accounting methods provided by AAA. Each port has only one accounting method. When the dot1x accounting function is enabled, this method will be used for accounting.

### Command Mode

Port configuration mode

### Example

The following example shows how to set the accounting method on interface g0/1 to abcd, which uses the radius server.

```
Switch_config # aaa accounting network abcd start-stop group radius
Switch_config #radius host 192.168.20.100
```

```
Switch_config #int g0/1
```

```
Switch_config _g0/1# dot1x accounting method abcd
```

### *17.1.17 dot1x authen-type, dot1x authentication type*

#### Syntax

To configure the dot1x authentication type in global configuration mode, run `dot1x authen-type`; to resume the default settings in global configuration mode, run `no dot1x authen-type`.

**dot1x authen-type {chap|eap}**

**no dot1x authen-type**

To configure the dot1x authentication type on an interface, run `dot1x authentication type`; to resume the default settings on an interface, run `no dot1x authentication type`.

**dot1x authentication type {chap|eap}**

**no dot1x authentication type**

#### Parameters

None

#### Default Value

The default dot1x authentication type is `eap`.

The default dot1x authentication type in global configuration mode is also used applied by default in interface configuration mode.

#### Usage Guidelines

The authentication type decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

#### Command Mode

Interface or global configuration mode

#### Example

The following example shows how to set the authentication type on interface `g0/1` to `chap` and the global authentication type to `eap`.

```
Switch_config #dot1x authen-type eap
```

```
Switch_config #int g0/1
```

```
Switch_config _g0/1# dot1x authentication type chap
```

### 17.1.18 dot1x guest-vlan

#### Syntax

To enable the guest-vlan function of dot1x in global configuration mode, run `dot1x guest-vlan`. To disable the guest-vlan function of dot1x in global configuration mode, run `no dot1x guest-vlan`.

```
dot1x guest-vlan
```

```
no dot1x guest-vlan
```

#### Parameters

None

#### Default Value

The debugging switch is disabled.

#### Usage Guidelines

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the `dot1x guest-vlan id` command.

Note: This command cannot be set together with the `multiple-auth` command.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to enable the guest-vlan function in global configuration mode.

```
Switch_config #dot1x guest-vlan
```

### 17.1.19 dot1x guest-vlan id

#### Syntax

To configure the value of `dot1x guest-vlan id` on an interface, run `dot1x guest-vlan id`; to resume the default value 0, run `no dot1x guest-vlan`.

```
dot1x guest-vlan id
```

```
no dot1x guest-vlan
```

#### Parameters

ID: stands for the value of guest vlan, which can be any vlan ID configured in the system.

#### Default Value

None

## Usage Guidelines

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the dot1x guest-vlan id command.

Note: This command cannot be set together with the multiple-auth command.

## Command Mode

Port configuration mode

## Example

The following example shows how to configure the guest-vlan id on port g0/1.

```
Switch_config_g0/1#dot1x guest-vlan 2
```

### *17.1.20 dot1x forbid multi-network-adapter*

#### Syntax

To forbid the supplicant of the multi-network-adapter on an interface, run `dot1x forbid multi-network-adapter`. To resume the default settings, run `no dot1x forbid multi-network-adapter`.

**dot1x forbid multi-network-adapter**

**no dot1x forbid multi-network-adapter**

#### Parameters

None

#### Default Value

None

## Usage Guidelines

This command can be used to forbid the supplicant terminal with multiple network adapters, preventing an agent from being occurred.

## Command Mode

Port configuration mode

## Example

The following example shows how to forbid the supplicant terminal with multiple network adapters on port g0/1.

```
Switch_config_g0/1 # dot1x forbid multi-network-adapter
```

### *17.1.21 dot1x keepalive*

#### Syntax

---

The following example shows how to enable or disable the keepalive detection for the authentication user.

**dot1x keepalive**

**no dot1x keepalive**

#### Parameters

None

#### Default Value

Enabled

#### Usage Guidelines

The default is enable the keepalive detection.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to enable/disable the keepalive detection for the authentication user, run the above commands.

```
Switch_config #no dot1x keepalive
```

```
Switch_config #
```

#### 17.1.22 aaa authentication dot1x

#### Syntax

```
aaa authentication dot1x {default | word} method1 [ method2...]
```

```
no aaa authentication dot1x {default | word}
```

#### Parameters

Parameters	Description
<i>default</i>	<b>Default method</b> Uses the authentication method when command dot1x authentication method does not run.
<i>word</i>	<b>Designate the name of the authentication method</b>
<i>method1</i> [ <i>method2...</i> ]	<b>group radius, local, local-case, none</b>

#### Default Value

None

#### Usage Guidelines



The method parameter provides a series of methods to authenticate the password of the client host. You'd better adopt the radius as the AAA authentication mode of 802.1x. You can also use the local configuration data for authentication, such as user password saved in the local configuration.

### Command Mode

Global configuration mode

### Example

The following example shows how to configure the dot1x authentication method to RADIUS.

```
Switch_config #aaa authentication dot1x default group radius
```

```
Switch_config #
```

### *17.1.23 debug dot1x errors*

#### Syntax

```
debug dot1x errors
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to export all error information occurred during dot1x running. The error information can help locating the errors.

### *17.1.24 debug dot1x state*

#### Syntax

```
debug dot1x state
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

The following shows the format of information output:

```
2003-3-18 17:40:09 802.1x:AuthSM(G0/1) state Connecting-> Authenticating, event rxRespId
```

```
2003-3-18 17:40:09 802.1x:G0/1 Create user for Enter authentication
```

```
2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Idle-> Response, event authStart
```

```
2003-3-18 17:40:09 802.1x:G0/1 user "myname" denied, Authentication Force Failed
```

2003-3-18 17:40:09 802.1x:G0/1 Authentication Fail

2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Response-> Fail, event aFail

### 17.1.25 debug dot1x packet

#### Syntax

**debug dot1x packet**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

2003-3-18 17:40:09 802.1xG0/1 Tx --> Supplicant(0008.74bb.d21f)

EAPOL ver:01, type:00, len:5

EAP code:01, id:03, type:01, len:5

00

2003-3-18 17:40:09 802.1x:G0/1 Rx <-- Supplicant(0008.74bb.d21f)

EAPOL ver:01, type:00, len:10

EAP code:02, id:03, type:01, len:10

62 64 63 6f 6d a5

### 17.1.26 show dot1x

#### Syntax

To display the 802.1x configuration information, run the following command.

**show dot1x** [*interface intf-id* | *statistics* | *misc-mab-db*]

#### Parameters

Parameters	Description
<i>interface</i>	Displays dot1x interface information.
<i>Intf-id</i>	Stands for a specific physical interface.
<i>statistics</i>	Displays dot1x statistics information.
<i>misc-mab-db</i>	Displays dot1x hybrid Mab database

#### Default Value

None

#### Usage Guidelines

This command is used to display the 802.1x configuration information.

### Command Mode

EXEC mode or configuration mode

### Example

The following example shows how to display 802.1x configuration information.

```
Switch_config#show dot1x
```

```
802.1X Parameters
```

```
reAuthen      No
```

```
reAuth-Period    3
```

```
quiet-Period 10
```

```
Tx-Period    30
```

```
Supp-timeout30
```

```
Server-timeout 30
```

```
reAuth-max    4
```

```
max-request  2
```

```
authen-type  Eap
```

```
IEEE 802.1x on port G0/1 enabled
```

```
Authorized    Yes
```

```
Authen Type  Eap
```

```
Authen Method  default
```

```
Permit Users  All Users
```

```
Multiple Hosts    Disallowed
```

```
Supplicant    aaa(0008.74bb.d21f)
```

```
Current Identifier    21
```

```
Authenticator State Machine
```

```
State  Authenticated
```

```
Reauth Count    0
```

```
Backend State Machine
```

```
State  Idle
```

```
Request Count    0
```

```
Identifier (Server)
```

```
Port Timer Machine 20
```

Auth Tx While Time 16

Backend While Time 16

reAuth Wait Time 3

Hold Wait Time 0

## Chapter 18 VLAN Configuration Commands

### 18.1 VLAN Configuration Commands

The VLAN configuration commands include:

- vlan
- name
- dot1q-tunnel
- switchport pvid
- switchport mode
- switchport trunk
- show vlan
- show interface vlan

#### 18.1.1 vlan

##### Syntax

**[no] vlan** *vlan-id*

To add a VLAN, run `vlan vlan-id`. To delete a VLAN, run `[no] vlan vlan-id`.

##### Parameters

Parameters	Description
<i>vlan-id</i>	<b>Defines the ID of the VLAN. Value range: 1-4094.</b>

##### Default Value

The default value is 1.

##### Command Mode

Global configuration mode

##### Usage Guidelines

After this command is run, the system enters the VLAN configuration mode and then you can modify some VLAN attributes.

##### Example

The following example shows how to add the VLAN whose ID is 2:

```
Switch_config#
```

```
Switch_config#vlan 2
```

```
Switch_config_vlan2#exit
```

### 18.1.2 name

#### Syntax

To name a VLAN, run name str.

**[no] name str**

#### Parameters

Parameters	Description
<i>str</i>	Defines the name of the VLAN. Value range: 1-32 characters.

#### Default Value

The default VLAN name is 'Default'. Other VLAN's name is VLANxxxx (xxxx is 4-digit stack ID)

#### Command Mode

VLAN configuration mode

#### Usage Guidelines

This command can be used to modify the VLAN name to symbolize a specific VLAN.

#### Example

The following example shows how to set the name of VLAN200 to main405: Switch\_config#

```
Switch_config#
```

```
Switch_config#vlan 200
```

```
Switch_config_vlan200#name ?
```

```
WORD The ascii name of VLAN(32bytes)
```

```
Switch_config_vlan200#name main405
```

### 18.1.3 dot1q-tunnel

#### Syntax

**dot1q-tunnel**

**no dot1q-tunnel**

To enable or disable the Dot1q tunnel globally, run the following commands.

#### Parameters

None

### Default Value

Dot1q Tunnel is not enabled globally.

### Command Mode

Global configuration mode

### Usage Guidelines

After Qot1Q Tunnel is globally enabled, all ports serve as the downlink ports of Qot1Q Tunnel by default and put the SPVLAN tag on the incoming packets.

### Example

The following example shows how to enable Dot1q tunnel in the global configuration mode.  
Switch\_config#dot1q-tunnel

#### 18.1.4 switchport pvid

### Syntax

To configure VLAN of the access-mode port, run `switchport pvid vlan-id`.

```
switchport pvid vlan-id
```

```
no switchport pvid
```

### Parameters

Parameters	Description
<i>vlan-id</i>	VLAN ID which the port belongs to, ranging between 1 and 4049 Value range: 1-4094

### Default Value

All ports belong to VLAN 1.

### Command Mode

Port configuration mode

### Usage Guidelines

If vlan which pvid belongs does not exist before the command, it will be created with the creation of pvid. The port can be configured in the access mode or the relay mode.

### Example

The following example shows how to set port GigaEthernet 0/1 to the access port of VLAN10: Switch\_config#interface g0/1

```
Switch_config_g0/1#switchport pvid 10
```

#### 18.1.5 switchport mode

### Syntax

```
switchport mode {access | trunk | dot1q-tunnel-uplink | dot1q-translating-tunnel
```

**no switchport mode**

To configure the mode of the port, run the following command.

## Parameters

Parameters	Description
<i>access</i>	<b>Access mode</b>
<i>trunk</i>	<b>Relay mode</b>
<i>dot1q-tunnel-uplink</i>	<b>VLAN tunnel uplink mode</b>
<i>dot1q-translating-tunnel</i>	<b>VLAN translating tunnel mode</b>

## Default Value

Access mode

## Command Mode

Port configuration mode

## Usage Guidelines

The switch's port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

The access mode indicates that the port belongs to just one VLAN; only the untagged Ethernet frame can be transmitted and received.

The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.

The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.

The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

The port mode collides with the 802.1X protocol. The 802.1X protocol cannot be configured in relay mode (including the VLAN translating tunnel mode and the VLAN tunnel uplink mode); the port on which the 802.1X protocol is configured cannot be set to the relay mode.

That is to say, the 802.1X protocol can be effective only on the access-mode port (including the VLAN tunnel mode).

The 802.1X standard does not support authentication on the trunk port. The reason is that the authentication object regulated in the standard is not the port. As to port multiplexing, if user authentication is approved in one VLAN, all other VLAN users who multiplex this port are also authorized correspondingly, therefore, the trunk port does not support authentication.

### Example

The following example shows how to configure the port to VLAN tunnel uplink port mode.  
Switch\_config\_g0/1#switchport mode dot1q-tunnel-uplink

### 18.1.6 switchport trunk

#### Syntax

To configure the attributes of the relay port, run the following command.

**[no] switchport trunk** {{**vlan-allowed** *vlan-list*} | {**vlan-untagged** *vlan-list*}}

#### Parameters

Parameters	Description
<i>vlan-allowed</i>	<b>VLAN ID which can be received and transmitted by the port Value Range: 1-4094</b>
<i>vlan-untagged</i>	<b>Frame that will be transmitted without adding the VLAN tag Value Range: 1-4094</b>

#### Default Value

The native VLAN ID of all relay ports is 1. The allowable value for all VLANs ranges between 1 and 4094.

#### Command Mode

Port configuration mode

#### Usage Guidelines

No matter the port is in access mode or in relay mode, you can run this command on the port. However, the port is in relay mode when this command functions.

The *vlan-allowed* parameter is used to control the VLAN range of the port; the *vlan-untagged* parameter is used to decide which packets need be added with the VLAN tag when a port transmits these packets.

When the *vlan list* is used, you can add, remove or set (none, all, except) the lists of the existing VLAN. The entered lists are separated by the comma or the hyphen. For example, "1, 3, 5, 7" stands for "vlan 1, vlan 3, vlan 5, vlan 7", while "1, 3-5, 7" stands for "vlan 1, vlan 3, vlan 4, vlan -5, vlan 7".

#### Example



The following example shows how to set the allowable VLAN range to 1-10, and the untagged VLAN range to 2-1000.

```
Switch_config_g0/1#switchport trunk vlan-allowed 1-10
```

```
Switch_config_g0/1#switchport trunk vlan-untagged 2-1000
```

### 18.1.7 show vlan

#### Syntax

To display relative information about all VLANs, run the following command.

```
show vlan [ id vlan-id | interface intf-id | dot1q-tunnel [interface intf] | mac-vlan | subnet  
| protocol-vlan | dot1q-translating-tunnel | flat-translation-table ]
```

#### Parameters

Parameters	Description
<i>id vlan-id</i>	<b>Displays the designated VLAN. Value range: 1-4094</b>
<i>Interface Intf-id</i>	<b>Displays the designated port.</b>
<i>dot1q-tunnel [interface intf]</i>	<b>Displays the global information and statistics information about Dot1Q tunnel, or displays the detailed information about Dot1Q tunnel of the designated port.</b>
<i>mac-vlan</i>	<b>Displays the configured MAC VLAN entries.</b>
<i>subnet</i>	<b>Displays the configured IP-subnet VLAN entries.</b>
<i>protocol-vlan</i>	<b>Displays the configured protocol VLAN template or entry.</b>
<i>dot1q-translating-tunnel</i>	<b>Displays the port vlan tunnel translation information</b>
<i>flat-translation-table</i>	<b>Checks the configured items of flat translation</b>

#### Default Value

None

#### Command Mode

Global configuration mode, port configuration and EXEC configuration mode

#### Usage Guidelines

None

#### Example

The following example shows how to display relative information about all VLANs.  
Switch#show vlan

```
-----
```

VLAN	Status	Name	Ports
1	Static	Default	g0/1, g0/2, g0/4.....

2	Static	VLAN0002	g0/3
3	Static	VLAN0003	g0/3
4	Static	VLAN0004	g0/3
5	Static	VLAN0005	g0/3

The status parameter stands for the VLAN generation source; the static parameter means that VLAN is generated through configuration; the dynamic parameter means that VLAN is generated dynamically through the GVRP protocol.

The following example shows the detailed information about a VLAN: Switch#show vlan id 1

VLAN id: 1, Name: default, TotalPorts:11

Ports            Attributes

-----

g0/1            Trunk, Untagged

g0/2            Access

The following example shows relative information about a VLAN on a port:

Switch#show vlan int g0/6

Interface        VLAN

Name            Property PVID Vlan-Map    uTagg-VLan-Map

-----

GigaEthernet0/2    Trunk 1        3,5,7,9,11,13,15 none

17,19

Switch#show vlan int g0/7

Interface        VLAN

Name            Property PVID Vlan-Map        uTagg-VLan-Map

GigaEthernet 0/3    Access 7        7                ----

### 18.1.8 show interface vlan

#### Syntax

To display relative information about the VLAN interface, run the following command.

**show interface vlan *intf-id***

#### Parameters

Parameters	Notes:	Value Range
<i>Intf-id</i>	Displays the designated port.	1-4094

**Default Value**

None

**Command Mode**

Global configuration mode, port configuration and EXEC configuration mode

**Usage Guidelines**

None

**Example**

The following example shows how to display the information about interface VLAN 1.

```
Switch#show int vlan 1
```

```
VLAN1 is up, line protocol is up
```

```
Hardware is EtherSVI, Address is 00e0.0f42.0071(00e0.0f42.0071) MTU 1500 bytes, BW  
1000000 kbit, DLY 2000 usec
```

```
Encapsulation ARPA, loopback not set
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 multicasts
```

```
0 input errors, 0 input discards
```

```
0 packets output, 0 bytes, 0 underruns
```

```
Transmitted 0 broadcasts, 0 multicasts
```

```
0 output errors, , 0 discards
```

```
ARP type: ARPA, ARP timeout 04:00:00
```

The statistics values are explained as follows:

Packets input means the input of all packets, including broadcast packets, multicast packets and unicast packets.

Bytes means the byte volume of all packets.

Broadcasts means received broadcast packets.

Broadcasts means received broadcast packets.

Input errors means received error packets.

Input discards means that the received packets are dropped, such as the received packets when the interface protocol is down.

Packets output means the output of all packets, including broadcast packets, multicast packets and unicast packets.

Bytes means the byte volume of all transmitted packets.

Broadcasts means transmitted broadcast packets.

---

Multicasts means transmitted multicast packets.

Output errors means transmitting error packets.

Output discards means that the transmitted packets are dropped, such as the transmitted packets when the interface protocol is down.

## Chapter 19 Voice VLAN Configuration Commands

### 19.1 *lldp*

#### Syntax

To enable or disable LLDP, run `lldp run`. To resume the default value, run `no lldp run`.

#### `lldp run`

#### `no lldp run`

#### Parameters

None

#### Default Value

The global LLDP is shut down, while LLDP on ports is enabled.

#### Usage Guidelines

### 19.2 *voice-vlan mac-address*

#### Syntax

To attach the MAC-address of IP phones to voice-vlan, need to execute the following command:

```
voice-vlan mac-address <IP-phone MAC-address> mask <MAC-mask>
```

#### Example

The following example shows how to attach the MAC-address of IP-phone to voice-vlan.

```
Switch_config#voice-vlan mac-address 5894.8100.01e5 mask ffff.0000.0000
```

```
Switch_config#
```

The values in MAC-mask `ffff.0000.0000` mean that **ONLY** the first octet of MAC-address matches.

### 19.3 *Interface configuration*

#### Syntax

In the following topology example VLAN 11 - voice vlan, VLAN 10 - is data vlan:



### Port configuration Example

```
PXT-SW(config)#interface GigaEthernet0/1
PXT-SW(config-if)#description PC-phone-port
PXT-SW(config-if)#switchport trunk vlan-allowed 10,11
PXT-SW(config-if)#switchport trunk vlan-untagged 10,11
PXT-SW(config-if)#switchport mode trunk
PXT-SW(config-if)#switchport pvid 10
PXT-SW(config-if)#switchport voice-vlan mode mac-address
PXT-SW(config-if)#switchport voice-vlan 11 dscp 46
```

Voice-vlan Mode MAC-address - is Mandatory.

## Chapter 20 GVRP Configuration Commands

### 20.1 GVRP Configuration Commands

#### 20.1.1 gvrp

##### Syntax

To enable or disable GVRP, run `gvrp`. To resume the default value, run `no gvrp`.

**gvrp**

**no gvrp**

##### Parameters

None

##### Default Value

The global GVRP is shut down, while GVRP on ports is enabled.

##### Usage Guidelines

GVRP can be enabled globally or on a port. Hence, GVRP can be really enabled only after GVRP is enabled both globally and on ports.

##### Example

The following example shows how to enable GVRP globally.

```
Switch_config#gvrp
```

```
Switch_config#
```

The following example shows how to enable GVRP on port 1.

```
Switch_config_g0/1#gvrp
```

```
Switch_config_g0/1#
```

### 20.1.2 gvrp dynamic-vlan-pruning

#### Syntax

To set the dynamic vlan to be effective on a registered port, run `gvrp dynamic-vlan-pruning`; to return to the default setting, use the “no” form of this command.

**gvrp dynamic-vlan-pruning**

**no gvrp dynamic-vlan-pruning**

#### Parameters

None

#### Default Value

dynamic-vlan-pruning is disabled by default, that is, dynamic VLAN can take effect on all ports.

#### Command Mode

Global configuration mode

#### Usage Guidelines

After this command is enabled and if a port has not registered a dynamic VLAN, this port will not belong to the dynamic VLAN even though this port is a trunk port and it allows the dynamic VLAN to pass through.

#### Example

The following example shows how to make dynamic VLAN validate on its registered port.

```
Switch_config#gvrp dynamic-vlan-pruning
```

```
Switch_config#
```

### 20.1.3 show gvrp statistics

#### Syntax

To display the GVRP statistics information, run this command.

**show gvrp statistics** [interface *intf-id*]

#### Parameters

Parameters	Description
<i>Intf-id</i>	Stands for a specific physical interface.

### Default Value

None

### Usage Guidelines

This command is used to display the GVRP statistics information.

### Example

The following example shows how to display the GVRP statistics information about interface g0/1.

```
Switch_config#show gvrp statistics interface g0/1 GVRP statistics on port g0/1
```

```
GVRP Status                : Enabled
GVRP Frames Received       : 0
GVRP Frames Transmitted    : 20
GVRP Frames Discarded     : 0
GVRP Last Pdu Origin      : 0000.0000.0000
```

#### *20.1.4 show gvrp status*

### Syntax

To display the GVRP state information, run this command.

```
show gvrp status
```

### Parameters

None

### Default Value

None

### Usage Guidelines

This command is used to display the GVRP state information.

### Example

The following example shows how to display the GVRP state information about a switch.

```
Switch_config#show gvrp status
```

```
GVRP is enabled
```

#### *20.1.5 debug gvrp event*

### Syntax

To enable the information output of GVRP debugging, run `debug gvrp event`. To shut down the information output of GVRP debugging, run `no debug GVRP event`.

```
debug gvrp event
```

**no debug gvrp event**

## Parameters

None

## Default Value

None

## Usage Guidelines

To enable the information output of GVRP debugging, run `debug gvrp event`. To shut down the information output of GVRP debugging, run `no debug GVRP event`.

## Example

```
Switch# debug gvrp event
```

```
Switch#
```

**20.1.6 debug gvrp packet**

## Syntax

To enable or disable GVRP displaying, run this command.

**debug gvrp packet****no debug gvrp packet**

## Parameters

None

## Default Value

None

## Usage Guidelines

To enable or disable GVRP displaying, run this command.

## Example

```
switch# debug gvrp packet
```

```
switch#
```

**20.2 GARPC onfiguration Commands**

GARP is the basic module of GVRP/CMRP. It schedules GVRP/GMRP running and provides services to GVRP/GMRP.

**20.2.1 garp timer leaveall**

## Syntax

To configure the `garp leaveall` timer, run `garp timer leaveall time_value`. To resume the corresponding default value, run `no garp timer leaveall`.



**garp timer leaveall** *time\_value*

**no garp timer leaveall**

#### Parameters

Parameters	Description
<i>timer_value</i>	Stands for the global leave all timer value. Value range: 10~ 32765 centiseconds.

#### Default Value

1000 centiseconds

#### Usage Guidelines

After the leave all timer times out, the bridge cancels all registered VLAN information and transmits Leave All Message to the outside.

#### Example

The following example configures leaveall timer on the switch to 1200 centiseconds.

```
Switch_config# garp timer leaveall 1200
```

```
Switch_config#
```

### 20.2.2 garp timer hold

#### Syntax

To configure the garp hold timer, run **garp timer hold time\_value**. To return to the default setting, run **no garp timer hold**.

**garp timer hold** *time\_value*

**no garp timer hold**

#### Parameters

Parameters	Description
<i>timer_value</i>	hold timer value of the port Value range: 10~ 32765 centiseconds.

#### Default Value

10 centiseconds

#### Command Mode

Port configuration mode

#### Usage Guidelines

None

## Example

The following example shows how to configure garp hold timer on the switch to 15 centiseconds.

```
Switch_config_g0/1#garp timer hold 15
```

```
Switch_config_g0/1#
```

### 20.2.3 garp timer join

#### Syntax

To configure the garp join timer, run `garp timer join time_value`. To return to the default setting, run `no garp timer join`.

**garp timer join** *time\_value*

**no garp timer join**

#### Parameters

Parameters	Description
<i>timer_value</i>	<b>join timer value of the port Value range: 10~ 32765 centiseconds.</b>

#### Default Value

20 centiseconds

#### Command Mode

Port configuration mode

#### Usage Guidelines

None

## Example

The following example shows how to configure garp join timer of the port g0/1 on the switch to 25 centiseconds.

```
Switch_config_g0/1#garp timer join 25
```

```
Switch_config_g0/1#
```

### 20.2.4 garp timer leave

#### Syntax

To configure the garp leave timer, run `garp timer leave time_value`. To return to the default setting, run `no garp timer leave`.

**garp timer leave** *time\_value*

**no garp timer leave**

#### Parameters

Parameters	Description
<i>timer_value</i>	leave timer value of the port Value range: 10~ 32765 centiseconds.

### Default Value

60 centiseconds

### Command Mode

Port configuration mode

### Usage Guidelines

None

### Example

The following example shows how to configure garp leave timer of the port g0/1 on the switch to 80 centiseconds.

```
Switch_config_g0/1#garp timer leave 80
```

```
Switch_config_g0/1#
```

## 20.2.5 show garp timers

### Syntax

To display theGARP-configured clock information, run the following command.

```
show garp timers [interface intf_id]
```

### Parameters

Parameters	Description
<i>Intf-id</i>	Stands for a specific physical interface.

### Default Value

None

### Usage Guidelines

This command is used to display theGARP-configured clock information, including the global leaveall timer value, the hold/join/leave timer value on the port.

### Example

The following example shows how to display the timer information on interface G0/1.

```
Switch# show garp timers interface g0/1
```

```
GARP timers on port 1(G0/1)
```

```
    Garp Join Time           : 20 centiseconds
```

Garp Leave Time : 60 centiseconds  
Garp LeaveAll Time : 1000 centiseconds  
Garp Hold Time : 10 centiseconds

### 20.2.6 *show garp status*

#### Syntax

To display the current GARP application instance by default, run the following command.

**show garp status**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

To display the current GARP application instance by default, run the following command.

#### Example

The following example shows the running GARP application instances.

```
Switch_config#show garp status
```

No GARP application is running.

### 20.2.7 *debug garp*

#### Syntax

To enable or disable the debug information about the GARP event or timer, run this command.

**debug garp {event | timer}**

**no debug garp {event | timer}**

#### Parameters

Parameters	Description
<i>event</i>	<b>event debug</b>
<i>timer</i>	<b>timer debug</b>

#### Default Value

None

#### Usage Guidelines

To enable or disable the debug information about the GARP event or timer, run this command.

### Example

The following example shows how to enable GARP event debug information.

```
Switch# debug garp event
```

```
Switch#
```

## Chapter 21 STP Configuration Commands

### 21.1 SSTP Configuration Commands

#### 21.1.1 *spanning-tree*

##### Syntax

To enable the default STP mode, run `spanning-tree`; to disable the STP, run `no spanning-tree`.

Enable or disable STP in interface configuration mode.

**spanning-tree**

**no spanning-tree**

##### Parameters

None

##### Default Value

RSTP is enabled by default.

##### Usage Guidelines

None

##### Command Mode

Global configuration mode

Physical interface configuration mode or aggregation port configuration mode

##### Example

None

#### 21.1.2 *spanning-tree mode sstp*

##### Syntax

To configure the spanning-tree operation mode, run `spanning-tree mode sstp` (**common STP mode IEEE 802.1D**). To return to the default setting, use the `no` form of this command.

**spanning-tree mode sstp**

**no spanning-tree mode****Parameters**

None

**Default Value**

The default STP mode is RSTP.

**Usage Guidelines**

None

**Command Mode**

Global configuration mode

**Example**

The following example shows how to enable the SSTP mode.

Switch\_config# spanning-tree mode sstp

Switch\_config#

**21.1.3 spanning-tree sstp priority****Syntax**

To configure the SSTP priority value, run `spanning-tree sstp priority value`. To resume the default value of the SSTP priority value, run `no spanning-tree sstp priority`.

**spanning-tree sstp priority *value*****no spanning-tree sstp priority****Parameters**

Parameters	Description
<i>value</i>	Priority value Value range: 0-61440

**Default Value**

32768

**Usage Guidelines**

When setting the priority value, you can make the switch as the root of the whole network spanning tree. The configuration value takes 4096 as a step and its value is the multiple of 4096. The configurable values are 0, 4096, 8192, 3\*4096, 4\*4096,..... and 15\*4096.

**Command Mode**

Global configuration mode

**Example**

The following example shows how to set the priority level of SSTP to 4096.

```
Switch_config# spanning-tree sstp priority 4096
```

```
Switch_config#
```

### 21.1.4 spanning-tree sstp hello-time

#### Syntax

To configure the transmission interval of SSTP packets, run `spanning-tree sstp hello-time time`. To resume the default transmission interval, run `no spanning-tree sstp hello-time`.

**spanning-tree sstp hello-time** *time*

**no spanning-tree sstp hello-time**

#### Parameters

Parameters	Description
<i>time</i>	Updates the interval. Range: 1-10 seconds

#### Default Value

2s

#### Usage Guidelines

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to configure the transmission interval of BPDUs of SSTP to 8 seconds.

```
Switch_config# spanning-tree sstp hello-time 8
```

```
Switch_config#
```

### 21.1.5 spanning-tree sstp max-age

#### Syntax

To configure the maximum lifespan of the SSTP BPDUs, run `spanning-tree sstp max-age time`. To resume the default interval time, run `no spanning-tree sstp max-age`.

**spanning-tree sstp max-age** *time*

**no spanning-tree sstp max-age**

#### Parameters

Parameters	Description
<i>seconds</i>	Means the maximum lifespan of BPDUs. Range: 6-40 seconds

**Default Value**

20s

**Usage Guidelines**

None

**Command Mode**

Global configuration mode

**Example**

The following example shows how to configure the maximum lifespan of SSTP to 24 seconds.

```
Switch_config# spanning-tree sstp max-age 24
```

```
Switch_config#
```

**21.1.6 spanning-tree sstp forward-time****Syntax**

To configure the forwarding delay, run `spanning-tree sstp forward-time time`. To resume the default forwarding delay, run `no spanning-tree sstp forward-time`.

**spanning-tree sstp forward-time** *time*

**no spanning-tree sstp forward-time**

**Parameters**

Parameters	Description
<i>time</i>	Time of the forwarding delay Value range: 4-30 seconds

**Default Value**

15 seconds

**Usage Guidelines**

None

**Command Mode**

Global configuration mode

**Example**

The following example shows how to configure the forwarding delay of SSTP to 20 seconds.

```
Switch_config# spanning-tree sstp forward-time 20
```

```
Switch_config#
```



### 21.1.7 *spanning-tree sstp cost*

#### Syntax

To configure the path cost of a port in SSTP mode, run `spanning-tree sstp cost value`. To resume the default path cost, run `no spanning-tree sstp cost`.

**`spanning-tree sstp cost value`**

**`no spanning-tree sstp cost`**

#### Parameters

Parameters	Description
<i>value</i>	<b>Value of the path cost Value range: 1-200000000</b>

#### Default Value

The value of the path cost of the 10M Ethernet is 100. The value of the path cost of the 100M Ethernet is 19. The value of the path cost of the 1000M Ethernet is 1.

#### Usage Guidelines

None

#### Command Mode

Port configuration mode

#### Example

The following example shows how to set the path cost of port G0/1 to 100 in SSTP mode.

```
Switch_config_g0/1#spanning-tree sstp cost 100
```

```
Switch_config_g0/1#
```

### 21.1.8 *spanning-tree cost*

#### Syntax

To configure the path cost of a port in all STP mode, run `spanning-tree cost value`. To resume the default path cost, run `no spanning-tree cost`.

**`spanning-tree cost value`**

**`no spanning-tree cost`**

#### Parameters

Parameters	Description
<i>value</i>	<b>Value of the path cost of a port Value range: 1-200000000</b>

#### Default Value

The default value depends on the rate of each port in all STP mode.

## Usage Guidelines

The results of this command validates in all STP modes. In VLAN-based STP mode, the path cost of a port will be updated in all VLAN spanning trees; In MSTP mode, the path cost of a port will be updated in all STP cases.

However, the results of this command cannot affect independent configurations in each mode. For example, After you run `spanning-tree sstp cost 100` and `spanning-tree cost 110`, the path cost of the port is still 100 in SSTP mode.

## Command Mode

Port configuration mode

## Example

The following example shows how to set the path cost of port g0/1 to 24:

```
Switch_config_g0/1# spanning-tree cost 24
```

```
Switch_config_g0/1#
```

### 21.1.9 *spanning-tree sstp port-priority*

## Syntax

To configure the priority value of a port in SSTP mode, run `spanning-tree sstp port-priority value`. To resume the default value of the priority value, run `no spanning-tree sstp port-priority`.

```
spanning-tree sstp port-priority value
```

```
no spanning-tree sstp port-priority
```

## Parameters

Parameters	Description
<i>value</i>	Means the priority level of a port. Value range: 0-240

## Default Value

128 (0x80)

## Usage Guidelines

The value of the priority level of a port must be the multiple of 16.

## Command Mode

Port configuration mode

## Example

The following example shows how to set the priority level of port g0/1 to 32:

```
Switch_config_g0/1# spanning-tree sstp port-priority 32
```

```
Switch_config_g0/1#
```

### 21.1.10 *spanning-tree port-priority*

#### Syntax

To configure the priority level of a port in all STP modes, run `spanning-tree port-priority value`. To resume the default priority level, run `spanning-tree port-priority`.

**spanning-tree port-priority** *value*

**no spanning-tree port-priority**

#### Parameters

Parameters	Description
<i>value</i>	Means the priority level of a port. Value range: 0-240 Step: 16

#### Default Value

The default value of the priority level of a port is 128 in all modes.

#### Usage Guidelines

The results of this command validates in all STP modes. In VLAN-based STP mode, the priority level of a port will be updated in all VLAN spanning trees; In MSTP mode, the priority level of a port will be updated in all STP cases.

However, the results of this command cannot affect independent configurations in each mode. For example, After you run `spanning-tree sstp port-priority 128` and `spanning-tree port-priority 48`, the port-priority of the port is still 128 in SSTP mode.

#### Command Mode

Port configuration mode

#### Example

The following example shows how to set the priority level of port `g0/1` to 16 in all STP modes.

```
Switch_config_g0/1#spanning-tree port-priority 16
```

```
Switch_config_g0/1#
```

### 21.1.11 *show spanning-tree*

#### Syntax

To display the spanning-tree information, run the following command.

**show spanning-tree** [**detail** | **interface** *intf-i*]

#### Parameters

Parameters	Description
<i>intf-i</i>	interface name, for instance, <b>G0/1</b>

**Default Value**

None

**Usage Guidelines**

This command is used to display the state of the spanning tree.

**Command Mode**

EXEC mode, Global configuration mode or interface mode

**Example**

```
Switch_config#show spanning-tree
```

```
Spanning tree enabled protocol SSTP
```

**SSTP**

```

Root ID                Priority          32768
                       Address          00E0.0FCC.F775
                       This bridge is the root
                       Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID              Priority          32768
                       Address          00E0.0FCC.F775
                       Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Interface              Role Sts Cost          Pri.Nbr Type
-----
G0/1                   Desg FWD 19          128.16 P2p

```

```
Switch_config#
```

**21.1.12 spanning-tree management trap****Syntax**

To enable STP Trap, run this command. To return to the default setting, use the no form of this command.

**[no] spanning-tree management trap [newroot | topologychange]**

**Parameters**

Parameters	Description
<i>newroot</i>	<b>Stands for the newRoot trap type.</b>
<i>topologychange</i>	<b>Stands for the topologyChange trap type.</b>

**Default Value**

STP Trap is disabled.

### Usage Guidelines

None

### Command Mode

Global configuration mode

### Example

None

## 21.2 VLAN STP Configuration Commands

### 21.2.1 *spanning-tree mode pvst*

#### Syntax

To enable VLAN-based STP mode, run `spanning-tree mode pvst`. To disable all STP modes, run `no spanning-tree mode`.

**spanning-tree mode pvst**

**no spanning-tree mode**

#### Parameters

None

#### Default Value

The default STP mode is RSTP.

### Usage Guidelines

None

### Example

The following example shows how to enable PVST on the switch.

```
Switch_config# spanning-tree mode pvst
```

```
Switch_config#
```

### 21.2.2 *spanning-tree vlan*

#### Syntax

To designate VLAN to distribute the STP case, run `spanning-tree vlan vlan-list`. To cancel the spanning tree of the designated VLAN, run `no spanning-tree vlan vlan-list`.

**spanning-tree vlan *vlan-list***

**no spanning-tree vlan *vlan-list***

#### Parameters

Parameters	Description
------------	-------------

<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
------------------	---

### Default Value

The switch only distributes spanning tree instances for certain VLANs. By default the exceeding VLANs will be added to STP forbidding list automatically.

### Usage Guidelines

None

### Command Mode

Global configuration mode

### Example

The following example shows how to cancel the spanning tree of VLAN 10, 11, 15-19 and then how to distribute the spanning trees to VLAN 40-50.

```
Switch_config#no spanning-tree vlan 10,11,15-19
```

```
Switch_config#spanning-tree vlan 40-50
```

```
Switch_config#
```

### 21.2.3 spanning-tree vlan priority

#### Syntax

To designate the priority level of the bridge of the VLAN STP, run `spanning-tree vlan vlan-list priority value`.

**spanning-tree vlan *vlan-list* priority *value***

**no spanning-tree vlan *vlan-list* priority**

#### Parameters

Parameters	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Value of the priority level, ranging between 0 and 61400 (step: 4096)

### Default Value

By default, the priority level of the bridge of each VLAN spanning tree is 32768 plus the VLAN number.

### Usage Guidelines

None

### Command Mode

Global configuration mode

## Example

The following example shows how to set the priority levels of the bridges of VLAN1-3, 5-10 to 4096.

```
Switch_config#spanning-tree vlan 1-3,5-10 priority 4096
```

```
Switch_config#
```

### 21.2.4 *spanning-tree vlan forward-time*

#### Syntax

To set the Forward Delay parameter of the spanning tree in the designated VLAN, run `spanning-tree vlan vlan-list forward-time value`.

**spanning-tree vlan *vlan-list* forward-time *value***

**no spanning-tree vlan *vlan-list* forward-time**

#### Parameters

Parameters	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Value of the forward-delay parameter Value range: 4-30 seconds Default value: 15 seconds

#### Default Value

The value of the forward-delay parameter of all VLANs is 15 seconds.

#### Usage Guidelines

None

#### Command Mode

Global configuration mode

## Example

The following example shows how to set the forward delay parameter of VLAN 1-3, 5-10 to 19 seconds.

```
Switch_config#spanning-tree vlan 1-3,5-10 forward-time 19
```

```
Switch_config#
```

### 21.2.5 *spanning-tree vlan max-age*

#### Syntax

To set the Max Age parameter of the spanning tree in the designated VLAN, run `spanning-tree vlan vlan-list max age value`. To resume the default value, run `no spanning-tree vlan vlan-list max age`.

**spanning-tree vlan *vlan-list* max-age *value***

**no spanning-tree vlan *vlan-list* max-age**

## Parameters

Parameters	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Value of the max-age parameter Value range: 6-40 seconds Default value: 20 seconds

## Default Value

The default value of the max-age parameter for all VLANs is 20 seconds.

## Usage Guidelines

None

## Command Mode

Global configuration mode

## Example

The following example shows how to set the max age parameter of VLAN 1-3, 5-10 to 19 seconds.

```
Switch_config#spanning-tree vlan 1-3,5-10 max-age 19
```

```
Switch_config#
```

**21.2.6 spanning-tree vlan hello-time**

## Syntax

To set the hello time parameter of the spanning tree in the designated VLAN, run `spanning-tree vlan vlan-list hello time value`. To resume the default value, run `no spanning-tree vlan vlan-list hello time`.

**spanning-tree vlan *vlan-list* hello-time *value***

**no spanning-tree vlan *vlan-list* hello-time**

## Parameters

Parameters	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Value of the hello time parameter Value range: 1-10 seconds Default value: 2 seconds

## Default Value

The default value of the Hello-Time parameter for all VLANs is 2 seconds.

## Usage Guidelines

None



## Command Mode

Global configuration mode

## Example

The following example shows how to set the Hello Time parameter of VLAN 1-3, 5-10 to 9 seconds.

```
Switch_config#spanning-tree vlan 1-3,5-10 hello-time 9
```

```
Switch_config#
```

### 21.2.7 *spanning-tree vlan cost*

## Syntax

To set the path cost of the spanning tree in the designated VLAN, run `spanning-tree vlan vlan-list cost value`. To resume the default value, run `no spanning-tree vlan vlan-list cost`.

**spanning-tree vlan *vlan-list* *cost* *value***

**no spanning-tree vlan *vlan-list* *cost***

## Parameters

Parameters	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Path cost of a port, which ranges between 1 and 200,000,000

## Default Value

The path cost of a port depends on the port rate.

The value of the path cost of the 10M Ethernet is 100.

The value of the path cost of the 100M Ethernet is 19.

The value of the path cost of the 1000M Ethernet is 1.

## Usage Guidelines

None

## Command Mode

Port configuration mode

## Example

The following example shows how to set the path cost of port G0/1 VLAN1-3,5-10 to 100.

```
Switch_config_g0/1#spanning-tree vlan 1-3,5-10 cost 100
```

```
Switch_config_g0/1#
```

### 21.2.8 *spanning-tree vlan port-priority*

#### Syntax

To set the priority level of the spanning tree in the designated VLAN, run `spanning-tree vlan vlan-list port-priority value`. To resume the default value, run `no spanning-tree vlan vlan-list port-priority`.

**spanning-tree vlan *vlan-list* port-priority *value***

**no spanning-tree vlan *vlan-list* port-priority**

#### Parameters

Parameters	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Priority level of a port, which ranges between 0 and 240 and whose step is 16

#### Default Value

128

#### Usage Guidelines

None

#### Command Mode

Port configuration mode

#### Example

The following example shows how to set the priority level of port g0/1 VLAN1-3,5-10 to 32.

```
Switch_config_g0/1#spanning-tree vlan 1-3,5-10 port-priority 32
```

```
Switch_config_g0/1#
```

### 21.2.9 *show spanning-tree vlan*

#### Syntax

To check the state of the spanning tree in the designated VLAN, run the following command:

**show spanning-tree vlan *vlan-list* [detail]**

#### Parameters

Parameters	Description
<i>vlan-list</i>	List of the VLAN numbers, such as 1,2,3-10,15
<i>value</i>	Displays the detailed information about the state of the spanning tree.

#### Default Value

None

### Usage Guidelines

None

### Command Mode

EXEC mode, Global configuration mode or interface mode

### Example

The following example shows how to check the spanning tree of VLAN 1-2.

```
Switch_config#show spanning-tree vlan 1-2
```

```
Spanning tree enabled protocol PVST
```

```
VLAN0001
```

```
Root ID                Priority          32769
                        Address          00E0.0FCC.F775
                        This bridge is the root
                        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID              Priority          32769
                        Address          00E0.0FCC.F775
                        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface              Role Sts Cost          Pri.Nbr Type
-----
```

```
G0/1                   Desg FWD 19          128.1 P2p
```

```
VLAN0002
```

```
Root ID                Priority          32770
                        Address          00E0.0FCC.F775
                        This bridge is the root
                        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID              Priority          32770
                        Address          00E0.0FCC.F775
                        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface              Role Sts Cost          Pri.Nbr Type
```

```
G0/1                   Desg FWD 19          128.1 P2p
```

Switch\_config#

### *21.2.10 show spanning-tree pvst instance-list*

#### Syntax

To check the corresponding relation between PVST instances and VLAN, run this command.

**show spanning-tree pvst instance-list**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Command Mode

EXEC mode, Global configuration mode or interface mode

#### Example

None

## Chapter 22 RSTP Configuration Commands

### *22.1 RSTP Configuration Commands*

#### *22.1.1 spanning-tree mode rstp*

#### Syntax

To enable the RSTP function, run `spanning-tree mode rstp`. To disable the STP, run `no spanning-tree mode`.

**spanning-tree mode rstp**

**no spanning-tree mode**

#### Parameters

None

#### Default Value

RSTP is enabled.

#### Usage Guidelines

None

#### Example

The following example shows how to enable RSTP on the switch.

```
Switch_config# spanning-tree mode rstp
```

```
Switch_config#
```

### 22.1.2 *spanning-tree rstp forward-time*

#### Syntax

To configure the forwarding delay of RSTP, run `spanning-tree rstp forward-time time`. To resume the default forwarding delay of RSTP, run `no spanning-tree rstp forward-time`.

**spanning-tree rstp forward-time *time***

**no spanning-tree rstp forward-time**

#### Parameters

Parameters	Description
<i>time</i>	Time of the forwarding delay Value Range:4-30s.

#### Default Value

15 seconds

#### Usage Guidelines

None

#### Example

The following example shows how to set the forwarding delay of RSTP to 20 seconds.

```
Switch_config# spanning-tree rstp forward-time 20
```

```
Switch_config#
```

### 22.1.3 *spanning-tree rstp hello-time*

#### Syntax

To configure the update interval of RSTP, run `spanning-tree rstp hello-time time`. To resume the default update interval of RSTP, run `no spanning-tree rstp hello-time`.

**spanning-tree rstp hello-time *time***

**no spanning-tree rstp hello-time**

#### Parameters

Parameters	Description
<i>time</i>	Updates the interval. Range: 1-10 seconds

#### Default Value

2 seconds

## Usage Guidelines

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch.

## Example

The following example shows how to set the update interval of RSTP to 8 seconds.

```
Switch_config# spanning-tree rstp hello-time 8
```

```
Switch_config#
```

### 22.1.4 *spanning-tree rstp max-age*

#### Syntax

To configure the maximum lifespan of the SSTP BPDU, run `spanning-tree sstp max-age time`. To resume the default interval time, run `no spanning-tree sstp max-age`.

**spanning-tree rstp max-age *time***

**no spanning-tree rstp max-age**

#### Parameters

Parameters	Description
<i>time</i>	<b>Maximum interval of the lifespan Range: 6-40 seconds</b>

#### Default Value

20 seconds

#### Usage Guidelines

None

## Example

The following example shows how to set the maximum lifespan of RSTP to 24 seconds.

```
Switch_config# spanning-tree rstp max-age 24
```

```
Switch_config#
```

### 22.1.5 *spanning-tree rstp priority*

#### Syntax

To configure the RSTP priority value, run `spanning-tree rstp priority value`. To resume the default value of the RSTP priority value, run `no spanning-tree rstp priority`.

**spanning-tree rstp priority *value***

**no spanning-tree rstp priority**

#### Parameters

Parameters	Description
<i>value</i>	Priority level of the bridge Value range: 0-61440 Step: 4096

#### Default Value

32768

#### Usage Guidelines

None

#### Example

The following example shows how to set the bridge priority of RSTP to 4096.

```
Switch_config# spanning-tree rstp priority 4096
```

```
Switch_config#
```

### 22.1.6 *spanning-tree rstp cost*

#### Syntax

To configure the path cost of a port, run `spanning-tree rstp cost value`. To resume the default value, run `no spanning-tree rstp cost`.

**`spanning-tree rstp cost value`**

**`no spanning-tree rstp cost`**

#### Parameters

Parameters	Description
<i>value</i>	Value of the path cost Value range: 1-200000000

#### Default Value

The path cost depends on the connection rate of the port.

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

#### Usage Guidelines

None

#### Example

The following example shows how to set the path cost of port g0/1 to 24:

```
Switch_config_g0/1# spanning-tree rstp cost 24
```

```
Switch_config_g0/1#
```

### 22.1.7 *spanning-tree rstp port-priority*

#### Syntax

To configure the priority level of a port, run `spanning-tree rstp port-priority value`. To resume the default value, run `no spanning-tree rstp port-priority`.

**`spanning-tree rstp port-priority value`**

**`no spanning-tree rstp port-priority`**

#### Parameters

Parameters	Description
<i>value</i>	Priority level of a port Value range: 0-240 Step: 16

#### Default Value

128

#### Usage Guidelines

None

#### Example

The following example shows how to set the priority level of port g0/1 to 16:

```
Switch_config_g0/1# spanning-tree rstp port-priority 16
```

```
Switch_config_g0/1#
```

### 22.1.8 *spanning-tree rstp edge*

#### Syntax

To set the port to the edge port. To return to the default setting, use the `no` form of this command.

**`spanning-tree rstp edge`**

**`no spanning-tree rstp edge`**

#### Parameters

None

#### Default Value

Auto-detection

#### Usage Guidelines

None

#### Command Mode

Port configuration mode



## Example

None

### 22.1.9 *spanning-tree rstp point-to-point*

#### Syntax

To set the point-to-point connection of a port to force-true, force-false or auto, run this command.

```
spanning-tree rstp point-to-point [force-true | force-false | auto]
```

#### Parameters

Parameters	Description
<i>force-true</i>	<b>Sets the point-to-point connection to be forcedly effective.</b>
<i>force-false</i>	<b>Sets the point-to-point connection to be forcedly ineffective.</b>
<i>auto</i>	<b>Sets the point-to-point connection to be automatic check (default).</b>

#### Default Value

Auto-detection

#### Usage Guidelines

None

#### Command Mode

Port configuration mode

## Example

None

### 22.1.10 *spanning-tree rstp migration-check*

#### Syntax

To restart checking protocol transfer of RSTP, run the following command.

```
spanning-tree rstp migration-check
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to restart the protocol transfer check on a port and to change the port in STP-compatible mode to the RSTP mode, enabling RSTP BPDU to be transmitted.

## Command Mode

Global or port configuration mode

## Example

The following example shows how to check protocol transfer on port G0/1.

```
Switch_config_g0/1#spanning-tree rstp migration-check
```

```
Switch_config_g0/1#
```

# Chapter 23 MSTP Configuration Commands

## 23.1 MSTP Configuration Commands

### 23.1.1 *spanning-tree mode mstp*

#### Syntax

To set the operation mode of the spanning tree to MSTP, run `spanning-tree mode mstp`. To return to the default set, run `no spanning-tree mode`.

**spanning-tree mode mstp**

**no spanning-tree mode**

#### Parameters

None

#### Default Value

MSTP is disabled, while SSTP is enabled.

#### Usage Guidelines

None

## Example

The following example shows how to enable MSTP on a switch.

```
Switch_config# spanning-tree mode mstp
```

```
Switch_config#
```

### 23.1.2 *spanning-tree mstp name*

#### Syntax

To configure the MSTP name, run `spanning-tree mstp name string`. To resume the default name, run `no spanning-tree mstp name`.

**spanning-tree mstp name *string***

**no spanning-tree mstp name**

#### Parameters

Parameters	Description
<i>string</i>	A character string to configure the name, which contains up to 32 characters and is capital sensitive. The default value is the character string of the MAC address.

### Default Value

Its default value is the MAC address of a switch.

### Usage Guidelines

None

### Example

The following example shows how to set the name of MSTP for a switch to reg-01.

```
Switch_config# spanning-tree mstp name reg-01
```

```
Switch_config#
```

### 23.1.3 spanning-tree mstp revision

#### Syntax

To configure the MSTP revision number, run `spanning-tree mstp revision value`. To resume the default revision number, run `no spanning-tree mstp revision`.

**spanning-tree mstp revision *value***

**no spanning-tree mstp revision**

#### Parameters

Parameters	Description
<i>value</i>	Revision number, which ranges between 0 and 65535 and whose default value is 0

### Default Value

The default value of the revision number is 0.

### Usage Guidelines

None

### Example

The following example shows how to set the revision number of MSTP to 100.

```
Switch_config# spanning-tree mstp revision 100
```

```
Switch_config#
```

### 23.1.4 spanning-tree mstp instance

#### Syntax

To map VLAN to MSTI, run `spanning-tree mstp instance instance-id vlan vlan-list`. To remap VLAN to CIST, run `no spanning-tree mstp instance instance-id`.

**spanning-tree mstp instance** *instance-id* **vlan** *vlan-list*

**no spanning-tree mstp instance** *instance-id*

#### Parameters

Parameters	Description
<i>instance-id</i>	<b>Instance ID of the spanning-tree, which stands for an MSTI Value range: 1-15</b>
<i>vlan-list</i>	<b>A VLAN list which is mapped to a spanning tree It ranges from 1 to 4094.</b>

#### Default Value

All VLANs are mapped to CIST (MST00).

#### Usage Guidelines

Instance ID is an independent value which stands for an STP instance.

The `vlan-list` parameter can stand for a VLAN group, such as VLANs 1,2 and3, VLANs 1-5 or VLANs 1,2,5-10.

#### Example

The following example shows how to map VLAN2 to STP instance 1, and VLANs 5, 7, 10-20 to STP instance 2 and then remap these VLANs to MST00.

```
Switch_config# spanning-tree mstp instance 1 vlan 2
```

```
Switch_config# spanning-tree mstp instance 2 vlan 5,7,10-20
```

```
Switch_config# no spanning-tree mstp instance 1
```

```
Switch_config# no spanning-tree mstp instance 2
```

### 23.1.5 *spanning-tree mstp root*

#### Syntax

To set a designated STP instance to a primary or secondary root, run `spanning-tree mstp instance-id root {primary | secondary}`. To resume the default value of the bridge priority of an STP instance, run `no spanning-tree mstp root`.

**spanning-tree mstp** *instance-id* **root** {**primary** | **secondary**}

[**diameter** *net-diameter* [**hello-time** *seconds*]]

**no spanning-tree mstp** *instance-id* **root**

The `diameter` command and the `hello-time` command are allowed to modify the network diameter and the `hello-time` parameter.

#### Parameters

Parameters	Description
<i>instance-id</i>	Number of the STP instance, which ranges between 0 and 15
<i>primary</i>	Sets an STP instance to a primary root.
<i>secondary</i>	Sets an STP instance to a secondary root.
<i>net-diameter</i>	An optional parameter which presents the network diameter. When instance-id is 0, net-diameter ranges between 2 and 7.
<i>seconds</i>	An optional parameter standing for the value of the Hello Time parameter, which ranges between 1 and 10 seconds

### Default Value

The default value of the bridge priority for all STP instances is 32768. The network diameter is 7, while Hello Time is 2 seconds.

### Usage Guidelines

The diameter command and the hello-time command validate only when the instance-id parameter is 0.

In general, after the command to set the primary root is executed, the protocol automatically check the bridge ID of the current network's root and then sets the priority of the bridge ID to 24576, which guarantees that the current switch serves as the root of the STP instance. If the priority value of the network root is less than 24576, the protocol will automatically set the STP priority of the current bridge to a value which is 4096 smaller than the priority of the root. It deserves attention that 4096 is the step of the priority value of the bridge.

Different from primary root configuration, after the command to set the secondary root is executed, the protocol directly set the STP priority of the switch to 28672. In case that the priority value of other switches in the network is 32768 by default, the current switch serves as the secondary root.

### Example

The following example shows how to set a switch to the primary root in CIST, and how to recalculate the time parameter of STP through diameter 3 and hello-time 3, and then set the switch to the secondary root in MST01.

```
Switch_config# spanning-tree mstp 0 root primary diameter 3 hello-time 3
```

```
Switch_config# spanning-tree mstp 1 root secondary
```

#### 23.1.6 *spanning-tree mstp priority*

##### Syntax

To configure the value of the bridge priority of a designated STP instance, run `spanning-tree mstp instance-id priority value`. To resume the default value of the bridge priority, run `spanning-tree mstp priority`.

```
spanning-tree mstp instance-id priority value
```

**no spanning-tree mstp *instance-id* priority**

## Parameters

Parameters	Description
<i>instance-id</i>	Number of the STP instance, which ranges between 0 and 15
<i>value</i>	Value of the bridge priority, which can be one of the following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440,

## Default Value

The default value of the bridge priority for all STP instances is 32768.

## Usage Guidelines

The priority values in each STP instance are independent and can be configured independently.

## Example

The following example shows how to set the priority values of a switch in CIST and MST01 to 4096 and 8192 respectively.

```
Switch_config# spanning-tree mstp 0 priority 4096
```

```
Switch_config# spanning-tree mstp 1 priority 8192
```

**23.1.7 spanning-tree mstp hello-time**

## Syntax

To configure the Hello Time of MSTP, run `spanning-tree mstp hello-time seconds`. To resume the default value of the Hello Time of MSTP, run `no spanning-tree mstp hello-time`.

**spanning-tree mstp hello-time *seconds***

**no spanning-tree mstp hello-time**

## Parameters

Parameters	Description
<i>seconds</i>	Value range: 1-10 seconds Default value: 2 seconds

## Default Value

2 seconds

## Usage Guidelines

None

## Example

The following example shows how to set the Hello Time parameter of MSTP to 10.

```
Switch_config# spanning-tree mstp hello-time 10
```

```
Switch_config# no spanning-tree mstp hello-time
```

### 23.1.8 *spanning-tree mstp forward-time*

#### Syntax

To configure the forward delay parameter of MSTP, run `spanning-tree mstp forward-time seconds`. To resume the default value of the forward delay parameter of MSTP, run `no spanning-tree mstp forward-time`.

**spanning-tree mstp forward-time** *seconds*

**no spanning-tree mstp forward-time**

#### Parameters

Parameters	Description
<i>seconds</i>	<b>Value range: 4-30 seconds Default value: 15 seconds</b>

#### Default Value

15 seconds

#### Usage Guidelines

None

## Example

The following example shows how to set the Forward Delay parameter of MSTP to 10.

```
Switch_config# spanning-tree mstp forward-time 10
```

```
Switch_config# no spanning-tree mstp forward-time
```

### 23.1.9 *spanning-tree mstp max-age*

#### Syntax

To configure the max age parameter of MSTP, run `spanning-tree mstp max-age seconds`. To resume the default value of the forward delay parameter of MSTP, run `no spanning-tree mstp max-age`.

**spanning-tree mstp max-age** *seconds*

**no spanning-tree mstp max-age**

#### Parameters

Parameters	Description
<i>seconds</i>	<b>Value range: 6-40 seconds Default value: 20 seconds</b>

### Default Value

20 seconds

### Usage Guidelines

None

### Example

The following example shows how to set the max age parameter of MSTP to 10.

```
Switch_config# spanning-tree mstp max-age 10
```

```
Switch_config# no spanning-tree mstp max-age
```

### 23.1.10 spanning-tree mstp diameter

#### Syntax

To configure the network diameter of MSTP, run `spanning-tree mstp diameter net-diameter`. To resume the default value of the network diameter, run `no spanning-tree mstp diameter`.

**spanning-tree mstp diameter** *net-diameter*

**no spanning-tree mstp diameter**

#### Parameters

Parameters	Description
<i>net-diameter</i>	<b>Value range: 2-7 Default value: 7</b>

### Default Value

The default value of the network diameter is 7.

### Usage Guidelines

The `net-diameter` parameter is not saved as an independent configuration in the switch. Only the time parameter which is modified through network diameter configuration can be saved. The `net-diameter` parameter is effective only to CIST. After configuration, the three time parameters of STP are automatically updated to a prior value.

It is recommended to modify the time parameter of STP through setting the root or network diameter, ensuring the rationality of the time parameter.

### Example

The following example shows how to set the network diameter of MSTP to 5 and then resume its default value.

```
Switch_config# spanning-tree mstp diameter 5
```

```
Switch_config# no spanning-tree mstp diameter
```



### 23.1.11 *spanning-tree mstp max-hops*

#### Syntax

To set the maximum hops of MSTP BPDU, run `spanning-tree mstp max-hops hop-count`. To resume the default settings, run `no spanning-tree mstp max-hops`.

**`spanning-tree mstp max-hops hop-count`**

**`no spanning-tree mstp max-hops`**

#### Parameters

Parameters	Description
<i>hop-count</i>	<b>Value range: 6-40 Default value: 20</b>

#### Default Value

The default value of the maximum hops is 20.

#### Usage Guidelines

None

#### Example

The following example shows how to set the maximum hops of MSTP BPDU to 5 and then resume the default value.

```
Switch_config# spanning-tree mstp max-hops 5
```

```
Switch_config# no spanning-tree mstp max-hops
```

### 23.1.12 *spanning-tree mstp port-priority*

#### Syntax

To configure the port priority in the designated spanning-tree instance, run `spanning-tree mstp instance-id port-priority value`. To resume the port priority to the default settings, run `no spanning-tree mstp instance-id port-priority`.

**`spanning-tree mstp instance-id port-priority value`**

**`no spanning-tree instance-id port-priority`**

#### Parameters

Parameters	Description
<i>instance-id</i>	<b>Number of the STP instance, which ranges between 0 and 15</b>
<i>value</i>	<b>Value of the port priority, which can be one of the following values 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240,</b>

### Default Value

The port priority in all STP instances is 128 by default.

### Usage Guidelines

None

### Example

The following example shows how to set the priority value of port G0/1 in CIST to 16 and then resume the default value.

```
Switch_config_g0/1# spanning-tree mstp 0 port-priority 16
```

```
Switch_config_g0/1# no spanning-tree mstp 0 port-priority
```

### 23.1.13 *spanning-tree mstp cost*

#### Syntax

To set the path cost of the spanning tree in the designated STP instance, run `spanning-tree mstp instance-id cost value`. To resume the default value, run `no spanning-tree mstp instance-id cost`.

**`spanning-tree mstp instance-id cost value`**

**`no spanning-tree mstp instance-id cost`**

#### Parameters

Parameters	Description
<i>instance-id</i>	Number of the STP instance, which ranges between 0 and 15
<i>value</i>	Path cost of a port, which ranges between 1 and 200,000,000

### Default Value

The path cost depends on the connection rate of the port.

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

### Usage Guidelines

None

### Example

The following example shows how to set the path cost of port G0/1 to 200 in CIST.

```
Switch_config_g0/1# spanning-tree mstp 0 cost 200
```

```
Switch_config_g0/1#
```

### 23.1.14 *spanning-tree mstp edge*

#### Syntax

To set the port to the edge port. To return to the default setting, use the no form of this command.

**spanning-tree mstp edge**

**no spanning-tree mstp edge**

#### Parameters

None

#### Default Value

Automatically checks the edge port.

#### Usage Guidelines

None

#### Example

None

### 23.1.15 *spanning-tree mstp point-to-point*

#### Syntax

To configure the connection type of a port, run `spanning-tree mstp point-to-point {force-true | force-false | auto}`. To resume the connection type to auto-check, run `no spanning-tree mstp point-to-point`.

**spanning-tree mstp point-to-point {force-true | force-false | auto}**

**no spanning-tree mstp point-to-point**

#### Parameters

Parameters	Description
<i>force-true</i>	<b>Sets the port connection mode to point-to-point.</b>
<i>force-false</i>	<b>Sets the port connection mode to sharing.</b>
<i>auto</i>	<b>Sets the port connection mode to auto-check (the default mode).</b>

#### Default Value

MSTP will automatically check the port connection mode by default.

#### Usage Guidelines

None

## Example

The following example shows how to set the connection mode of port G0/1 to sharing.

```
Switch_config_g0/1# spanning-tree mstp point-to-point force-false
```

```
Switch_config_g0/1#
```

### 23.1.16 *spanning-tree mstp mst-compatible*

#### Syntax

To enable or disable multiple spanning tree compatible mode, run this command in global configuration mode.

**spanning-tree mstp mst-compatible**

**no spanning-tree mstp mst-compatible**

To enable or disable multiple spanning tree compatible mode, run this command in interface configuration mode.

**spanning-tree mstp mst-compatible {enable | disable}**

**no spanning-tree mstp mst-compatible**

#### Parameters

Parameters	Description
<i>enable</i>	<b>The mst-compatible mode is enabled.</b>
<i>disable</i>	<b>The mst-compatible mode is disabled.</b>

#### Default Value

The compatible mode is not activated by default and the switch cannot establish an area with other switches which transmit BPDU in compatible mode.

#### Usage Guidelines

After the compatible mode is enabled, you are recommended to set a connected switch which runs other MSTP to the root of CIST, securing that the switch can enter the compatible mode through receiving packets.

## Example

The following example shows how to activate the MST-compatible mode of a switch in global configuration mode.

```
Switch_config#spanning-tree mstp mst-compatible
```

### 23.1.17 *spanning-tree mstp migration-check*

#### Syntax

To remove the STP information which is checked on a port and then restart the protocol transform process, run the following command.

**spanning-tree mstp migration-check****Parameters**

None

**Default Value**

None

**Usage Guidelines**

This command validates both in global configuration mode and in port configuration mode.

**Example**

The following example shows how to conduct the protocol transfer check on all ports and then conduct the second protocol transfer check on port G0/1.

```
Switch_config# spanning-tree mstp migration-check Switch_config# interface g0/1
```

```
Switch_config_g0/1# spanning-tree mstp migration-check
```

**23.1.18 spanning-tree mstp restricted-role****Syntax**

To enable role restriction of the port, run the following command. To return to the default setting, use the no form of this command.

**[no] spanning-tree mstp restricted-role****Parameters**

None

**Default Value**

The role restriction of the port is disabled by default.

**Command Mode**

Port configuration mode

**Usage Guidelines**

The port will not be selected as the root port if the role restriction of the port is enabled.

**Example**

None

**23.1.19 spanning-tree mstp restricted-tcn****Syntax**

To enable TCN restriction of the port, run the following command. To return to the default setting, use the no form of this command.

**[no] spanning-tree mstp restricted-tcn**

## Parameters

None

## Default Value

TCN restriction of the port is disabled by default.

## Command Mode

Port configuration mode

## Usage Guidelines

The topology change will not be transferred to other port if TCN restriction of the port is enabled.

## Example

None

### 23.1.20 show spanning-tree mstp

## Syntax

To browse the MSTP information, run `show spanning-tree mstp [instance instance-id]`. If the instance parameter is not in the command syntax, the information about all spanning-tree instances will be displayed.

**show spanning-tree mstp [instance *instance-id*]**

## Parameters

Parameters	Description
<i>instance-id</i>	<b>Number of the STP instance, which ranges between 0 and 15</b>

## Default Value

None

## Usage Guidelines

This command can be used in monitoring mode, global configuration mode or port mode.

## Example

The following example shows how to browse all spanning-tree instances. MST00 stands for CIST, while Type stands for the connection type of the corresponding port.

```
Switch#show spanning-tree mstp
```

```

MST00          Vlans Mapped:          1,4-4094
Bridge         Address      00E0.0F64.8365      Priority 32768 (32768 mst-id 0)
Root           This bridge is the CIST and regional root

```

```
Configured          Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times         Hello Time 2, Forward Delay 15, Max Age 20
Interface          Role Sts Cost      Pri.Nbr Type
-----
G0/1              Desg FWD 200000   128.1 P2p
G0/2              Desg FWD 200000   128.2 Edge
MST01             Vlans Mapped: 2
Bridge            Address 00E0.0F64.8365  Priority 32769 (32768 mst-id 1)
Root              This bridge for MST01
```

```
Interface          Role Sts Cost      Pri.Nbr Type
-----
G0/1              Desg FWD 200000   128.1 P2p
```

MST02 Vlans Mapped: 3

Bridge Address 00E0.0F64.8365 Priority 32770 (32768 mst-id 2)

Root This bridge for MST02

```
Interface          Role Sts Cost Pri.Nbr Type
-----
G0/1              Desg FWD 200000   128.1 P2p
```

### 23.1.21 *show spanning-tree mstp region*

#### Syntax

To browse the area configuration information about MSTP, run the following command.

**show spanning-tree mstp region**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Example

In the following example, MST Config Table is to display the relationship between VLAN and spanning-tree instance.

```
Switch_config# show spanning-tree mstp region
```

MST Region:

Name: [reg01]

Revision: [0]

MST Config Table:

Instance	VLAN IDs
0	1,4-4094
1	2
2	3

### 23.1.22 show spanning-tree mstp detail

#### Syntax

To browse the detailed information about MSTP, run the following command.

```
show spanning-tree mstp detail
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to browse the detailed information about MSTP, which includes the port connection types and the configuration of optional attributes.

```
Switch#show spanning-tree mstp detail
```

```
MST00      Vlans Mapped:      1,4-4094
Bridge      Address 00E0.0F64.8365   Priority 32768 (32768 mst-id 0)
Root        This bridge is the CIST and regional root
Configured  Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times  Hello Time 2, Forward Delay 15, Max Age 20
```



GigaEthernet0/1 of MST00 is designated forwarding

Port Info            Port ID 128.1            Priority 128            Cost 200000

Designated Root    Address 00E0.0F64.8365 Priority 32768    Cost 0

CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0

Designated Bridge Address 00E0.0F64.8365 Priority 32768 Port ID 128.1

Edge Port:    disabled                            Link Type: point-to-point (auto)

Bpdu Guard:   disabled (default)    Root Guard: disabled (default)

Loop Guard: disabled (default)

Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec

Number of transitions to forwarding state: 1

Bpdu sent 335, received 5

GigaEthernet0/2 of MST00 is designated forwarding

Port Info            Port ID 128.47            Priority 128            Cost 200000

Designated Root    Address 00E0.0F64.8365    Priority 32768            Cost 0

CIST Regional Root Address 00E0.0F64.8365    Priority 32768            Cost 0

Designated Bridge Address 00E0.0F64.8365    Priority 32768            Port ID 128.2

Edge Port: enabled (auto)                            Link Type: point-to-point (auto)

Bpdu Guard:   disabled (default)                            Root Guard: disabled (default)

Loop Guard: disabled (default)

Timers: message expires in 0 sec, forward delay 0 sec, up time 1485 sec

Number of transitions to forwarding state: 1

Bpdu sent 744, received 0

MST01            Vlans Mapped: 2

Bridge            Address 00E0.0F64.8365    Priority 32769 (32768 mst-id 1)

Root              This bridge for MST01

GigaEthernet0/1 of MST01 is designated forwarding

Port Info            Port ID 128.1            Priority 128            Cost 200000

```

Designated Root    Address 00E0.0F64.8365    Priority 32769    Cost 0
Desingated Bridge Address 00E0.0F64.8365    Priority 32769    Port ID 128.1
Timers:    message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0

```

MST02Vlans Mapped: 3

```

Bridge            Address 00E0.0F64.8365    Priority 32770 (32768 mst-id 2)
Root              This bridge for MST02

```

GigaEthernet0/1 of MST02 is designated forwarding

```

Port Info          Port ID 128.1            Priority 128        Cost 200000
Designated Root   Address 00E0.0F64.8365    Priority 32770     Cost 0
Desingated Bridge Address 00E0.0F64.8365    Priority 32770     Port ID 128.1
Timers:    message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0

```

### 23.1.23 show spanning-tree mstp interface

#### Syntax

To browse the information about a port under MSTP, run the following command.

```
show spanning-tree mstp interface interface-id
```

#### Parameters

Parameters	Description
<i>interface-id</i>	interface name, for instance, "G0/1", "GigaEthernet0/2".

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to browse the information about interface G0/1.

```
Switch#show spanning-tree mstp interface g0/1
```

GigaEthernet0/1 of MST00 is designated forwarding

```
Port Info      Port ID 128.1 Priority 128 Cost 200000 Designated Root      Address
00E0.0F64.8365 Priority 32768 Cost 0 CIST Regional Root      Address 00E0.0F64.8365
Priority 32768 Cost 0
```

```
Designated Bridge  Address 00E0.0F64.8365 Priority 32768 Port ID 128.1 Edge Port:
disabled          Link Type: point-to-point (auto)
```

```
Bpdu Guard: disabled (default) Root Guard: disabled (default) Loop Guard: disabled
(default)
```

Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1

Bpdu sent 430, received 5

GigaEthernet0/1 of MST01 is designated forwarding

```
Port Info      Port ID 128.1          Priority 128          Cost 200000
```

```
Designated Root  Address 00E0.0F64.8365 Priority 32769      Cost 0
```

```
Designated Bridge  Address 00E0.0F64.8365 Priority 32769      Port ID 128.1
```

Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1

MST Config Message transmitted 430, received 0

GigaEthernet0/1 of MST02 is designated forwarding

```
Port Info      Port ID 128.1          Priority 128          Cost 200000
```

```
Designated Root  Address 00E0.0F64.8365 Priority 32770      Cost 0
```

```
Designated Bridge  Address 00E0.0F64.8365 Priority 32770      Port ID 128.1
```

Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1

MST Config Message transmitted 430, received 0

```
Instance Role Sts Cost      Pri.Nbr      Vlans Mapped
-----
```

```
0      Desg FWD 200000 128.1      1,4-4094
```

```
1    Desg FWD 200000 128.1    2
2    Desg FWD 200000 128.1    3
```

### 23.1.24 *show spanning-tree mstp protocol-migration*

#### Syntax

To browse the protocol transfer information on an interface under MSTP, run the following command.

**show spanning-tree mstp protocol-migration**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to browse the information about protocol transfer on an interface. In the following example, interface G0/1 is running in 802.1D STP mode.

```
Switch#show spanning-tree mstp protocol-migration
```

```
MSTP Port Protocol Migration
```

```
Interface    Protocol
```

```
-----
```

```
G0/1        802.1D
```

## Chapter 24 STP Optional Characteristic Configuration Commands

### 24.1 STP Optional Characteristic Configuration Commands

#### 24.1.1 spanning-tree portfast

##### Syntax

To configure the portfast attribute in global configuration mode, run `spanning-tree portfast {bpdufilter default | bpduguard default | default}`. To cancel this attribute in global configuration mode, run `no spanning-tree portfast {bpdufilter default | bpduguard default | default}`.

**spanning-tree portfast** {bpdufilter | bpduguard | default}

**no spanning-tree portfast** {bpdufilter | bpduguard | default}

To configure the portfast attribute in port configuration mode, run `spanning-tree portfast [disable | trunk]`. To cancel this attribute in port configuration mode, run `no spanning-tree portfast`.

**spanning-tree portfast** [disable]

**no spanning-tree portfast**

##### Parameters

Parameters	Description
<i>bpdufilter</i>	<b>Starts the BPDU filtration.</b>
<i>bpduguard</i>	<b>Starts the BPDU protection.</b>
<i>default</i>	<b>Means the default mode.</b>

##### Default Value

This function is not enabled by default.

##### Usage Guidelines

The portfast attribute enables a port in SSTP/PVST mode to promptly enter the forwarding state without state change. This configuration invalidates in RSTP/MSTP mode.

After the portfast attribute is configured, it need be protected through BPDU Guard configuration or BPDU Filter configuration.

##### Command Mode

Global or port configuration mode

##### Example

The following example shows how to enable the Port Fast attribute in global configuration mode.

```
Switch_config# spanning-tree portfast default
```

```
Switch_config#
```

The following example shows how to enable the attributes of port g0/1:

```
Switch_config_g0/1# spanning-tree portfast
```

```
Switch_config_g0/1#
```

### *24.1.2 spanning-tree bpduguard*

#### Syntax

To configure BPDU Guard, run `spanning-tree bpduguard {disable | enable}`. To cancel BPDU Guard, run `no spanning-tree bpduguard`.

**spanning-tree bpduguard {disable | enable}**

**no spanning-tree bpduguard**

#### Parameters

None

#### Default Value

This function is not enabled by default.

#### Usage Guidelines

In SSTP/PVST mode, if a port that has the BPDU Guard function and the Portfast function configured receives BPDU, this port will be mandatorily shut down. You have to configure the port manually to resume this port. In RSTP/MSTP mode, if a BPDU-Guard-configured port receives BPDU, the port will be set to the Blocking state in a period of time.

#### Command Mode

Port configuration mode

#### Example

The following example shows how to enable BPDU protection on port g0/1.

```
Switch_config_g0/1# spanning-tree bpduguard enable
```

```
Switch_config_g0/1#
```

### *24.1.3 spanning-tree bpdupfilter*

#### Syntax

To configure the BPDU filtration, run `spanning-tree bpdupfilter {disable | enable}`. To cancel the BPDU filtration, run `no spanning-tree bpdupfilter`.

**spanning-tree bpdupfilter {disable | enable}**

**no spanning-tree bpdupfilter**

#### Parameters

None

### Default Value

This function is not enabled by default.

### Usage Guidelines

In SSTP/PVST mode, a port which has the BPDU Filter function and the Port Fast function configured receives BPDU, the BPDU Filter attribute and the Port Fast attribute are automatically shut down. In this case, the port resumes to be a normal port which first enters the listening state, the learning state and then the forwarding state.

This function invalidates in RSTP/MSTP mode.

### Command Mode

Port configuration mode

### Example

The following example shows how to enable BPDU filtration on port g0/1.

```
Switch_config_g0/1# spanning-tree bpdufilter enable
```

```
Switch_config_g0/1#
```

#### *24.1.4 spanning-tree uplinkfast*

### Syntax

To configure the Uplink Fast function, run this command. To return to the default setting, use the no form of this command.

**spanning-tree uplinkfast**

**no spanning-tree uplinkfast**

### Parameters

None

### Default Value

This function is not enabled by default.

### Usage Guidelines

The Uplink Fast function validates only in SSTP/PVST mode.

### Command Mode

Global configuration mode

### Example

The following example shows how to enable the Uplink Fast attribute.

```
Switch_config# spanning-tree uplinkfast
```

```
Switch_config#
```

### 24.1.5 *spanning-tree backbonefast*

#### Syntax

To configure the backbonefast function, run `spanning-tree backbonefast`. To cancel the backbonefast function, run `no spanning-tree backbonefast`.

**spanning-tree backbonefast**

**no spanning-tree backbonefast**

#### Parameters

None

#### Default Value

This function is not enabled by default.

#### Usage Guidelines

The backbonefast function validates only in SSTP/PVST mode.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to enable the backbonefast function:

```
Switch_config# spanning-tree backbonefast
```

```
Switch_config#
```

### 24.1.6 *spanning-tree guard*

#### Syntax

To configure the Port Guard function, run `spanning--tree guard {loop | none | root}`. To cancel this function, run `no spanning--tree guard`.

**spanning-tree guard {loop | none | root}**

**no spanning-tree guard**

#### Parameters

Parameters	Description
<i>loop</i>	<b>Guard loop.</b>
<i>none</i>	<b>Guard none.</b>
<i>root</i>	<b>Guard root</b>

#### Default Value



This protection function is not enabled.

### Usage Guidelines

The Root Guard attribute can prevent a port from serving as a root port after it receives a higher-priority BPDU.

The Loop Guard attribute can protect a port after it changes from a root port or an alternate port to a designated port. This function can prevent a port from generating a loop when the port cannot receive BPDU continuously.

### Command Mode

Port configuration mode

### Example

The following example shows how to prevent port g0/1 from being the root:

```
Switch_config_g0/1# spanning-tree guard root
```

```
Switch_config_g0/1#
```

### 24.1.7 *spanning-tree loopguard*

#### Syntax

To configure the guard loop in global configuration mode, run `spanning-tree loopguard default`. To cancel the guard loop in global configuration mode, run `no spanning-tree loopguard default`.

**spanning-tree loopguard default**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

### Command Mode

Global configuration mode

### Example

The following example shows how to enable the loopguard function.

```
Switch_config# spanning-tree loopguard default
```

```
Switch_config#
```

### 24.1.8 *spanning-tree loopfast*

#### Syntax

To enable Loop Fast in global configuration mode, run `spanning-tree loopfast`. To return to the default setting, use the `no` form of this command.

#### **spanning-tree loopfast**

To set Loop Fast attribute, run this command.

#### **spanning-tree loopfast**

To disable the Loop Fast attribute, use the `no` form of this command.

#### **spanning-tree loopfast disable**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

**Please configure this command under the guide of technical engineers.**

#### Command Mode

Global configuration mode and interface configuration mode

#### Example

The following example shows how to enable loopfast in global configuration mode and disable the function on port G0/1.

```
Switch_config#spanning-tree loopfast
Switch_config#int g0/1
Switch_config_g0/1#spanning-tree loopfast disable
Switch_config_g0/1#exit
Switch_config#
```

### 24.1.9 *spanning-tree fast-aging*

#### Syntax

To enable or disable the fast aging mechanism of the address table, run the following commands.

#### **spanning-tree fast-aging**

#### **no spanning-tree fast-aging**

To enable or disable the protection of fast aging of the address table, run the following commands.

**spanning-tree fast-aging protection**

**no spanning-tree fast-aging protection**

To configure the time of aging protection of the address table, run the following commands.

**spanning-tree fast-aging protection time *value***

**no spanning-tree fast-aging protection time**

Parameters

Parameters	Description
<i>value</i>	Stands for the aging protection time. 10-60 seconds (15 seconds by default)

Default Value

Fast aging is enabled by default. However protection is not enabled by default.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to enable fast aging protection and set the protection time to 30 seconds.

```
Switch_config#spanning-tree fast-aging protection
```

```
Switch_config#spanning-tree fast-aging protection time 30
```

#### ***24.1.10 spanning-tree fast-aging flush-fdb***

Syntax

To enable or disable FDB-Flush, run the following commands.

**spanning-tree fast-aging flush-fdb**

**no spanning-tree fast-aging flush-fdb**

Parameters

None

Default Value

FDB-Flush is enabled by default.

Usage Guidelines

**Please configure this command under the guide of technical engineers.**

FDB-Flush is independent of fast aging. FDB-Flush can be configured while **nono spanning-tree fast-aging** is configured. But fast aging protection function has no effect on FDB-Flush.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to disable fast aging and enable FDB-Flush.

```
Switch_config#no spanning-tree fast-aging
```

```
Switch_config#spanning-tree fast-aging flush-fdb
```

#### *24.1.11 spanning-tree bpdu-terminal*

#### Syntax

To enable or disable BPDU Terminal, run the following commands.

**spanning-tree bpdu-terminal**

**no spanning-tree bpdu-terminal**

#### Parameters

None

#### Default Value

BPDU Terminal is disabled by default.

#### Usage Guidelines

BPDU terminal function can forbid forwarding BPDU when there is no STP running.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to enable BPDU Terminal:

```
Switch_config#spanning-tree bpdu-terminal
```

## Chapter 25 Port Aggregation Commands

### 25.1 Port Aggregation Commands

#### 25.1.1 aggregator-group

##### Syntax

To configure port aggregation, run `aggregator-group id mode {lacp-negotiation | static}`. To resume the default settings, run `no aggregator-grou`.

**aggregator-group** *id* mode {lacp | static}

**no aggregator-group**

##### Parameters

Parameters	Description
<i>id</i>	Stands for the ID of a logistic port. Value range: 1-32
<i>lacp</i>	Enables LACP negotiation.
<i>static</i>	Disables port negotiation.

##### Default Value

The port is not aggregated.

##### Usage Guidelines

Port's link aggregation is to bind several ports of same attributes into a logic port. The binding process is conducted through LACP negotiation or is mandatorily conducted without any negotiation.

If the static aggregation is used, please make sure the attribute of the ports to be binded is the same and vlan attribute is consisted.

When configuring port aggregation, you can select the LACP negotiation mode. In Active mode, the port will transmit the LACP packet actively for LACP negotiation; In passive mode, the port responds to the LACP packets passively and conducts the LACP negotiation passively.

Some models of switches do not support the dynamic negotiation mode, hence, the corresponding configuration command is not provided.

##### Command Mode

Port configuration mode

##### Example

The following example shows how to bind port `g0/1` and port `g0/2` to logic port `port-aggregator 3`, and then to use LACP negotiation.

```
Switch_config_g0/1# aggregator-group 3 mode lacp
```

```
Switch_config_g0/1# interface g0/2
```

```
Switch_config_g0/2# aggregator-group 3 mode lacp
```

### 25.1.2 aggregator-group load-balance

#### Syntax

```
aggregator-group load-balance {dst-mac | src-mac | both-mac}
```

```
no aggregator-group load-balance
```

To configure load balance after port aggregation, run `aggregator-group load-balance {dst-mac | src-mac | both-mac | src-ip | dst-ip | both-ip}`. To resume the default settings, run `no aggregator-group load-balance`.

#### Parameters

Parameters	Description
<i>dst-mac</i>	Means taking the destination MAC address as the standard.
<i>src-mac</i>	Means taking the source MAC address as the standard.
<i>both-mac</i>	Means taking the destination/source MAC address as the standard.

#### Default Value

```
scr-mac
```

#### Usage Guidelines

To ensure each physical port to reach load balance after port aggregation, you need averagely distribute data flow on each physical port. This command can help reaching this function.

When the `dst-mac` mode is chosen, the distributed data flow takes the destinationmacaddress of the data packet as the standard. Packets with a same MAC address are transmitted from just one physical port. However, the `SRC-MAC` mode takes the sourcemacaddress as the standard.

Switches of different models have different load balance policies. Only the load balance policy is displayed in the command prompt. If no load balance policies is supported or only one load balance policy is supported, the related sub-command will not be displayed.

#### Command Mode

```
Port configuration mode
```

#### Example

The following example shows how to change the load balance mode of port-aggregator to the `src-mac` mode.

```
Switch_config# int port-aggregator 1
```

```
Switch_config_p1#
```

```
Switch_config_p1# aggregator-group load-balance src-mac
```

### 25.1.3 *show aggregator-group*

#### Syntax

**show aggregator-group** [*id*] {detail|brief|summary}

To display the detailed information about the aggregator-group, run the following command.

#### Parameters

Parameters	Description
<i>id</i>	ID of a specific logic port

#### Default Value

None

#### Usage Guidelines

This command is used to display the information about port aggregation.

#### Command Mode

EXEC

### 25.1.4 *show interface port-aggregator*

#### Syntax

To display the detailed information about the aggregator-group, run the following command.

**show interface port-aggregator** *id*

#### Parameters

Parameters	Description
<i>id</i>	ID of a specific port

#### Default Value

None

#### Usage Guidelines

This command is used to display the information about port aggregation.

#### Command Mode

EXEC

#### Example

The following example shows how to display the information about aggregated port 1.

```
Switch#show interface port-aggregator 1
```

```
Port-aggregator1 is down, line protocol is down
```

```
Hardware is PortAggregator, Address is 0000.0000.0000(0000.0000.0000)
```

```
MTU 1500 bytes, BW 1000 kbit, DLY 2000 usec
```

```
Encapsulation ARPA, loopback not set
```

```
Members in this Aggregator:
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 multicasts
```

```
0 input errors, 0 input discards
```

```
0 CRC, 0 frame, 0 overrun, 0 ignored
```

```
0 packets output, 0 bytes, 0 underruns
```

```
Transmitted 0 broadcasts, 0 multicasts
```

```
0 output errors, 0 discards
```

```
0 output buffer failures, 0 output buffers swapped out
```

Note: Members in this Aggregator means physical ports which are aggregated to the logical port. The statistics values are explained as follows:

Packets input means the input of all packets, including broadcast packets, multicast packets and unicast packets.

Bytes means the byte volume of all packets. Broadcasts means received broadcast packets. Broadcasts means received broadcast packets. Input errors means received error packets.

Input discards means that the received packets are dropped, such as the received packets when the interface protocol is down.

Packets output means the output of all packets, including broadcast packets, multicast packets and unicast packets.

Bytes means the byte volume of all transmitted packets. Broadcasts means transmitted broadcast packets.

Multicasts means transmitted multicast packets. Output errors means transmitting error packets.

Output discards means that the transmitted packets are dropped, such as the transmitted packets when the interface protocol is down.

### *25.1.5 debug lacp errors*

Syntax

```
debug lacp errors
```



**no debug lacp errors**

To export the LACP debugging error, run debug lacp errors.

**Parameters**

None

**Default Value**

None

**Usage Guidelines**

This command is used to export all error information occurred during LACP running. The error information can help locating the errors.

**Command Mode**

EXEC

**Example**

```
Switch# debug lacp errors
```

```
Switch#
```

**25.1.6 debug lacp state****Syntax**

```
debug lacp state
```

**no debug lacp state**

To export the information about the LACP state machine, run debug lacp state.

**Parameters**

None

**Default Value**

None

**Command Mode**

EXEC

**Example**

```
Switch# debug lacp state
```

```
Switch#
```

**25.1.7 debug lacp packet****Syntax**

```
debug lacp packet
```

**no debug lacp packet**

To export the information about LACP receiving or transmitting packets, run `debug lacp packet`.

#### Parameters

None

#### Default Value

None

#### Command Mode

EXEC

#### Example

```
Switch# debug lacp packet
```

```
Switch#
```

## Chapter 26 PDP Configuration Commands

PDP is a two-layer protocol specially used to detect network devices. PDP is used in Network Management Service (NMS) to detect all neighboring devices of an already known device. Using `PDP enable` you can learn the SNMP agent address and the types of neighboring devices. After neighboring devices are detected through PDP, the NMS can require neighboring devices through SNMP to obtain the network topology.

### 26.1 PDP Configuration Commands

PDP commands include:

- `pdp timer`
- `pdp holdtime`
- `pdp version`
- `pdp run`
- `pdp enable`
- `show pdp traffic`
- `show pdp neighbor`

#### 26.1.1 `pdp timer`

##### Syntax

To set the time of the PDP timer, run this command. To return to the default setting, use the `no` form of this command.

```
[no|default] pdp timer seconds
```

##### Parameters

Parameters	Description
------------	-------------

<i>seconds</i>	<b>Means the interval for PDP to transmit packets outside, which ranges from 5 seconds to 254 seconds. The unit is second.</b>
----------------	--

### Default Value

The default settings is 60 seconds.

### Usage Guidelines

This command is configured in global configuration mode.

### Example

The following example shows that a switch transmits PDP packets every 5 seconds.

```
pdp timer 5
```

### 26.1.2 *pdp holdtime*

#### Syntax

To set the time of the PDP timer, run this command. To return to the default setting, use the no form of this command.

```
[no|default] pdp holdtime seconds
```

#### Parameters

Parameters	Description
<i>seconds</i>	<b>Means the time needed for deleting the neighbor information, which ranges from 10 to 255 seconds.</b>

### Default Value

The default settings is 180 seconds.

### Usage Guidelines

This command is configured in global configuration mode.

### Example

The following example shows that the neighbor information is kept for 15 seconds.

```
pdp holdtime 15
```

### 26.1.3 *pdp version*

#### Syntax

To set the PDP version, run `pdp version <1|2>`. To disable this command, use the no form of this command.

```
[no] pdp version <1|2>
```

#### Parameters

Parameters	Description
<i>version</i>	Means the PDP version, which is 1 or 2.

### Default Value

The default version is version 2.

### Usage Guidelines

This command is configured in global configuration mode.

### Example

The following example shows that the PDP version of a switch is version 1.

```
pdp version 1
```

#### 26.1.4 *pdp run*

### Syntax

To enable PDP, run `pdp run`. To disable PDP, use the `no` form of this command.

```
[no] pdp run
```

### Parameters

None

### Default Value

The PDP protocol is disabled.

### Usage Guidelines

This command is configured in global configuration mode.

### Example

The following example shows to disable PDP.

```
no pdp run
```

#### 26.1.5 *pdp enable*

### Syntax

To enable PDP on a port, run `pdp enable`. To return to the default setting, use the `no` form of this command.

```
[no] pdp enable
```

### Parameters

None

### Default Value

PDP is enabled by default.

### Usage Guidelines

This command is set in port configuration mode and takes effect in port or global mode only when PDP is enabled. It is usually used in disabling protocols of some ports.

### Example

The following example shows that PDP is disabled on port g0/1.

```
switch_config_g0/1#no pdp enable
```

### 26.1.6 show pdp traffic

#### Syntax

To display the number of received PDP packets, run this command.

```
show pdp traffic
```

#### Parameters

None

#### Default Value

None

### Usage Guidelines

It is used to browse the running of PDP.

### Example

```
Switch_config#show pdp traffic
```

```
Packets output: 253491, Input: 0
```

```
Hdr syntax: 0, Chksum error: 0
```

```
No memory: 0, Invalid packet: 0
```

### 26.1.7 show pdp neighbor

#### Syntax

To display the PDP neighbor, run this command. show pdp neighbor

#### Parameters

None

#### Default Value

None

### Usage Guidelines

It is used to browse the running of PDP.

### Example

```
Switch_config#show pdp neighbor
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Gig0/1	169	Gig0/1	COM, RISC	R S

## Chapter 27 LLDP Configuration Commands

### 27.1 LLDP Commands

#### 27.1.1 *Ildp run*

##### Syntax

To enable LLDP, run `Ildp run`; to disable LLDP, run `no Ildp run`.

**Ildp run**

**no Ildp run**

##### Parameters

None

##### Default Value

The debugging switch is disabled.

##### Usage Guidelines

The port will send Ildp packets after the Ildp function is enabled.

##### Command Mode

Global configuration mode

##### Example

The following command is used to enable LLDP.

```
switch_config# Ildp run
```

#### 27.1.2 *Ildp holdtime*

##### Syntax

To configure the ttl value of LLDP, run `Ildp holdtime time`. To resume the default transmission delay, run `no Ildp holdtime`.

`Ildp holdtime time`

`no Ildp holdtime`

##### Parameters

Parameters	Description
<i>time</i>	Holdtime of the to-be-transmitted packet Range: 0-65535 seconds

### Default Value

120s

### Usage Guidelines

In normal condition, the remote information stored in MIB will update before aging. But the frame may loss in sending and causes the information ages. For avoiding this, you need to set the value of TTL and ensure the update LLDP frame is forwarded time after time.

### Command Mode

Global configuration mode

### Example

The following example shows how to set the ttl value of LLDP to 100 seconds.

```
switch_config# lldp holdtime 100
```

```
switch_config#
```

### 27.1.3 lldp timer

#### Syntax

To configure the transmission delay of LLDP, run `lldp timer time`. To resume the default transmission delay, run `no lldp timer`.

**lldp timer** *time*

**no lldp timer**

#### Parameters

Parameters	Description
<i>time</i>	Interval for LLDP to transmit the packets Range: 5-65534 seconds

### Default Value

30s

### Usage Guidelines

The transmission interval of the LLDP message must be shorter than its storage time, ensuring multiple updates in the storage time and preventing error which is led by packet loss.

### Command Mode

Global configuration mode

### Example

The following example shows how to configure the transmission interval of LLDP to 24 seconds.

```
switch_config# lldp timer 24
```

```
switch_config#
```

### 27.1.4 *lldp reinit*

#### Syntax

To configure the transmission delay of LLDP, run `lldp reinit time`. To resume the default transmission delay, run `no lldp reinit`.

```
lldp reinit time
```

```
no lldp reinit
```

#### Parameters

Parameters	Description
<i>time</i>	Transmission delay of LLDP, whose values range from two to five seconds Range: 2-5 seconds

#### Default Value

```
2 s
```

#### Usage Guidelines

LLDP information will be forwarded automatically in two conditions: first, the status or value of one or more information elements (management objects) change; second, the sending timer timeouts. A single information change cause the LLDP packet is forwarded and a series of information change may cause many LLDP frames forwarded, but a frame can only report one change. For avoiding this, the web management defines the interval of two continuous LLDP frames.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to set the transmission delay of LLDP to five seconds.

```
switch_config# lldp reinit 5
```

```
switch_config#
```

### 27.1.5 *lldp tlv-select*

#### Syntax

To add TLV which is transmitted by the LLDP message, run `lldp med-tlv-select tlv-type`. To delete TLV which is transmitted by the LLDP message, run `no lldp med-tlv-select tlv-type`.

```
lldp tlv-select tlv-type
```

```
no lldp tlv-select tlv-type
```

#### Parameters

Parameters	Description
------------	-------------



<i>tlv-type</i>	<p>Stands for TLV that are available for selective transmission. Its values are:</p> <p>management-address      management address  TLV port-description      port description TLV  system-capabilities      system-capabilities TLV  system-description      system description TLV  system-name      system name TLV</p>
-----------------	--

### Default Value

All TLVs are sent.

### Usage Guidelines

Three mandatory TLVs must be sent.

### Command Mode

Global configuration mode

### Example

The following example shows how to enable the port description not to be transmitted in the message.

```
switch_config#no lldp tlv-select port-description
```

```
switch_config#
```

#### 27.1.6 lldp dot1-tlv-select

### Syntax

To add TLV which is transmitted by the LLDP message, run `lldp med-tlv-select tlv-type`. To delete TLV which is transmitted by the LLDP message, run `no lldp med-tlv-select tlv-type`.

```
lldp dot1-tlv-select tlv-type
```

```
no lldp dot1-tlv-select tlv-type
```

### Parameters

Parameters	Description
<i>tlv-type</i>	<p>Stands for TLV that are available for selective transmission. Its values are:</p> <p>port-vlan-id      port vlan address TLV  protocol-vlan-id      port and protocol VLAN ID TLV  vlan-name      vlan名TLV</p>

### Default Value

All TLVs are sent.

### Usage Guidelines

The TLV of the protocol identity does not support transmission but supports reception.

### Command Mode

Port configuration mode

### Example

The following example shows how to enable the TLV not to be transmitted by deletion of the VLAN address of a port in the transmitted packet.

```
switch_config#int g0/1
switch_config_g0/1#no lldp dot1-tlv-select port-vlan-id
switch_config_g0/1#
```

### 27.1.7 lldp dot3-tlv-select

#### Syntax

To add TLV which is transmitted by the LLDP message, run `lldp med-tlv-select tlv-type`. To delete TLV which is transmitted by the LLDP message, run `no lldp med-tlv-select tlv-type`.

**lldp dot3-tlv-select** *tlv-type*

**no lldp dot3-tlv-select** *tlv-type*

#### Parameters

Parameters	Description
<i>tlv-type</i>	<p><b>Stands for TLV that are available for selective transmission. Its values are:</b></p> <p><b>link-aggregation</b>      link aggregation TLV</p> <p><b>macphy-config</b>        MAC/Phy configuration/status TLV</p> <p><b>max-frame-size</b>        max frame size TLV</p> <p><b>power</b>                    Power Via MDI TLV</p>

#### Default Value

All TLVs are sent.

#### Usage Guidelines

None

#### Command Mode

Port configuration mode

### Example

The following example shows how to enable the TLV not to be transmitted by deletion of the MAC/Phy configuration/status of a port in the transmitted packet.

```
switch_config#int g0/1
```

```
switch_config_g0/1#no lldp dot3-tlv-select macphy-config
```

```
switch_config_g0/1#
```

### 27.1.8 lldp med-tlv-select

#### Syntax

To add TLV which is transmitted by the LLDP message, run `lldp med-tlv-select tlv-type`. To delete TLV which is transmitted by the LLDP message, run `no lldp med-tlv-select tlv-type`.

```
lldp med-tlv-select tlv-type
```

```
no lldp med-tlv-select tlv-type
```

#### Parameters

Parameters	Description								
<i>tlv-type</i>	<p>Stands for TLV that are available for selective transmission. Its values are:</p> <table> <tr> <td><b>network-policy</b></td> <td><b>network policy TLV</b></td> </tr> <tr> <td><b>inventory</b></td> <td><b>inventory management TLV</b></td> </tr> <tr> <td><b>location</b></td> <td><b>location identification TLV</b></td> </tr> <tr> <td><b>power-management</b></td> <td><b>expand Power Via MDI TLV</b></td> </tr> </table>	<b>network-policy</b>	<b>network policy TLV</b>	<b>inventory</b>	<b>inventory management TLV</b>	<b>location</b>	<b>location identification TLV</b>	<b>power-management</b>	<b>expand Power Via MDI TLV</b>
<b>network-policy</b>	<b>network policy TLV</b>								
<b>inventory</b>	<b>inventory management TLV</b>								
<b>location</b>	<b>location identification TLV</b>								
<b>power-management</b>	<b>expand Power Via MDI TLV</b>								

#### Default Value

All TLVs are sent.

#### Usage Guidelines

By default, the TLV of MED cannot be transmitted. When the TLV of MED need be transmitted, the MED capability TLV must be transmitted. Hence it does not fall into the choice.

#### Command Mode

Port configuration mode

#### Example

The following example shows how to enable the TLV not to be transmitted by deletion of the detailed list management in a transmitted packet.

```
switch_config#int g0/1
```

```
switch_config_g0/1#no lldp med-tlv-select inventory
```

```
switch_config_g0/1#
```

### 27.1.9 lldp transmit

#### Syntax

```
lldp transmit
```

```
no lldp transmit
```

To set the port to send the LLDP message, run `lldp transmit`. To forbid receiving the LLDP message, run `no lldp transmit`.

#### Parameters

None

#### Default Value

Transmittable LLDP message mode

#### Usage Guidelines

Only after the LLDP module is enabled can the command be valid.

#### Command Mode

Port configuration mode

#### Example

The following example shows how to set port `g0/1` not to send the LLDP message.

```
switch_config_g0/1# no lldp transmit
switch_config_g0/1#
```

#### 27.1.10 *lldp receive*

#### Syntax

**lldp receive**

**no lldp receive**

To set the port to the receivable LLDP message mode, run `lldp receive`. To forbid receiving the LLDP message, run `no lldp receive`.

#### Parameters

None

#### Default Value

Receivable LLDP message mode

#### Usage Guidelines

Only after the LLDP module is enabled can the configuration be valid.

#### Command Mode

Port configuration mode

#### Example

The following example shows how to set port `g0/1` not to receive the LLDP message.

```
switch_config_g0/1# no lldp receive
switch_config_g0/1#
```

### 27.1.11 lldp management-ip

#### Syntax

```
lldp management-ip A.B.C.D
```

```
no lldp management-ip
```

To configure the management address of the LLDP port, run `lldp management-ip A.B.C.D`. To resume the default transmission delay, run `no lldp management-ip`.

#### Parameters

Parameters	Description
<i>A.B.C.D</i>	Stands for the management IP address that will be specified.

#### Default Value

The default management address is the IP address of the VLAN interface that `pvid` corresponds to; if this IP address does not exist, the default management address is 0.0.0.0.

#### Usage Guidelines

The configured management IP address should be the IP address related with a port.

#### Command Mode

Port configuration mode

#### Example

The following example shows how to set the management IP address of port `g0/1` to 90.0.0.99.

```
switch_config_g0/1# lldp management-ip 90.0.0.99
switch_config_g0/1#
```

### 27.1.12 lldp trap-send

#### Syntax

```
lldp tranp-send lldp-mib
```

To forward trap notification to `lldp mib`, run this command.

```
lldp tranp-send ptopo-mib
```

To forward trap notification to `ptopo mib`, run this command.

#### Parameters

None

#### Default Value

None

## Usage Guidelines

None

## Command Mode

Global configuration mode

## Example

The following example shows how to send trap notification to lldp mib.

```
switch_config#lldp trap-send lldp-mib
switch_config#
```

The following example shows how to send trap notification to ptopo mib.

```
switch_config#lldp trap-send ptopo-mib
switch_config#
```

### 27.1.13 location elin identifier id WORD

## Syntax

**location elin identifier** *id* *WORD*

**no location elin identifier** *id*

To add the elin information, run `location elin identifier id WORD`; to delete the elin information, run `no location elin identifier id`.

## Parameters

Parameters	Description
<i>id</i>	Stands for the ID of the to-be-set elin, which ranges from 1 to 65535.
<i>WORD</i>	Stands for the content of the configured elin, which ranges from 10 to 25 bytes.

## Default Value

None

## Usage Guidelines

None

## Command Mode

Global configuration mode

## Example

The following example shows how to set the identifier to 1 and the content of elin to 1234567890.

```
switch_config# location elin identifier 1 1234567890
```

switch\_config#

### 27.1.14 location civic identifier id

#### Syntax

**location civic identifier id****no location civic identifier id**

To enter the location configuration mode and set the civic information, run `location civic identifier id`. To delete the civic information, run `no location civic identifier id`.

#### Parameters

Parameters	Description
<i>id</i>	Stands for the ID of the to-be-set civic, which ranges from 1 to 65535.

#### Default Value

None

#### Usage Guidelines

After the system enters the location configuration mode, you can run the following commands to conduct the corresponding configuration to the civic of the ID.

Parameters	Purpose
<i>(no) language WORD</i>	Sets the language.
<i>(no) state WORD</i>	Sets the state's (provincial) name, such as shanghai.
<i>(no) county WORD</i>	Sets the name of a county.
<i>(no) city WORD</i>	Sets the name of a city.
<i>(no) division WORD</i>	Sets the name of a division.
<i>(no) neighborhood WORD</i>	Sets the name of neighborhood.
<i>(no) street WORD</i>	Sets the name of a street.
<i>(no) leading-street-dir WORD</i>	Sets the direction of a main street, such as N (north).
<i>(no) trailing-street-suffix WORD</i>	Sets the suffix of a small street, such as SW.
<i>(no) street-suffix WORD</i>	Sets the suffix of a street, such as platz.
<i>(no) number WORD</i>	Sets the street number, such as number 123.
<i>(no) street-number-suffix WORD</i>	Sets the suffix of the street number, such as number 1/2 of A road.
<i>(no) landmark WORD</i>	Sets the landmark, such as Columbia University.
<i>(no) additional-location WORD</i>	Sets the additional location.
<i>(no) name WORD</i>	Sets the information about a resident, such as Joe's haircut shop.

<i>(no) postal-code WORD</i>	<b>Sets the postal code.</b>
<i>(no) building WORD</i>	<b>Sets the information about a building.</b>
<i>(no) unit WORD</i>	<b>Sets the information about a unit.</b>
<i>(no) floor WORD</i>	<b>Sets the information about a floor.</b>
<i>(no) room WORD</i>	<b>Sets the information about a room.</b>
<i>(no) type-of-place WORD</i>	<b>Sets the type of a place, such as office.</b>
<i>(no) postal-community WORD</i>	<b>Sets the name of a postal office.</b>
<i>(no) post-office-box WORD</i>	<b>Sets the name of a postal box, such as 12345.</b>
<i>(no) additional-code WORD</i>	<b>Sets the additional code.</b>
<i>(no) country WORD</i>	<b>Sets the name of a country.</b>
<i>(no) script WORD</i>	<b>Sets the script.</b>

## Command Mode

Global configuration mode

### Example

The following example shows how to set the civic information of identifier 1.

```
Switch_config#location civic identifier 1
Switch_config_civic#language English
Switch_config_civic#city Shanghai
Switch_config_civic#street Curie
Switch_config_civic#script EN
Switch_config_civic#quit
Switch_config#
```

### 27.1.15 location elin/civic id

#### Syntax

```
location elin/civic id
```

**no location elin/civic**

To set the location for a port, run `location elin/civic id`. To delete the location of a port, run `no location elin/civic id`.

#### Parameters

Parameters	Description
------------	-------------



<i>id</i>	Stands for the ID of the to-be-set elin/civic, which ranges from 1 to 65535.
-----------	--

#### Default Value

None

#### Usage Guidelines

None

#### Command Mode

Port configuration mode

#### Example

The following example shows how to set the elin and the civic for a port.

```
Switch_config#int g0/8
Switch_config_g0/8#location elin 1
Switch_config_g0/8#location civic 1
```

#### 27.1.16 show lldp errors

##### Syntax

```
show lldp errors
```

To display the error information about the LLDP module, run this command.

##### Parameters

None

##### Default Value

None

##### Usage Guidelines

None

##### Command Mode

EXEC/global configuration mode

##### Example

The following example shows how to check the error information of lldp module.

```
switch_config#show lldp errors LLDP errors/overflows:
Total memory allocation failures: 0
Total encapsulation failures: 0
Total table overflows: 0
```

```
switch_config#
```

### 27.1.17 show lldp interface

#### Syntax

```
Show lldp interface interface-name
```

To check the transmission and reception mode, run show lldp interface interface name.

#### Parameters

Parameters	Description
<i>interface-name</i>	The interface name, for instance, "G0/1", "GigaEthernet0/1".

#### Default Value

None

#### Usage Guidelines

Only when lldp is enabled can the state of the port, the transmission and reception mode of lldp packets can be checked.

#### Command Mode

EXEC/global configuration mode

#### Example

The following example shows how to check the transmission and reception mode of port g0/1.

```
switch_config#show lldp interface g0/1
```

```
GigaEthernet0/1:
```

```
Rx: enabled
```

```
Tx: enabled
```

```
switch_config#
```

### 27.1.18 show lldp neighbors

#### Syntax

```
show lldp neighbors
```

To display the simple information about neighbors, run this command.

#### Parameters

None

#### Default Value

None

### Usage Guidelines

The command is used to display the simple information about neighbor list, including Device-ID, Local-Intf, Hldtme, Port-ID and Capability.

### Command Mode

EXEC/global configuration mode

### Example

```
switch_config#show lldp neighbors
```

Capability Codes:

(R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone

(W)WLAN Access Point,(P)Repeater,(s)station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
switch	Gig0/2	115	Gig0/32	B
switch	Gig0/32	114	Gig0/2	B

Total entries dispalyed: 2 switch\_config#

### *27.1.19 show lldp neighbors detail*

#### Syntax

```
show lldp neighbors detail
```

It is used to display the detailed information about the neighbor.

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Command Mode

EXEC/global configuration mode

#### Example

```
switch_config#show lldp neighbors detail
```

```
chassis id: 00e0.0f61.ca53
```

```
port id: Gig0/32
```

```
port description: GigaEthernet0/32
```

```
system name: switch
```

system description: s3448 software, Version 2.0.1K

serial: s35000456

Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 98

system capabilities: R B

enabled capabilities: B

Managment Address:

IP: 192.168.213.62

Auto Negotiation -- supported,enabled

Physical media capabilitise:

100baseTX(FD)

100baseTX(HD)

10baseT(FD)

10baseT(HD)

Media Attachment Unit type: 16

-----

chassis id: 00e0.0f61.ca35

port id: Gig0/2

port description: GigaEthernet0/2

system name: switch

system description: s3448 software, Version 2.0.1K

serial: s35000456

Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 95

system capabilities: R B

enabled capabilities: B

Managment Address:

IP: 90.0.0.66

Auto Negotiation -- supported, enabled

Physical media capabilitise:

100baseTX(FD)

100baseTX(HD)

10baseT(FD)

10baseT(HD)

Media Attachment Unit type: 16

-----

Total entries displayed: 2

switch#

### *27.1.20 show lldp traffic*

#### Syntax

**show lldp traffic**

To display all statistics information about LLDP, run show lldp traffic.

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Command Mode

EXEC/global configuration mode

#### Example

```
switch_config#show lldp traffic
```

```
LLDP traffic statistics:
```

```
Total frames out: 1599
```

```
Total entries aged: 0
```

```
Total frames in: 624
```

```
Total frames received in error: 0
```

```
Total frames discarded: 0
```

```
Total TLVs unrecognized: 0
```

```
switch_config#
```

### *27.1.21 show location elin*

#### Syntax

**show location elin**

To display the elin configuration of the location, run the previous command.

---

**Parameters**

None

**Default Value**

None

**Usage Guidelines**

None

**Command Mode**

EXEC/global configuration mode

**Example**

```
Switch_config#show location elin
elin information:
elin 2: 0987654321
elin 1: 1234567890
total: 2
Switch_config#
```

**27.1.22 show location civic [identifier id]****Syntax****show location civic [identifier id]**

To display the civic information of the location, run the previous command.

**Parameters**

Parameters	Description
<i>id</i>	Stands for the ID of the to-be-set civic, which ranges from 1 to 65535.

**Default Value**

None

**Usage Guidelines**

None

**Command Mode**

EXEC/global configuration mode

**Example**

```
Switch_config#show location civic
```

civic address information:

identifier: 2

Language: Chinese

Script: CN

-----

identifier: 1

City: Shanghai

Language: English

Script: EN

-----

total: 2

Switch\_config#

### *27.1.23 clear lldp counters*

#### Syntax

**clear lldp counters**

To clear the statistics information, run clear lldp counters.

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Command Mode

EXEC

#### Example

```
switch#clear lldp counters
```

```
switch#
```

```
switch#show lldp traffic
```

```
LLDP traffic statistics:
```

```
Total frames out: 0
```

```
Total entries aged: 0
```

```
Total frames in: 0
```

Total frames received in error: 0

Total frames discarded: 0

Total TLVs unrecognized: 0

switch#

switch#show lldp errors

LLDP errors/overflows:

Total memory allocation failures: 0

Total encapsulation failures: 0

Total table overflows: 0

switch#

### *27.1.24 clear lldp table*

#### Syntax

**clear lldp table**

To remove the neighbor list, run cleas lldp table.

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

None

#### Command Mode

EXEC

#### Example

```
switch#clear lldp table
```

```
switch#
```

```
switch#show lldp neighbors
```

Capability Codes:

(R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone (W)WLAN Access Point,  
(P)Repeater,(s)station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
-----------	------------	--------	---------	------------

Total entries displayed: 0



## Chapter 28 Backuplink Configuration Commands

### 28.1 Global Commands

#### 28.1.1 backup-link-group id

BackupLink provides link backup through a pair of link-layer interfaces while solving the STP problem of slow convergence. In one group of BackupLink ports, one is configured as primary port and the other as the alternate port. These ports can be exchange ports or aggregate ports. In the case that the user does not use STP protocol, BackupLink can ensure the redundancy and backup of link.

#### Syntax

To set the BackupLink group, run this command.

```
backup-link-group id
```

To delete the BackupLink group, use the no form of this command.

```
no backup-link-group id
```

#### Parameters

Parameters	Description
<i>id</i>	Stands for the instance ID of the backuplink group.

#### Default Value

The backuplink group is not configured by default.

#### Command Mode

Global configuration mode

#### Usage Guidelines

None

#### Example

```
Switch_config#backup-link-group 1
```

```
Switch_config#
```

#### Related Command

None

#### 28.1.2 backup-link-group id preemption-mode forced {delay value}

#### Syntax

To set the port-based preemption mode for the backuplink group, run this command.

```
backup-link-group id preemption-mode forced {delay value}
```

To delete the port-based preemption mode for the backuplink group, run the following command: `no backup-link-group id`

#### Parameters

Parameters	Description
<i>id</i>	Stands for the instance ID of the backuplink group.
<i>value</i>	Stands for the delay time.

#### Default Value

The backuplink group has not been set with the trait of port-based preemption by default.

#### Command Mode

Global configuration mode

#### Usage Guidelines

The command **backup-link-group *id* preemption-mode forced {delay *value*}** can be used to create BackupLink group directly.

#### Example

```
Switch_config#backup-link-group 1 preemption-mode forced delay 5
```

```
Switch_config#
```

#### Related Command

```
backup-link-group id
```

```
backup-link-group id preemption-mode bandwidth {delay value}
```

#### 28.1.3 backup-link-group id preemption-mode bandwidth {delay value}

#### Syntax

To set port bandwidth preemption mode for the backuplink group, run the following command: `backup-link-group id preemption-mode bandwidth {delay value}`

To delete port bandwidth preemption mode for the backuplink group, run the following command: `no backup-link-group id`

#### Parameters

Parameters	Description
<i>id</i>	Stands for the instance ID of the backuplink group.
<i>value</i>	Stands for the delay time.

#### Default Value

The backuplink group has not been set with the trait of port bandwidth preemption by default.

## Command Mode

Global configuration mode

## Usage Guidelines

None

## Example

```
Switch_config#backup-link-group 1 preemption-mode bandwidth delay 5
```

```
Switch_config#
```

## Related Command

backup-link-group id

backup-link-group id preemption-mode forced {delay value}

### 28.1.4 monitor-link-group id

## Syntax

To set the MonitorLink group, run the following command:

```
monitor-link-group id
```

To delete the MonitorLink group, run the following command:

```
no monitor-link-group id
```

## Parameters

Parameters	Description
<i>id</i>	<b>Stands for the instance ID of the monitorlink group.</b>

## Default Value

The MonitorLink group is not configured by default.

## Command Mode

This command is run in global configuration mode.

## Usage Guidelines

None

## Example

```
Switch_config# monitor-link-group 1
```

```
Switch_config#
```

## Related Command

None

## 28.2 Port Configuration Commands

### 28.2.1 backup-link-group id active

#### Syntax

To set a port to be an active port, run the following command:

```
backup-link-group id active
```

To cancel the primary port configuration of a port, run the following command:

```
no backup-link-group id
```

#### Parameters

Parameters	Description
<i>id</i>	Stands for the instance ID of the backuplink group.

#### Default Value

The primary port is not configured by default.

#### Command Mode

The physical port configuration mode and the converged port configuration mode

#### Usage Guidelines

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly.

#### Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group 1 active
Switch_config_g0/1#exit
```

#### Related Command

```
backup-link-group id
backup-link-group id backup
```

### 28.2.2 backup-link-group id backup

#### Syntax

To set a port to be a backup port, run the following command:

```
backup-link-group id backup
```

To cancel the edge port configuration of a port, run the following command:

```
no backup-link-group id
```

#### Parameters

Parameters	Description
<i>id</i>	Stands for the instance ID of the backuplink group.

### Default Value

The backup port is not configured by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly.

### Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group 1 backup
Switch_config_g0/1#exit
```

### Related Command

```
backup-link-group id
backup-link-group id active
```

## 28.2.3 *share-load vlan vlanmap*

### Syntax

To set VLAN load balance for the backup port, run the following command:

```
share-load vlan vlanmap
```

To delete VLAN load balance for the backup port, run the following command:

```
no share-load vlan
```

### Parameters

Parameters	Description
<i>vlanmap</i>	Stands for the VLAN value.

### Default Value

VLAN load balance is not set for the backup port by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

This command can be set only on the backup port, that is, a port must be set to be a backup port before VLAN load balance is set on the port.

For different BackupLink groups, the same group VLAN can be configured, or they have overlapping VLAN segments. If there are overlapped VLAN segments, the system will classify these VLANs into different MSTs (STGs) and conduct operations toward a group of ports, the statuses of these ports in different MSTs vary. So, typically, when the load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

### Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# share-load vlan 100-200
Switch_config_g0/1#exit
```

### Related Command

```
backup-link-group id
backup-link-group id backup
```

## 28.2.4 backup-link-group mmu transmit

### Syntax

To set MMU transmission for the ports of the backuplink group, run the following command:  
backup-link-group mmu transmit

To delete MMU transmission for the ports of the backuplink group, run the following command:  
no backup-link-group mmu

### Parameters

None

### Default Value

The MMU transmission function for the ports of the backuplink group is not set by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

**Only the ports of the backuplink group can be set to transmit, that is, the ports must be set to active or backup.**

### Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group mmu transmit
Switch_config_g0/1#exit
```

### Related Command

```
backup-link-group id
```

### 28.2.5 backup-link-group mmu receive

#### Syntax

To set MMU reception for ports, run the following command:

```
backup-link-group mmu receive
```

To delete MMU reception for ports, run the following command:

```
no backup-link-group mmu
```

#### Parameters

None

#### Default Value

The MMU reception function for the ports is not set by default.

#### Command Mode

The physical port configuration mode and the converged port configuration mode

#### Usage Guidelines

**The ports that are set to receive are not necessarily the ports of the backuplink group.**

#### Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group mmu receive
Switch_config_g0/1#exit
```

#### Related Command

None

### 28.2.6 monitor-link-group id uplink

#### Syntax

To set a port to be an uplink port, run the following command:

```
monitor-link-group id uplink
```

To cancel the uplink port configuration, run the following command:

```
no monitor-link-group id
```

#### Parameters

Parameters	Description
<i>id</i>	Stands for the instance ID of the monitorlink group.

#### Default Value

The uplink port is not configured by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

If the MonitorLink group port role is directly configured for the port in the case that the MonitorLink group is not established, the system will automatically create the MonitorLink group.

### Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# monitor-link-group 1 uplink
Switch_config_g0/1#exit
```

### Related Command

```
monitor-link-group id
monitor-link-group id downlink
```

### 28.2.7 *monitor-link-group id downlink*

#### Syntax

To set a port to be a downlink port, run the following command:

```
monitor-link-group id downlink
```

To cancel the downlink port configuration, run the following command:

```
no monitor-link-group id
```

### Parameters

Parameters	Description
<i>id</i>	<b>Stands for the instance ID of the monitorlink group.</b>

### Default Value

The downlink port is not configured by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

If the MonitorLink group port role is directly configured for the port in the case that the MonitorLink group is not established, the system will automatically create the MonitorLink group.

### Example



```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# monitor-link-group 1 downlink
Switch_config_g0/1#exit
```

### Related Command

```
monitor-link-group id
monitor-link-group id uplink
```

## 28.3 Show

### 28.3.1 show backup-link-group id

#### Syntax

To display the information about the backuplink group, run the following command:

```
show backup-link-group id
```

#### Parameters

Parameters	Description
<i>id</i>	Stands for the instance ID of the backuplink group.

#### Default Value

None

#### Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

#### Usage Guidelines

None

#### Example

```
Switch_config# show backup-link-group 1
```

```
Active Interface          Backup          Interface      State          Vlan State
-----
GigaEthernet0/2         GigaEthernet0/4  Forward/Block          Block/Block
```

```
Share load vlan: 100-200,port[GigaEthernet0/4] vlan state: Forwarding
```

```
Preemption Mode: No Preempt
```

```
Preemption Delay: 0 seconds
```

#### Related Command

None

### 28.3.2 *show monitor-link-group id*

#### Syntax

To configure the instance ID of the monitorlink group, run the following command.

```
show monitor-link-group id
```

#### Parameters

Parameters	Description
<i>id</i>	<b>Stands for the instance ID of the monitorlink group.</b>

#### Default Value

None

#### Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

#### Usage Guidelines

None

#### Example

```
Switch_config#show monitor-link-group 1
uplink interface: GigaEthernet0/2 Forwarding
downlink interface:
GigaEthernet0/1    Forwarding
GigaEthernet0/3    Forwarding
```

#### Related Command

None

## Chapter 29 EAPS Configuration Commands

### 29.1 Global Commands

#### 29.1.1 ether-ring

To set an instance of ring and enter the node mode, run the following command:

```
ether-ring id
```

To cancel an instance of ring, run the following command:

```
no ether-ring id
```

Parameters

Parameters	Description
<i>id</i>	ID of the node

Default Value

By default, the ring node is not configured.

Command Mode

Global configuration mode

Usage Guidelines

STP should not be disabled before the configuration of node instance.

Example

```
S1_config#ether-ring 1
```

```
S1_config_ring1#
```

Related Command

None

#### 29.1.2 control-vlan

To set the control VLAN of the ring node, run the following command:

```
control-vlan vlan-id
```

Parameters

Parameters	Description
<i>vlan-id</i>	ID of the control VLAN Value range: 1-4094

Default Value

By default, the control VLAN of a node is not configured.

## Command Mode

Node configuration mode for the Ethernet ring

## Usage Guidelines

1. Any VLAN can be configured as the control VLAN of the node. If you specify the control VLAN, the system VLAN will be created consequently. The user doesn't need to create the system VLAN manually.
2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the Ethernet ring has already been started.

## Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
```

## Related Command

ether-ring  
master-node  
transit-node

### *29.1.3 master-node*

To configure an Ethernet ring as a master node, run the following command:

## **master-node**

### Parameters

None

### Default Value

By default, the node type is not configured.

## Command Mode

Node configuration mode

## Usage Guidelines

1. A node can be set to be a master node or a transit node.
2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started.

## Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
```

**Related Command**

control-vlan

transit-node

**29.1.4 transit-node**

To configure the node type to be a transit node, run the following command.

**transit-node****Parameters**

None

**Default Value**

By default, the node type is not configured.

**Command Mode**

Node configuration mode

**Usage Guidelines**

1. A node can be set to be a master node or a transit node.
2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started.

**Example**

S1\_config#ether-ring 1

S1\_config\_ring1#control-vlan 2

S1\_config\_ring1#transit-node

**Related Command**

control-vlan

master-node

**29.1.5 hello-time**

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

**hello-time** *value*

To resume the default value of the cycle, run the following command:

**no hello-time****Parameters**

Parameters	Description
------------	-------------

<i>value</i>	<b>Stands for a time value, whose unit is second. The default value is one second. The value ranges between 1 and 10 seconds.</b>
--------------	---

### Default Value

By default, the hello-time is one second.

### Command Mode

Node configuration mode for the Ethernet ring

### Usage Guidelines

1. The hello-time configuration validates only on the master node.
2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

### Example

```
S1_config#ether-ring 1
```

```
S1_config_ring1#control-vlan 2
```

```
S1_config_ring1#master-node
```

```
S1_config_ring1#hello-time 2
```

### Related Command

fail-time

### 29.1.6 fail-time

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

**fail-time** *value*

To resume the default value of the fail-time, run the following command:

**no fail-time**

### Parameters

Parameters	Description
<i>value</i>	<b>Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.</b>

### Default Value

By default, the fail-time is 3 seconds.

### Command Mode

Node configuration mode for the Ethernet ring

### Usage Guidelines

1. The fail-time configuration validates only on the master node.
2. By default, the value of the fail-time is triple of the hello-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

### Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
S1_config_ring1#hello-time 2
S1_config_ring1#fail-time 6
```

### Related Command

hello-time

### 29.1.7 pre-forward-time

To configure the time of maintaining the pre-forward state on the transit port, run the following command.

**pre-forward-time** *value*

To resume the default value of the pre-forward-time, run this command.

**no pre-forward-time**

### Parameters

Parameters	Description
<i>value</i>	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

### Default Value

By default, the pre-forward-time is 3 seconds.

### Command Mode

Node configuration mode for the Ethernet ring

### Usage Guidelines

1. The pre-forward-time configuration validates only on the transit node.
2. By default, the pre-forward-time on the transit node is triple the value of the hello-time on the master node, which avoids the network loop from being occurred after the

transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node need be adjusted.

### Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#transit-node
S1_config_ring1#pre-forward-time 8
```

### Related Command

None

## 29.2 Port Configuration Commands

### 29.2.1 ether-ring primary-port

To set a port to be the primary port of a master node, run the following command:

**ether-ring *id* primary-port**

To cancel the primary port configuration of a port, run the following command:

**no ether-ring *id* primary-port**

### Parameters

Parameters	Description
<i>id</i>	ID of the node

### Default Value

The primary port is not configured by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

### Usage Guidelines

The primary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type is the master node.

### Example

```
S1_config#interface GigaEthernet 0/1
S1_config_g0/1#ether-ring 1 primary-port
S1_config_g0/1#exit
```



## Related Command

master-node

ether-ring secondary-port

### 29.2.2 ether-ring secondary-port

To set a port to be the secondary port of a master node, run the following command:

**ether-ring *id* secondary-port**

To cancel the secondary port configuration, run the following command:

**no ether-ring *id* secondary-port**

## Parameters

Parameters	Description
<i>id</i>	ID of the node

## Default Value

The secondary port on the master node is not configured by default.

## Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

## Usage Guidelines

The primary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type is the master node.

## Example

```
S1_config#interface GigaEthernet 0/3
```

```
S1_config_g0/3#ether-ring 1 secondary-port
```

```
S1_config_g0/3#exit
```

## Related Command

master-node

ether-ring primary-port

### 29.2.3 ether-ring transit-port

To set a port to be the transit port of a transit node, run the following command:

**ether-ring *id* transit-port**

To cancel the transit port, run the following command:

**no ether-ring *id* transit-port**

## Parameters

Parameters	Description
<i>id</i>	ID of the node

## Default Value

The transit port on the transit node is not configured by default.

## Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

## Usage Guidelines

The transit port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type must be the transit node. Two transit ports can be configured on one transit node.

## Example

```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1#ether-ring 1 transit-port
S1_config_g0/1#exit S1_config#interface GigaEthernet 0/3
S1_config_g0/3#ether-ring 1 transit-port
S1_config_g0/3#exit
```

## Related Command

transit-node

**29.3 Show****29.3.1 show ether-ring**

To display the summary information about the Ethernet-ring node, run the following command:

```
show ether-ring id
```

To display the detailed information about the Ethernet-ring node, run the following command:

```
show ether-ring id detail
```

To display the information about the Ethernet-ring port, run the following command:

**show ether-ring *id* interface *intf-name***

To display all summary information about the Ethernet-ring node, run the following command:

**show ether-ring** <cr>

**Parameters**

Parameters	Description
<i>id</i>	<b>ID of the node</b>
<i>intf-name</i>	<b>Name of an interface</b>

**Default Value**

None

**Command Mode**

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

**Usage Guidelines**

None

**Example**

None

**Related Command**

None

## Chapter 30 MEAPS Configuration Commands

### 30.1 Global Commands

#### 30.1.1 mether-ring id1 domain id2

To set an instance of ring and enter the node mode, run the following command:

```
mether-ring id1 domain id2
```

To cancel an instance of ring, run the following command:

```
no mether-ring id1 domain id2
```

Parameters

Parameters	Description
<i>id1</i>	Stands for the node instance ID, which ranges from 0 to 7.
<i>id2</i>	Stands for the domain instance ID, which ranges from 0 to 3.

Default Value

By default, the ring node is not configured.

Command Mode

Global configuration mode

Usage Guidelines

If the configured domain is 0, that is **id2 is 0**, *domain id2* can be omitted.

Example

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1#
```

Related Command

None

#### 30.1.2 master-node

To configure an Ethernet ring as a master node, run the following command:

```
master-node
```

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

### Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.
2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

### Example

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1#master-node
```

```
S1_config_ring1#
```

### Related Command

transit-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

### 30.1.3 *transit-node*

To configure the node type to be a transit node, run the following command.

#### **transit-node**

### Parameters

None

### Default Value

By default, the node type is not configured.

### Command Mode

Node configuration mode

### Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.
2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

### Example

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1# transit-node
```

```
S1_config_ring1#
```

### Related Command

master-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

### *30.1.4 edge-node*

To set the node type to be an edge node, run the following command:

```
edge-node
```

### Parameters

None

### Default Value

By default, the node type is not configured.

### Command Mode

Node configuration mode

### Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.
2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

### Example

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1# edge-node
```

```
S1_config_ring1#
```

### Related Command

master-node

transit-node

assistant-node

major-ring

sub-ring

control-vlan

### ***30.1.5 assistant-node***

To set the node type to be an assistant edge node, run the following command:

**assistant-node**

#### **Parameters**

None

#### **Default Value**

By default, the node type is not configured.

#### **Command Mode**

Node configuration mode

#### **Usage Guidelines**

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.
2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

#### **Example**

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1# assistant-node
```

```
S1_config_ring1#
```

#### **Related Command**

master-node

transit-node

edge-node

major-ring

sub-ring

control-vlan

### ***30.1.6 major-ring***

To set the node ring's level to be the major ring node, run the following command:

**major-ring**

### Parameters

None

### Default Value

By default, the node ring's level is not configured.

### Command Mode

Node configuration mode

### Usage Guidelines

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring.
2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified.
3. The edge node and the assistant node cannot be set to major ring.

### Example

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1# transit-node
```

```
S1_config_ring1#major-ring
```

```
S1_config_ring1#
```

### Related Command

master-node

transit-node

edge-node

assistant-node

sub-ring

control-vlan

### *30.1.7 sub-ring*

To set the node ring's level to be the sub-ring node, run the following command:

#### **sub-ring**

### Parameters

None

### Default Value

By default, the node type is not configured.

### Command Mode



Node configuration mode

### Usage Guidelines

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring.
2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified.
3. If the edge node or the assistant node is set, they are regarded as sub-rings by default. Of course, you can set them not to be sub-rings.

### Example

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1#master-node
```

```
S1_config_ring1#sub-ring
```

```
S1_config_ring1#
```

### Related Command

master-node

transit-node

edge-node

assistant-node

major-ring

control-vlan

### 30.1.8 control-vlan

To set the control VLAN of the ring node, run the following command:

```
control-vlan vlan-id
```

### Parameters

Parameters	Description
<i>vlan-id</i>	<b>ID of the control VLAN</b> <b>Value range: 1-4094</b>

### Default Value

By default, the control VLAN of a node is not configured.

### Command Mode

Node configuration mode for the Ethernet ring

### Usage Guidelines

1. You can set any VLAN to be the control VLAN of a node and at the same time the system will create the corresponding system VLAN and another control VLAN according to the ring level.
2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the ring control VLAN can never be modified.

### Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#
```

### Related Command

master-node  
transit-node  
edge-node  
assistant-node  
major-ring  
sub-ring

### 30.1.9 single-subring-mode

To configure the edge node or assistant edge node and enter the single subring mode, run the following command.

#### **single-subring-mode**

##### Parameters

None

##### Default Value

Don't enter the single subring mode by default.

##### Command Mode

Node configuration mode for the Ethernet ring

##### Usage Guidelines

1. Configuration of single-subring-node can only be effective in the edge node and the assistant edge node.
2. As in the single ring mode the subring protocol packet channel status detection on the main ring is not run, the dual-homing networking can't appear in the Ethernet ring.

### Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#edge-node
S1_config_ring1#control-vlan 2
S1_config_ring1#single-subring-mode
```

### Related Command

None

### 30.1.10 hello-time

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

**hello-time** *value*

To resume the default value of the cycle, run the following command:

**no hello-time**

### Parameters

Parameters	Description
<i>value</i>	Stands for a time value, whose unit is second. The default value is one second. The value ranges between 3 and 10 seconds.

### Default Value

By default, the hello-time is three seconds.

### Command Mode

Node configuration mode for the Ethernet ring

### Usage Guidelines

1. The hello-time configuration validates only on the master node.
2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

### Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#hello-time 4
```

## Related Command

fail-time

### 30.1.11 fail-time

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

**fail-time** *value*

To resume the default value of the fail-time, run the following command:

**no fail-time**

## Parameters

Parameters	Description
<i>value</i>	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 9 and 30 seconds.

## Default Value

By default, the fail-time is 9 seconds.

## Command Mode

Node configuration mode for the Ethernet ring

## Usage Guidelines

1. The fail-time configuration validates only on the master node.
2. By default, the value of the fail-time is triple of the hello-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

## Example

```
S1_config#methernet-ring 1 domain 2
```

```
S1_config_ring1#master-node
```

```
S1_config_ring1#sub-ring
```

```
S1_config_ring1#control-vlan 2
```

```
S1_config_ring1#hello-time 4
```

```
S1_config_ring1#fail-time 12
```

## Related Command

hello-time

### 30.1.12 pre-forward-time

To configure the time of maintaining the pre-forward state on the transit port, run the following command.

**pre-forward-time** *value*

To resume the default value of the pre-forward-time, run this command.

**no pre-forward-time**

Parameters

Parameters	Description
<i>value</i>	<b>Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 9 and 30 seconds.</b>

Default Value

By default, the pre-forward-time is 9 seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The pre-forward-time configuration validates only on the transit node.
2. By default, the pre-forward-time on the transit node is triple the value of the hello-time on the master node, which avoids the network loop from being occurred after the transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node need be adjusted.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#transit-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#pre-forward-time 12
```

Related Command

None

## 30.2 Port Configuration Commands

### 30.2.1 mether-ring id1 domain id2 primary-port

To set a port to be the primary port of a master node, run the following command:

**mether-ring** *id1* **domain** *id2* **primary-port**

To cancel the primary port configuration of a port, run the following command:

```
no mether-ring id1 domain id2 primary-port
```

#### Parameters

Parameters	Description
<i>id1</i>	ID of the node
<i>id2</i>	ID of the domain

#### Default Value

The primary port is not configured by default.

#### Command Mode

The physical port configuration mode and the converged port configuration mode

#### Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node.

If the configured domain is 0, that *id2* is 0, domain *id2* can be omitted.

#### Example

```
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 1 domain 2 primary-port
S1_config_g0/1#exit
```

#### Related Command

master-node

mether-ring *id1* domain *id2* secondary-port

#### 30.2.2 mether-ring *id1* domain *id2* secondary-port

To set a port to be the secondary port of a master node, run the following command:

```
mether-ring id1 domain id2 secondary-port
```

To cancel the secondary port configuration, run the following command:

```
no mether-ring id1 domain id2 secondary-port
```

#### Parameters

Parameters	Description
<i>id1</i>	ID of the node
<i>id2</i>	ID of the domain

### Default Value

The secondary port on the master node is not configured by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node.

If the configured domain is 0, that `id2` is 0, domain `id2` can be omitted.

### Example

```
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 1 domain 2 secondary-port
S1_config_g0/3#exit
```

### Related Command

```
master-node
mether-ring id1 domain id2 primary-port
```

### 30.2.3 *mether-ring id1 domain id2 transit-port*

To set a port to be the transit port of a transit node, run the following command:

**mether-ring *id1* domain *id2* transit-port**

To cancel the transit port, run the following command:

**no mether-ring *id1* domain *id2* transit-port**

### Parameters

Parameters	Description
<i>id1</i>	ID of the node
<i>id2</i>	ID of the domain

### Default Value

The transit port on the transit node is not configured by default.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the transit node. Two transit ports can be configured on one transit node.

If the configured domain is 0, that `id2` is 0, domain `id2` can be omitted.

### Example

```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 1 domain 2 transit-port
S1_config_g0/1#exit
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 1 domain 2 transit-port
S1_config_g0/3#exit
```

### Related Command

`transit-node`

### 30.2.4 `mether-ring id1 domain id2 common-port`

To set a port to be a public port of an edge node (assistant edge node), run the following command:

**`mether-ring id1 domain id2 common-port`**

To cancel the public port, run the following command:

**`no mether-ring id1 domain id2 common-port`**

### Parameters

Parameters	Description
<code>id1</code>	ID of the node
<code>id2</code>	ID of the domain

### Default Value

By default, there is no configuration of the public port of an edge node.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

The public port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node.

If the configured domain is 0, that `id2` is 0, domain `id2` can be omitted.

### Example



```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 2 domain 2 common-port
S1_config_g0/1#exit
```

### Related Command

```
edge-node
assistant-node
mether-ring id1 domain id2 edge-port
```

### 30.2.5 mether-ring id1 domain id2 edge-port

To set a port to be an edge port of an edge node (assistant edge node), run the following command:

```
mether-ring id1 domain id2 edge-port
```

To cancel the edge port configuration of a port, run the following command:

```
no mether-ring id1 domain id2 edge-port
```

### Parameters

Parameters	Description
<i>id1</i>	<b>ID of the node</b>
<i>id2</i>	<b>ID of the domain</b>

### Default Value

By default, there is no configuration of the edge port of an edge node.

### Command Mode

The physical port configuration mode and the converged port configuration mode

### Usage Guidelines

The edge port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node.

If the configured domain is 0, that is **id2 is 0**, *domain id2* can be omitted.

### Example

```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 2 domain 2 edge-port
S1_config_g0/3#exit
```

## Related Command

edge-node

assistant-node

mether-ring id1 domain id2 common-port

### 30.3 Show

#### 30.3.1 show mether-ring

To display the summary information about the Ethernet-ring node, run the following command:

```
show mether-ring id1 domain id2
```

To display the detailed information about the Ethernet-ring node, run the following command:

```
show mether-ring id1 domain id2 detail
```

To display the information about the Ethernet-ring port, run the following command:

```
show mether-ring id1 domain id2 interface intf-name
```

To display all summary information about the Ethernet-ring node, run the following command:

```
show mether-ring
```

#### Parameters

Parameters	Description
<i>id1</i>	<b>ID of the node</b>
<i>id2</i>	<b>ID of the domain</b>
<i>intf-name</i>	<b>Name of an interface</b>

#### Default Value

None

#### Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

#### Usage Guidelines

If the configured domain is 0, that is **id2 is 0**, *domain id2* can be omitted.

#### Example

None

#### Related Command

None

## Chapter 31 UDLD Configuration Commands

UDLD is a L2 protocol that monitors the physical location of the cable through the devices which are connected by optical cable or twisted-pair, and detects whether the unidirectional link exists. Only when the connected device supports UDLD can the unidirectional link be detected and shut down. The unidirectional link can cause a lot of problems, including the STP topology ring. Hence, when detecting a unidirectional link, UDLD will shut down the affected interface and notify users.

UDLD works with the physical-layer protocol mechanism to judge the status if the physical link. On the physical layer, the physical signals and incorrect detections are automatically negotiated and processed, while UDLD processes other matters, such as detecting the ID of a neighbor and shutting down the incorrect connection port. If you enable automatic negotiation and UDLD, the detection at layer 1 and layer 2 can prevent physical/logical links and other protocols' problems.

### 31.1 UDLD Configuration Commands

The UDLD configuration commands are listed below:

- `udld enable`
- `udld aggressive`
- `udld port`
- `udld port aggressive`
- `udld message`
- `udld reset`
- `show udld`

#### 31.1.1 `udld enable`

##### Syntax

##### **`udld enable`**

It is used to enable UDLD globally in **normal** mode.

##### **`no udld enable`**

It is used to disable UDLD globally in **normal** mode.

##### Parameter

None

##### Default settings

None

##### Usage explanation

This command is used to enable UDLD on all interfaces in **normal** mode. In **normal** mode, if UDLD determines that the connection is gone, UDLD will set the state of the

port to **undetermined**, not to **down**. If UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

#### Command mode

Global

#### Example

The following example shows how to enable UDLD in normal mode:

```
Switch_config#udld enable
```

### 31.1.2 *udld aggressive*

#### Syntax

**udld aggressive**

It is used to enable UDLD globally in **aggressive** mode.

**no udld aggressive**

It is used to disable UDLD globally in **aggressive** mode.

#### Parameter

None

#### Default Settings

None

#### Usage explanation

This command is used to enable UDLD on all interfaces in **aggressive** mode. In **aggressive** mode, if UDLD determines that the link is gone and the link cannot be reconnected, it is thought that interrupted communication is a severe network problem and UDLD will set the state of the protocol to **down** and the port is in **down** state. If UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

#### Command mode

Global

#### Example

The following example shows how to enable UDLD in **aggressive** mode:

```
Switch_config#udld aggressive
```

### 31.1.3 *udld port*

#### Syntax

**udld port**

This command is used to enable UDLD on a port in **normal** mode.

**no udld port**

This command is used to disable UDLD on a port in **normal** mode.

#### Parameter

None

#### Default Settings

None

#### Usage explanation

This command is used to enable UDLD on the local port in normal mode. In normal mode, if UDLD determines that the connection is gone, UDLD will set the state of the port to undetermined, not to down. If UDLD maintains it is a bidirectional link, the port will be set to bidirectional.

#### Command mode

Interface configuration mode

#### Example

The following example shows how to enable UDLD in normal mode:

```
Switch_config_f0/1#udld port
```

#### *31.1.4 udld port aggressive*

##### Syntax

##### **udld port aggressive**

It is used to enable UDLD on the local interface in **aggressive** mode.

##### **no udld port aggressive**

It is used to disable UDLD on the local interface in **aggressive** mode.

#### Parameter

None

#### Default Settings

None

#### Usage explanation

This command is used to enable UDLD on the local interface in aggressive mode. In aggressive mode, if UDLD determines that the link is gone and the link cannot be reconnected, it is thought that interrupted communication is a severe network problem and UDLD will set the state of the protocol to down and the port is in down state. If UDLD maintains it is a bidirectional link, the port will be set to bidirectional.

#### Command mode

Interface configuration mode

#### Example

The following example shows how to enable UDLD in aggressive mode:

```
Switch_config_f0/1#udld port aggressive
```

### 31.1.5 *udld message*

#### Syntax

**udld message** *time*

It is used to set the message interval in **aggressive** mode.

**no udld message**

It is to resume the default message interval in **aggressive** mode.

#### Parameter

Parameters	Description
<i>time</i>	<b>Stands for the message interval in aggressive mode. It ranges between 7 and 90 seconds.</b>

#### Default Settings

15s

#### Usage explanation

This command is used to set the message interval in aggressive mode. After the message is set, you need to reset the aggressive mode and then the new message interval takes effect.

#### Command mode

Global

#### Example

The following example shows how to set the message interval to 7 seconds in aggressive mode, which takes effect after the aggressive mode is restarted.

```
Switch_config#udld message 7
```

### 31.1.6 *udld reset*

#### Syntax

**udld reset**

It is used to reset the interface which is down by UDLD to **up**.

#### Parameter

None

#### Default Settings

None

#### Usage explanation

This command is used to reset the interface which is down by UDLD to up.

### Command mode

EXEC

### Example

The following example shows how to restart the interface which is closed by UDLD.

```
Switch#udld reset
```

```
1 ports shutdown by UDLD were reset.
```

```
%%UDLD-2-UDLD_PORT_RESET: UDLD reset interface FastEthernet0/1.
```

```
%%PM-4-ERR_RECOVER: Attempting to recover from udld err-disable
state on FastEthernet0/1.
```

### 31.1.7 show udld

#### Syntax

```
show udld [interface]
```

It is used to display the information about UDLD running.

#### Parameter

Parameters	Description
<i>interface</i>	Shows the running of the UDLD module on a specific interface.

#### Default Settings

None

#### Usage explanation

This command can display the running of the UDLD module. When the interface parameter is not entered, the information about the running of all UDLDs on all interfaces will be displayed; when the interface parameter is entered, only the running of the UDLD on this interface will be displayed.

#### Command mode

EXEC / global

#### Example

The following commands will display the running states of UDLD modules on all interfaces.

```
Switch_config#show udld
```

```
Interface FastEthernet0/1
```

```
---
```

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

Interface FastEthernet0/2

---

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

Interface FastEthernet0/3

---

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

....

....

....

The following commands will display the running state of the UDLD module on the f0/1 interface.



```
Switch_config#show udld interface f0/1
```

```
Interface FastEthernet0/1
```

```
---
```

```
Port enable administrative configuration setting: Enabled
```

```
Port enable operational state: Enabled
```

```
Current bidirectional state: Unknown
```

```
Current operational state: Link down
```

```
Message interval: 15
```

```
Time out interval: 1
```

```
No neighbor cache information stored
```

```
Switch_config#
```

## Chapter 32 IGMP-Snooping Configuration Commands

The IGMP-Snooping configuration commands include:

- ip igmp-snooping
- ip igmp-snooping static
- ip igmp-snooping immediate-leave
- ip igmp-snooping mrouter
- ip igmp-snooping policy
- ip igmp-snooping dlf-drop
- ip igmp-snooping router age
- ip igmp-snooping response time
- ip igmp-snooping querier
- ip igmp-snooping forward-l3-to-mrouter
- ip igmp-snooping sensitive
- ip igmp-snooping v3-leave-check
- ip igmp-snooping forward-wrongiif-within-vlan
- ip igmp-snooping policy
- ip igmp-snooping limit
- show ip igmp-snooping
- show ip igmp-snooping timer

- show ip igmp-snooping groups
- show ip igmp-snooping statistics
- debug ip igmp-snooping packet
- debug ip igmp-snooping timer
- debug ip igmp-snooping event
- debug ip igmp-snooping error

### 32.1.1 igmp-snooping

#### Syntax

**ip igmp-snooping [vlan *vlan\_id*]**

**no ip igmp-snooping [vlan *vlan\_id*]**

To enable or disable the IGMP-snooping function, run `ip igmp-snooping [ vlan vlan_id ]`. To resume the corresponding default settings, run `no ip igmp-snooping [ vlan vlan_id ]`.

#### Parameters

Parameters	Description
<i>vlan id</i>	<b>Stands for the ID of a VLAN. Value range: 1-4094</b>

#### Default Value

The IGMP-Snooping function of the designated VLAN is shut down by default.

#### Usage Guidelines

If the `vlan` parameter is not designated, all VLANs in the system will be enabled or disabled after you run this command (IGMP-snooping supports at most 16 VLANs simultaneously).

#### Example

The following example shows how to enable the IGMP snooping function of VLAN1.

```
switch_config# ip igmp-snooping vlan 1
```

```
switch_config#
```

### 32.1.2 igmp-snooping static

#### Syntax

**ip igmp-snooping vlan *vlan\_id* static *A.B.C.D* interface *intf***

**no ip igmp-snooping vlan *vlan\_id* static *A.B.C.D* interface *intf***

#### Parameters

Parameters	Description
<i>vlan id</i>	<b>Stands for the ID of a VLAN. Value range: 1-4094</b>

<i>A.B.C.D</i>	<b>IP address of the multicast</b>
<i>intf</i>	<b>Port</b>

### Default Value

None

### Usage Guidelines

This command is used to configure the static multicast address of VLAN. Its negative form is used to cancel the static multicast address.

### Example

The following example shows how to add static multicast address 234.5.6.7 to interface FastEthernet0/5 of VLAN 2.

```
switch_config# ip igmp-snooping vlan 2 static 234.5.6.7 interface GigaEthernet0/5
switch_config#
```

### Note:

224.0.0.0-224.0.0.255 stands for unroutable multicast addresses which cannot be registered on each port.

### 32.1.3 *igmp-snooping immediate-leave*

#### Syntax

To configure the immediate-leave attribute of VLAN, run `ip igmp-snooping vlan vlan_id immediate-leave`. To resume the default value, run `no ip igmp-snooping vlan vlan_id immediate-leave`.

**ip igmp-snooping vlan *vlan\_id* immediate-leave**

**no ip igmp-snooping vlan *vlan\_id* immediate-leave**

#### Parameters

Parameters	Description
<i>vlan id</i>	<b>Stands for the ID of a VLAN. Value range: 1-4094</b>

### Default Value

The immediate-leave attribute is shut down by default.

### Usage Guidelines

None

### Example

The following example shows how to enable the immediate-leave attribute of VLAN1.

```
switch_config# ip igmp-snooping vlan 1 immediate-leave
```

```
switch_config#
```

### 32.1.4 igmp-snooping mrouter

#### Syntax

```
ip igmp-snooping vlan vlan_id mrouter interface intf
```

```
no ip igmp-snooping vlan vlan_id mrouter interface intf
```

#### Parameters

Parameters	Description
<i>vlan id</i>	Stands for the ID of a VLAN. Value range: 1-4094
<i>intf</i>	Port

#### Default Value

None

#### Usage Guidelines

The command is used to set the static routing port of VLAN. Use the no form of this command to delete the routing port.

#### Example

The following example shows how to add gigabit Ethernet port 0/5 to the static routing port of VLAN 2.

```
switch_config# ip igmp-snooping vlan 2 mrouter interface GigaEthernet0/5
```

```
switch_config#
```

### 32.1.5 igmp-snooping policy

#### Syntax

```
ip igmp-snooping policy word
```

```
no ip igmp-snooping policy
```

#### Parameters

Parameters	Description
<i>Word</i>	IP ACL name

#### Default Value

None

#### Usage Guidelines

The command is used to set the to be detected IP ACL list of igmp-snooping when adding multicast forwarding table. Use the no form of this command to cancel the detection of the list.

### Example

The following example is to detect the IP ACL whose name is 123 when adding multicast forwarding table.

```
switch_config# ip igmp-snooping policy 123
switch_config#
```

### 32.1.6 igmp-snooping dlf-drop

#### Syntax

```
ip igmp-snooping dlf-drop
no ip igmp-snooping dlf-drop
```

#### Default Value

None

#### Usage Guidelines

This command is used to set the multicast packets whose destination multicast addresses are not registered to the filtration mode. The negative form of this command is used to resume the default settings.

### Example

The following example shows how to drop the multicast packets with unregistered destination addresses in all VLANs.

```
switch_config# ip igmp-snooping dlf-drop
switch_config#
```

### 32.1.7 igmp-snooping router age

#### Syntax

```
ip igmp-snooping timer router-age time_value
no ip igmp-snooping timer router-age
```

#### Parameters

Parameters	Description
<i>time value</i>	Queries the time of the timer. Value range: 10-2147483647

#### Default Value

260 seconds

#### Usage Guidelines

This command is used to query the time of the timer of IGMP-Snooping. The negative form of this command is used to resume the default value.

### Example

The following example shows how to set the query time of the router to 300 seconds.

```
switch_config# ip igmp-snooping timer router-age 300
switch_config#
```

### 32.1.8 igmp-snooping response time

#### Syntax

To configure the maximum response time of IGMP snooping, run `ip igmp-snooping timer response-time timer_value`. To resume the default value of IGMP snooping, run `no ip igmp-snooping timer response-time timer_value`.

**ip igmp-snooping timer response-time *time\_value***

**no ip igmp-snooping timer response-time**

#### Parameters

Parameters	Description
<i>time value</i>	Queries the time of the timer. Value range: 1-2147483647

#### Default Value

15 seconds

#### Usage Guidelines

None

### Example

The following example shows how to set the query response time of IGMP snooping to 20 seconds.

```
switch_config# ip igmp-snooping timer response-time 20
switch_config#
```

### 32.1.9 igmp-snooping querier

#### Syntax

To activate the IGMP-snooping querier mechanism, or set the source IP address of the automatic query packet, run `ip igmp-snooping querier [address <ip_addr>]`. To resume the default value, run `no ip igmp-snooping querier [address <ip_addr>]`.

**ip igmp-snooping querier [address <ip\_addr>]**

**no ip igmp-snooping querier [address]**

#### Parameters

Parameters	Description
<i>ip_addr</i>	IP address of a normal unicast

### Default Value

By default, the querier function is not enabled and the source IP address is 10.0.0.200.

### Usage Guidelines

None

### Example

The following example shows how to activate IGMP Querier to serve as a multicast router if no multicast router is working.

```
switch_config# ip igmp-snooping querier
switch_config#
```

#### 32.1.10 *igmp-snooping querier querier-timer*

### Syntax

To configure the forward interval of forwarding query packets by the local querier, run the first one of the above commands. To return to the default setting, use the no form of this command.

**ip igmp-snooping querier querier-timer *time\_value***

**no ip igmp-snooping querier querier-timer**

### Parameters

Parameters	Description
<i>time_value</i>	local querier interval

### Default Value

The default interval is 200 seconds in enabling Querier.

### Usage Guidelines

None

### Example

The following command shows how to configure the query period of the local querier to 140s.

```
switch_config# ip igmp-snooping querier querier-timer 140
switch_config#
```

### 32.1.11 *igmp-snooping forward-l3-to-mrouter*

#### Syntax

To send the data packets to the multicast routing port, run `ip igmp-snooping forward-l3-to-mrouter`. To resume the default settings, use the “no” form of this command.

**ip igmp-snooping forward-l3-to-mrouter**

**no ip igmp-snooping forward-l3-to-mrouter**

#### Parameters

None

#### Default Value

If the `forward-l3-to-mrouter` command is not enabled, the data packets will not be sent to the related multicast routing port.

#### Usage Guidelines

This command is mainly to send the data packets to the IGMP JOIN port and meanwhile to the multicast routing port. Especially in case of L3 multicast cascading, the upstream L3 switches cannot receive the IGMP JOIN packets from a relative group and hence cannot learn the information about the relative group, and then the data packets will be sent to all physical ports in the L3 egress VLAN. After this command is run, the data packets will only be sent to the multicast routing port, which is registered on PIM-SM.

#### Example

The following example shows how to activate IGMP `forward-l3-to-mrouter` and make the upstream multicast data packets be sent to the multicast routing port:

```
switch_config# ip igmp-snooping forward-l3-to-mrouter
```

```
switch_config#
```

### 32.1.12 *igmp-snooping sensitive*

#### Syntax

To activate the IGMP-snooping sensitive mechanism or set the value of the sensitive parameter, run `ip igmp-snooping sensitive [value int<3-30>]`. To resume the default value, use the “no” form of this command.

**ip igmp-snooping sensitive [value int<3-30>]**

**no ip igmp-snooping sensitive [value]**

#### Parameters

Parameters	Description
<i>int</i>	<b>3-30</b>

#### Default Value

The sensitive function is disabled by default.



### Usage Guidelines

This command is mainly used to modify the router-age of the mrouter port in active state and deliver the new query packets rapidly when a port in trunk mode is shut down.

### Example

The following example shows how to activate IGMP sensitive and set the route-age of mrouter to be a converged one.

```
switch_config# ip igmp-snooping sensitive
switch_config# ip igmp-snooping sensitive value 10
```

#### *32.1.13 igmp-snooping v3-leave-check*

### Syntax

To send the special query packets after the v3-leave packet is received, run `ip igmp-snooping v3-leave-check`; to resume the default settings, run the "no" form of this command.

**ip igmp-snooping v3-leave-check**

**no ip igmp-snooping v3-leave-check**

### Default Value

v3-leave-check is disabled and the special query packet will not be sent after v3-leave packet is received.

### Usage Guidelines

None

### Example

The following example shows how to activate IGMP v3-leave-check and send the special query packet after the v3-leave packet is received.

```
switch_config# ip igmp-snooping v3-leave-check
switch_config#
```

#### *32.1.14 igmp-snooping forward-wrongiif-within-vlan*

### Syntax

To send the multicast data packets, received from the wrongiif port, to the relative physical ports in the local vlan, run `ip igmp-snooping forward-wrongiif-within-vlan`; to resume the default value, run the "no" form of this command.

**ip igmp-snooping forward-wrongiif-within-vlan**

**no ip igmp-snooping forward-wrongiif-within-vlan**

### Default Value

This command is enabled by default and the multicast packets from the wrongiif port will be sent to the relative physical ports.

## Usage Guidelines

The command takes its importance only when the L3 multicast is enabled. After this command is enabled, the multicast packets, entering from the wrongiif port, will be sent to the physical ports that are added into the group of vlan; otherwise, the multicast packets will be dropped.

## Example

The following example shows how to activate IGMP forward-wrongiif-within-vlan, and how to send the multicast packets from the wrongiif port to the relative physical ports in the local VLAN:

```
switch_config# ip igmp-snooping forward-wrongiif-within-vlan
switch_config#
```

### 32.1.15 igmp-snooping policy

#### Syntax

**ip igmp-snooping policy** *word*

**no ip igmp-snooping policy**

#### Parameters

Parameters	Description
<i>Word</i>	IP ACL name

#### Default Value

None

## Usage Guidelines

Enable IPACL function of IGMP-snooping and determine the pakcets of some multicast IP address are to be deleted or ignored.

## Configuration Mode

Port Configuration

## Example

The following example is to detect the IP ACL whose name is 123 when dealing with the packets.

```
switch_config_G0/1# ip igmp-snooping policy 123
switch_config_G0/1#
```

### 32.1.16 igmp-snooping limit

#### Syntax

**ip igmp-snooping limit** *value*

**no ip igmp-snooping limit**

## Parameters

Parameters	Description
<i>value</i>	<b>1-2048</b>

## Default Value

2048

## Usage Guidelines

The command configures the max multicast IP address number in the port of IGMP-snooping. The command will estimate whether the applied groups have reached the configuration number when IGMP-snooping generating the forward table. Otherwise, the table of the port is no longer generated.

## Configuration Mode

Port Configuration

## Example

The following example shows how to set the max number of the joining group as 1000.

```
switch_config_G0/1# ip igmp-snooping limit 1000
```

```
switch_config_G0/1#
```

**32.1.17 show ip igmp-snooping**

## Syntax

```
show ip igmp-snooping
```

## Parameters

None

## Default Value

None

## Usage Guidelines

This command is used to display the information about IGMP-snooping configuration.

## Example

The following example shows how to display each VLAN where IGMP-snooping is running.

```
switch_config# show ip igmp-snooping
```

```
Global IGMP snooping configuration:
```

```
-----
```

```
Globally enable      : Enabled
```

VLAN nodes : 1,50,100,200,400,500

Dlf-frames filtering : Disabled

Sensitive : Disabled

Querier : Enabled

Querier address : 10.0.0.200

Querier interval : 140 s

Router age : 260 s

Response time : 15 s

vlan_id	Immediate-leave	Ports	Router Ports
1	Disabled	5-10	SWITCH(querier);
50	Disabled	1-4	SWITCH(querier);
100	Disabled	NULL	SWITCH(querier);G0/1(static);
200	Disabled	NULL	SWITCH(querier);
400	Disabled	NULL	SWITCH(querier);
500	Disabled	NULL	SWITCH(querier);

switch\_config#

### 32.1.18 show ip igmp-snooping timer

#### Syntax

**show ip igmp-snooping timer**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to display the information about the IGMP-snooping clock.

#### Example

The following example shows how to display the information about the IGMP-snooping clock.

```
switch_config# show ip igmp-snooping timer
```

```
vlan 1 mrouter on port 3 : 251
```

```
switch_config#
```

### ***32.1.19 show ip igmp-snooping groups***

#### **Syntax**

**show ip igmp-snooping groups**

#### **Parameters**

None

#### **Default Value**

None

#### **Usage Guidelines**

This command is used to display the information about the multicast group of IGMP-snooping.

#### **Example**

The following example shows how to display the information about the multicast group of IGMP-snooping.

```
switch_config# show ip igmp-snooping groups
```

```
The total number of groups      2
```

Vlan Group	Type	Port(s)
-----		
1 226.1.1.1	IGMP G0/1	G0/3
1 225.1.1.16	IGMP G0/1	G0/3

```
switch_config#
```

### ***32.1.20 show ip igmp-snooping statistics***

#### **Syntax**

**show ip igmp-snooping statistics**

#### **Parameters**

None

#### **Default Value**

None

#### **Usage Guidelines**

This command is used to display the information about IGMP-snooping statistics.

#### **Example**

The following example shows how to display the information about IGMP-snooping statistics.

```
switch_config# show ip igmp-snooping statistics
vlan 1
-----
v1_packets:1
v2_packets:2
v3_packets:0
general_query_packets:1
special_query_packets:2
join_packets:0
leave_packets:0
send_query_packets:0
err_packets:0
switch_config#
```

### *32.1.21 debug ip igmp-snooping packet*

#### Syntax

**debug ip igmp-snooping packet**

**no debug ip igmp-snooping packet**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to enable or disable the igmp-snooping packet.

#### Example

The following example shows how to enable the packet debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping packet
switch #
```

### *32.1.22 debug ip igmp-snooping timer*

#### Syntax

**debug ip igmp-snooping timer**

**no debug ip igmp-snooping timer****Parameters**

None

**Default Value**

None

**Usage Guidelines**

This command is used to enable or disable the timer debugging switch of IGMP-snooping.

**Example**

The following example shows how to enable the timer debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping timer
switch #
```

**32.1.23 debug ip igmp-snooping event****Syntax****debug ip igmp-snooping event****no debug ip igmp-snooping event****Parameters**

None

**Default Value**

None

**Usage Guidelines**

This command is used to enable or disable the event debugging switch of IGMP-snooping.

**Example**

The following example shows how to enable the event debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping event
switch #
```

**32.1.24 debug ip igmp-snooping error****Syntax****debug ip igmp-snooping error****no debug ip igmp-snooping error****Parameters**

None

**Default Value**

None

**Usage Guidelines**

This command is used to enable or disable the error debugging switch of IGMP-snooping.

**Example**

The following example shows how to enable the error debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping error
switch #
```

**Chapter 33 OAM Configuration Commands**

EFM OAM of IEEE 802.3ah provides point-to-point link trouble/performance detection on the single link. However, EFM OAM cannot

be applied to EVC and so terminal-to-terminal Ethernet monitoring cannot be realized. OAM PDU cannot be forwarded to other

interfaces. Ethernet OAM regulated by IEEE 802.3ah is a relatively slow protocol. The maximum transmission rate is 10 frames per

second and the minimum transmission rate is 1 frame per second.

**33.1 OAM Configuration Commands OAM configuration commands include:**

- ethernet oam
- ethernet oam {max-rate | min-rate | mode | timeout }
- ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window
- ethernet oam link-monitor high-threshold action
- ethernet oam link-monitor negotiation-supported

**33.1.1 ethernet oam****Syntax**

To enable or disable the OAM function, run [no] ethernet oam.

**[no] ethernet oam**

**Parameters**



None

### Default Value

Ethernet OAM is disabled by default.

### Command Mode

Port configuration mode

### Usage Guidelines

None

### Example

The following commands are used to enable the OAM function on GigaEthernet 0/2 interface. Switch#

```
Switch#config
```

```
Switch_config#interface g0/2
```

```
Switch_config_g0/2#ethernet oam
```

### 33.1.2 ethernet oam {max-rate | min-rate | mode | timeout }

#### Syntax

**[no] ethernet oam {max-rate value1 | min-rate value2 | mode {active | passive} | timeout value3}**

ethernet oam max-rate value1 is used to set the fastest transmission rate of the OAM packet.

ethernet oam max-rate value2 is used to set the slowest transmission rate of the OAM packet.

ethernet oam mode {active | passive} is used to set the OAM mode.

ethernet oam timeout value3 is used to set the timeout time of the OAM connection.

#### Parameters

Parameters	Description
<i>value1</i>	<b>Fastest transmission rate, which ranges between 1 and 10. Its unit is packet/second.</b>
<i>value2</i>	<b>Slowest transmission rate, which ranges between 1 and 10. Its unit is second.</b>
<i>value3</i>	<b>Timeout time of the OAM connection, which ranges between 2 and 30 and whose unit is second</b>

### Default Value

The value of max-rate is 10.

The value of min-rate is 1.

The value of timeout is 5.

The value of mode is active.

### Command Mode

Port configuration mode

### Usage Guidelines

This command can be used to configure some optional parameters for establishing the OAM connection.

### Example

The following example shows how to set the fastest and slowest connection rates of the OAM on the GigaEthernet 0/2 interface to 5 packets/second, the connection timeout time to 10 seconds and the OAM mode to passive.

```
Switch #config
Switch_config#
Switch_config#interface g0/2
Switch_config_g0/2# ethernet oam max-rate 5
Switch_config_g0/2#ethernet oam min-rate 5
Switch_config_g0/2#ethernet oam timeout 10
Switch_config_g0/2#ethernet oam mode passive
```

### *33.1.3 ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action*

#### Syntax

To configure the trigger action after the remote fault instruction is received, run the following command. To return to the default setting, use the no form of this command.

**ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface**

no ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action

#### Parameters

None

#### Default Value

No trigger action is conducted after the remote fault instruction is received.

#### Command Mode

Port configuration mode

#### Usage Guidelines

The switch cannot generate the LINK FAULT packets and the Critical Event packets. However, these packets will be handled if they are received from the remote terminal.

router can transmit and receive the Dying Gasp packet. When the local port enters the err disabled state or is closed by the administrator or the OAM function of the local port is closed by the manager, the Dying Gasp packet will be transmitted to the remote terminal that connects the local port.

### Example

The following example shows how to enable error-disable-interface after receiving remote link fault on GigaEthernet 0/1.

```
Switch_config#interface g0/1
```

```
Switch_config_g0/1#ethernet oam remote-failure link-fault action error-disable-interface
```

### 33.1.4 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high

#### Syntax

To configure the high threshold for link monitoring, run the following command.

```
[no] ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high {none | value}
```

#### Parameters

Parameters	Description
<i>Value</i>	<p><b>Error-signal period events ranges between 1 and 65535, whose unit is signal number.</b></p> <p><b>Error-frame event ranges between 1 and 65535, whose unit is frame number.</b></p> <p><b>Error-frame event ranges between 1 and 65535, whose unit is frame number.</b></p> <p><b>Error-frame second event ranges between 1 and 900, whose unit is second.</b></p> <p><b>Error-CRC event ranges between 1 and 65535, whose unit is frame number.</b></p>

#### Default Value

The default value of each general link event is none.

#### Command Mode

Port configuration mode

#### Usage Guidelines

After the high threshold of an event and ethernet oam link-monitor high-threshold action error-disable-interface are configured, the local port enters the errdisabled state when the local port receives the high threshold of the event.

### Example

The following example shows how to configure the high threshold of the error-frame event to 10 on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold high 10
```

### 33.1.5 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low

#### Syntax

To configure the high threshold for link monitoring, run the following command.

```
[no] ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low {none | value}
```

#### Parameters

Parameters	Description
<i>Value</i>	<p>Error-signal period events ranges between 0 and 65535, whose unit is signal number.</p> <p>Error-frame event ranges between 0 and 65535, whose unit is frame number.</p> <p>Error-frame event ranges between 0 and 65535, whose unit is frame number.</p> <p>Error-frame second event ranges between 0 and 900, whose unit is second.</p> <p>Error-CRC event ranges between 0 and 65535, whose unit is frame number.</p>

#### Default Value

The default value of the error-signal period event is 1.

The default value of the error-frame event is 1.

The default value of the error-frame period event is 1.

The default value of the error-frame second event is 1.

The default value of the error-CRC event is 10.

#### Command Mode

Port configuration mode

#### Usage Guidelines

After the low threshold of an event is configured and the locally-received event exceeds the low threshold, the Event Notification OAM packet will be transmitted to notify the peer terminal.

#### Example

The following example shows how to set the low threshold of the error-frame event to 10 on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold low 10
```

### 33.1.6 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window

#### Syntax

To configure the size of the round-query window for link monitoring, run the following command.

```
ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window value
```

#### Parameters

Parameters	Description
<i>Value</i>	<p>The error-signal period event ranges between 10 and 600 on GigaEthernet and ranges between 1 and 60 on FastEthernet. The unit is 100M signals. The error-frame event ranges between 1 and 60, whose unit is second.</p> <p>The error-frame period event ranges between 100 and 6000 on GigaEthernet and ranges between 10 and 600 on FastEthernet. The unit is 14881 frames.</p> <p>Error-frame second event ranges between 10 and 900, whose unit is second.</p> <p>The error-CRC event ranges between 1 and 180, whose unit is second.</p>

#### Default Value

The default value of the error-signal period event is 10 on GigaEthernet and is 1 on FastEthernet.

The default value of the error-frame event is 1.

The default value of the error-frame period event is 100 on GigaEthernet and is 10 on FastEthernet.

The default value of the error-frame second event is 60.

The default value of the error-CRC event is 1.

#### Command Mode

Port configuration mode

#### Usage Guidelines

None

#### Example

The following example shows how to set the window of the error-frame period event to 50 on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period window 50
```

### 33.1.7 ethernet oam link-monitor high-threshold action

#### Syntax

To configure the link-monitor trigger event with the high threshold, run `ethernet oam link-monitor high-threshold action error-disable-interface`. To return to the default setting, use the `no` form of this command.

### **ethernet oam link-monitor high-threshold action error-disable-interface**

#### **[no] ethernet oam link-monitor high-threshold action**

##### Parameters

None

##### Default Value

The high-threshold trigger event does not exist by default.

##### Command Mode

Port configuration mode

##### Usage Guidelines

After the high threshold of an event and `ethernet oam link-monitor high-threshold action error-disable-interface` are configured, the local port enters the `err disabled` state when the local port receives the high threshold of the event.

##### Example

The following example shows how to set the high-threshold trigger event on interface `GigaEthernet 0/2` to `error-disable-interface`.

```
Switch_config_g0/2#ethernet oam link-monitor high-threshold action error-disable-interface
```

### ***33.1.8 ethernet oam link-monitor negotiation-supported***

#### Syntax

To configure the link-monitor negotiation, run `ethernet oam link-monitor negotiation-supported`. To return to the default setting, use the `no` form of this command.

### **ethernet oam link-monitor negotiation-supported**

#### **[no] ethernet oam link-monitor negotiation-supported**

##### Parameters

None

##### Default Value

Link-monitor negotiation is supported.

##### Command Mode

Port configuration mode

##### Usage Guidelines

Devices support link monitoring. However, if the third-party devices do not support link monitoring, devices automatically do not support link monitoring during OAM Discovery and the OAM connection can be established through the third-party devices in this case. Otherwise, when the link-monitor negotiation is not configured, devices mandatorily support the link-monitor function, but the OAM connection cannot be created if the third-party devices do not support the link-monitor function.

### Example

The following example shows that the link-monitor function is not supported on interface GigaEthernet 0/2.

```
Switch_config_g0/2#no ethernet oam link-monitor negotiation-supported
```

### 33.1.9 clear ethernet oam statistics

#### Syntax

To clear the OAM statistics information, run the following command.

```
clear ethernet oam statistics [interface intf-type intf-id]
```

#### Parameters

Parameters	Description
<i>Intf-id</i>	<b>Designates an designated interface. If an interface is not designated, the OAM statistics information on all interfaces will be deleted.</b>

#### Default Value

None

#### Command Mode

Privileged mode

#### Usage Guidelines

After this command is run, the following statistics information (type-classified packet numbering information, link-event statistics information and remote trouble statistics information) is deleted meanwhile.

### Example

The following example shows how to clear the OAM statistics information on interface GigaEthernet 0/2.

```
Switch#clear ethernet oam statistics interface g0/2
```

### 33.1.10 show ethernet oam discovery

#### Syntax

To display the OAM discovery information on all interfaces or a designated interface, including local DTE port loopback state, information about Local information TLV and Remote information TLV of OAM Information packet, run the following command.

**show ethernet oam discovery interface [intf-type intf-id]**

## Parameters

Parameters	Description
<i>Intf-id</i>	<b>Displays the Discovery information on the designated interface or on all protocol-up ports and enables the Discovery information on the OAM interface.</b>

## Default Value

None

## Usage Guidelines

None

## Example

The following example shows how to display OAM discovery information on port GigaEthernet 0/2. Switch\_config\_g0/2#show ethernet oam discovery interface g0/2

GigaEthernet0/2

Local Info TLV

-----

PDU revision: 1

Loopback status: LB\_DISABLED

OAM configurations field:

Mode : active

Unidirection : not supported

Remote loopback : supported

Link Events : supported

Variable retrieval : not supported

Mtu size: 1500

OUI: 00e00f

Remote Info TLV

-----

MAC address: 001b.0d9c.e703

PDU revision: 0

OAM configurations field:

Mode : active

Unidirection : not supported



Remote loopback : not supported

Link Events : supported

Variable retrieval: not supported

Mtu size: 1500

OUI: 00000c

### 33.1.11 show ethernet oam statistics {pdu | link-monitor | remote-failure}

#### Syntax

To display the OAM statistics information on a designated interface or all interfaces, run the following command. The OAM statistics information includes packet type statistics information, general link event statistics information and remote fault statistics information.

**show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id]**

#### Parameters

Parameters	Description
<i>Intf-id</i>	<b>Displays the statistics information on the designated interface or on all protocol-up ports and enables the statistics information on the OAM interface.</b>

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to display the packet statistics information on interface GigaEthernet 0/2.

```
Switch#show ethernet oam statistics pdu interface g0/2
```

```
GigaEthernet0/2
```

```
Counters:
```

```
-----
```

```
Information OAMPDU Tx           :59
```

```
Information OAMPDU Rx           :56
```

```
Unique Event Notification OAMPDU Tx      :0
```

```
Unique Event Notification OAMPDU Rx      :0
```

```
Duplicate Event Notification OAMPDU TX    :0
```

Duplicate Event Notification OAMPDU RX	:0
Loopback Control OAMPDU Tx	:0
Loopback Control OAMPDU Rx	:0
Variable Request OAMPDU Tx	:0
Variable Request OAMPDU Rx	:0
Variable Response OAMPDU Tx	:0
Variable Response OAMPDU Rx	:0
Organization Specific OAMPDU Tx	:0
Organization Specific OAMPDU Rx	:0
Unsupported OAMPDU Tx	:0
Unsupported OAMPDU Rx	:0
Frames Lost due to OAM	:0

### 33.1.12 show ethernet oam configuration

#### Syntax

To display the OAM configuration information on all interfaces or a designated interface, run the following command.

**show ethernet oam configuration interface [intf-type intf-id]**

#### Parameters

Parameters	Description
<i>Intf-id</i>	Displays the OAM configuration information on the designated interface or on all protocol-up ports and enables the configuration information on the OAM interface.

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to display the OAM configuration information on interface GigaEthernet 0/2.

```
Switch#show ethernet oam configuration interface g0/2
```

```
GigaEthernet0/2
```

```
General
```

-----

Admin state : enabled  
Mode : active  
PDU max rate: 10 packets/second  
PDU min rate : 1 seconds/packet  
Link timeout : 1 seconds  
High threshold action: no action

#### Remote Failure

-----

Link fault action : no action  
Dying gasp action : no action  
Critical event action : no action

#### Remote Loopback

-----

Is supported : supported  
Loopback timeout :2

#### Link Monitoring

-----

Negotiation : supported  
Status : on

#### Errored Symbol Period Event

Window : 10\*100M symbols  
Low threshold : 1 error symbol(s)  
High threshold : none

#### Errored Frame Event

Window : 1 seconds  
Low threshold : 1 error frame(s)

High threshold : none

#### Errored Frame Period Event

Window : 100\*14881 frames

Low threshold : 1 error frame(s)

High threshold : none

#### Errored Frame Seconds Summary Event

Window : 60 seconds

Low threshold : 1 error second(s)

High threshold : none

#### Errored CRC Frames Event

Window : 1 seconds

Low threshold : 10 error frame(s)

High threshold : none

### 33.1.13 show ethernet oam runtime

#### Syntax

To display the OAM running information on all interfaces or a designated interface, run the following command. The OAM running information includes the control variables in some protocols and the latest 10 times status changing records.

**show ethernet oam runtime interface [intf-type intf-id]**

#### Parameters

Parameters	Description
<i>Intf-id</i>	<b>Displays the Runtime information on the designated interface or on all protocol-up ports and enables the Runtime information on the OAM interface.</b>

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to display the OAM Runtime information on interface

GigaEthernet 0/2.

Switch#show ethernet oam runtime interface g0/2

GigaEthernet0/2

Runtime Settings:

-----

local\_pdu : NOT\_WORKING

local\_mux : FWD

local\_par : FWD

local\_link\_status : OK

local\_satisfied : FALSE

local\_stable : FALSE

pdu\_cnt :10

pdu\_timer : stopped

lost\_link\_timer : stopped

remote\_state\_valid: FALSE

remote\_stable : FALSE

remote\_evaluating : FALSE

Discovery State Machine:

-----

Last 10 state transition recorded: INACTIVE -> FAULT -> ACTIVE\_SEND\_LOCAL -> SEND\_LOCAL\_REMOTE -> SEND\_LOCAL\_REMOTE\_OK -> SEND\_ANY -> INACTIVE

## Chapter 34 Overview

### 34.1 Stipulation

### 34.2 Format Stipulation in the Command Line

Syntax	Meaning
<b>Bold</b>	Stands for the keyword in the command line, which stays unchanged and must be entered without any modification. It is presented as a bold in the command line.
<i>{italic}</i>	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the brace.
< <i>italic</i> >	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the point bracket.
[ ]	Stands for the optional parameter, which is in the square bracket.

<code>{x   y   ...}</code>	Means that you can choose one option from two or more options.
<code>[x   y   ...]</code>	Means that you can choose one option or none from two or more options.
<code>{x   y   ...}*</code>	Means that you has to choose at least one option from two or more options, or even choose all options.
<code>[x   y   ...]*</code>	Means that you can choose multiple options or none from two or more options.
<code>&amp;&lt;1-n&gt;</code>	Means that the parameter before the “&” symbol can be entered 1~n times.
<code>#</code>	Means that the line starting with the “#” symbol is an explanation line.

## Chapter 35 CFM

### 35.1 CFM Configuration Commands

#### 35.1.1 Adding the Maintenance Domain and Entering the Maintenance Domain Mode

##### Syntax

To add a maintenance domain or enter the already existent maintenance domain, run the following command.

```
ethernet cfm md mdnf {string} <char_string> [level <0-7> | creation <MHF_creation_type> | sit <sender_id_type> | ip <IP_address>]
```

##### Parameters

Parameters	Description
<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>level</i>	(optional parameter) Stands for the level of a maintenance domain. It is 0 by default.
<i>creation</i>	MIP It is none by default.
<i>sit</i>	Stands for the identifier type of the sender. It is none by default.
<i>ip</i>	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default.

##### Command Mode

Global configuration mode

##### Example

```
Switch_config#ethernet cfm md mdnf string customer level 5
```

##### Related Command

None

### 35.1.2 Deleting the Maintenance Domain

#### Syntax

To delete a designated maintenance domain, run the following command.

```
no ethernet cfm md mdnf {string} <char_string>
```

#### Parameters

Parameters	Description
<i>mdnf</i>	<b>Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.</b>

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#no ethernet cfm md mdnf string customer
```

#### Related Command

None

### 35.1.3 Browsing the Maintenance Domain

#### Syntax

To browse all the maintenance domains or the designated maintenance domains of the local device, run the following command.

```
show ethernet cfm md [mdnf {string} <char_string>]
```

#### Parameters

Parameters	Description
<i>mdnf</i>	<b>Stands for the format of the name of a to-be-browsed designated maintenance domain. At present only the char-string format is supported. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.</b>

#### Command Mode

EXEC, global, interface, maintenance domain

#### Example

```
Switch_config#show ethernet cfm md mdnf string customer
```

## Related Command

None

### 35.1.4 Adding a maintenance association

#### Syntax

To add a maintenance association, run the following command.

```
ma manf {string} <char_string> ci {100ms | 1s | 10s | 1min | 10min} meps <mepids> [vlan
<1-4094> | creation <MHF_creation_type> | sit <sender_id_type> | ip <IP_address>]
```

#### Parameters

Parameters	Description
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported. It is the name of the maintenance association. It is in character string mode.
<i>ci</i>	Stands for the transmission interval of CCM. The shortest transmission interval which is supported presently is 100ms.
<i>meps</i>	Stands for the MEPID of all MEPs in the local maintenance domain.
<i>vlan</i>	Stands for the identifier of the VLAN where the maintenance association is located. It is 1 by default.
<i>creation</i>	MIP It is none by default.
<i>sit</i>	Stands for the identifier type of the sender. It is none by default.
<i>ip</i>	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default.

## Command Mode

Maintenance domain mode

#### Example

```
Switch_config_cfm#ma manf string customer1 ci 1s meps 1-2,2009 vlan 10
```

## Related Command

None

### 35.1.5 Deleting the Maintenance Association

#### Syntax

To delete a designated maintenance association, run the following command.

```
no ma manf {string} <char_string>
```

#### Parameters

Parameters	Description
------------	-------------



<i>manf</i>	<p>Stands for the format of the name of the maintenance association. At present only the char-string format is supported.</p> <p>&lt;char_string&gt; is the name of the maintenance association. It is in character string mode.</p>
-------------	--

### Command Mode

Maintenance domain mode

### Example

```
Switch_config_cfm#no ma manf string man customer
```

### Related Command

None

## 35.1.6 Browsing the Maintenance Association

### Syntax

To browse all or designated maintenance associations in a designated maintenance domain on the local device, run the following command.

```
show ethernet cfm ma mdnf {string} <char_string> [manf {string} <char_string>]
```

### Parameters

Parameters	Description
<i>mdnf</i>	<p>Stands for the format of the name of the maintenance domain where the to-be-browsed maintenance association is located. At present only the char-string format is supported. &lt;char_string&gt; is the name of the maintenance domain where the to-be-browsed maintenance association is located. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.</p>
<i>manf</i>	<p>Stands for the format of the name of a to-be-browsed maintenance association.</p> <p>At present only the char-string format is supported. &lt;char_string&gt; is the name of a to-be-browsed maintenance association. It is in character string mode.</p>

### Command Mode

EXEC, global, interface, maintenance domain

### Example

```
Switch_config#show ethernet cfm ma mdnf string customer manf string customer1
```

### Related Command

None

### 35.1.7 Adding MIP

#### Syntax

To add an MIP of a specific level, which belongs to a designated VLAN, on a specific interface, run the following command.

```
ethernet cfm mip add level <0-7> [vlan <1-4094>]
```

#### Parameters

Parameters	Description
<i>level</i>	<b>Stands for the level of a maintenance domain.</b>
<i>vlan</i>	<b>Stands for the identifier of the VLAN where the maintenance association is located. It is 1 by default.</b>

#### Command Mode

Physical interface configuration mode

#### Example

```
Switch_config_g0/1#ethernet cfm mip add level 1 vlan 10
```

#### Related Command

None

### 35.1.8 Deleting MIP

#### Syntax

To delete a designated MIP, run the following command.

```
ethernet cfm mip del vlan <1-4094>
```

#### Parameters

Parameters	Description
<i>vlan</i>	<b>Stands for the identifier of the VLAN where MIP is located.</b>

#### Command Mode

Interface configuration mode

#### Example

```
Switch_config_g0/1#ethernet cfm mip del vlan 10
```

#### Related Command

None

### 35.1.9 Browsing MIP

【Method 1】

## Syntax

To browse all MIPs of a designated interface in the local device or MIPs in a specific VLAN, run the following command.

```
show ethernet cfm mip vlan <1-4094> interface <interface_name>
```

```
show ethernet cfm mip interface <interface_name>
```

## Parameters

Parameters	Description
<i>interface</i>	<b>Stands for a to-be-browsed interface.</b>
<i>vlan</i>	<b>Stands for the identifier of a to-be-browsed VLAN.</b>

## Command Mode

EXEC, global, interface, maintenance domain

## Example

```
Switch_config#show ethernet cfm mip vlan 1 interface g0/1
```

## Related Command

None

【Method 2】

## Syntax

To browse all MIPs on the current interface of the local device, run the following command.

```
ethernet cfm mip display
```

## Parameters

None

## Command Mode

Physical interface mode

## Example

```
Switch_config_g0/1#ethernet cfm mip display
```

## Related Command

None

### 35.1.10 Adding MEP

## Syntax

To add an MEP, which belongs to a designated maintenance association, on a specific interface, run the following command.

```

ethernet cfm mep add mdnf {string} <char_string> manf {string} <char_string> mepid
<1-8191> [direction {up | down} | ip <ip_address> | lap {all | mac | rCCM | eCCM | xcon |
none}]

```

### Parameters

Parameters	Description
<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. <char_string> is the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported. <char_string> is the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>mepid</i>	Stands for the MEPID of the to-be-added MEP.
<i>direction</i>	(optional parameter) Stands for the direction of the to-be-added MEP. It is down by default.
<i>ip</i>	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default.
<i>lap</i>	Stands for the lowest priority of trouble report. It is all by default.

### Command Mode

Physical interface configuration mode

### Example

```

Switch_config_g0/1#ethernet cfm mep add mdnf string customer manf string customer1
mepid

```

```

2009 direction up lap all

```

### Related Command

None

### 35.1.11 Deleting MEP

#### Syntax

To delete a designated MEP, run the following command.

```

ethernet cfm mep del mdnf {string} <char_string> manf {string} <char_string> mepid
<1-8191>

```

### Parameters

Parameters	Description
------------	-------------

<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. <char_string> is the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported. <char_string> is the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>mepid</i>	Stands for the MEPID of the to-be-added MEP.

## Command Mode

Physical interface configuration mode

## Example

```
Switch_config_g0/1#ethernet cfm mep del mdnf string customer manf string customer1
mepid 2009
```

## Related Command

None

### 35.1.12 Browsing MEP

【Method 1】

## Syntax

To browse the detailed or brief information about all MEPs in the designated maintenance domain of the local device, or that about a specific MEP, run the following command.

```
show ethernet cfm mep mdnf {string} <char_string> manf {string} <char_string> [mepid
<1-8191>] [view {detail | brief}]
```

## Parameters

Parameters	Description
<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. <char_string> is the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
<i>man</i>	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>mepid</i>	Stands for the MEPID of the to-be-browsed MEP.

<i>view</i>	<b>Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default.</b>
-------------	---

### Command Mode

EXEC, global, interface, maintenance domain

### Example

```
Switch_config#show ethernet cfm mep mdnf string x manf string x view brief
```

### Related Command

None

【Method 2】

### Syntax

To browse all MEPs on the current interface of the local device, run the following command.

**ethernet cfm mep display**

### Parameters

None

### Command Mode

Physical interface mode

### Example

```
Switch_config_g0/1#ethernet cfm mep display
```

### Related Command

None

## 35.3 CFM Maintenance Commands

### 35.2.1 loopback

### Syntax

To use a designated MEP at the local terminal to conduct loopback towards another designated MEP at the remote terminal, run the following command.

**ethernet cfm loopback mdnf** *{string}* *<char\_string>* **manf** *{string}* *<char\_string>* **mepid** *<1-8191>*

mac *<AA:BB:CC:DD:EE:FF>* [**number** *<1-64>*]

### Parameters

Parameters	Description
<i>mdnf</i>	<b>Stands for the format of the name of the maintenance domain. At present only the char-string format is</b>

	supported. <char_string> is the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported. <char_string> is the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>mepid</i>	Stands for the MEPID of the local MEP.
<i>mac</i>	Stands for the MAC address of the remote MEP.
<i>number</i>	(optional parameter) Stands for the times of conducting loopback. It is 3 by default.

## Command Mode

EXEC

## Example

```
Switch#ethernet cfm loopback mdnf string x manf string x mepid 1 mac 00:15:E9:43:AD:E3
number 3
```

## Related Command

None

## 35.2.2 linktrace

### Syntax

To use a designated local MEP to conduct linktrace towards a designated remote MEP, run the following command.

```
ethernet cfm linktrace mdnf {string} <char_string> manf {string} <char_string> mepid <1-8191>
```

```
mac <AA:BB:CC:DD:EE:FF> [ttl {1-255} | fdb-only {yes}]
```

### Parameters

Parameters	Description
<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. <char_string> is the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
<i>mepid</i>	Stands for the MEPID of the local MEP.
<i>mac</i>	Stands for the MAC address of the remote MEP.

<i>ttl</i>	(optional parameter) Stands for the ttl value. It is 64 by default.
<i>fdb-only</i>	(optional parameter) Means to use the forward database or not. It is yes by default.

## Command Mode

EXEC

## Example

```
Switch#ethernet cfm linktrace mdnf s x manf string x mepid 1 mac 00:15:E9:43:AD:E3 ttl 64
```

## Related Command

None

### 35.2.3 Deleting the Linktrace Result Table

## Syntax

To delete the linktrace result table of a designated MEP, run the following command.

```
clear ethernet cfm linktrace mdnf {string} <char_string> manf {string} <char_string>
[mepid <1-8191>]
```

## Parameters

Parameters	Description
<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. <char_string> is the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported. <char_string> is the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>mepid</i>	Stands for the MEPID of the local MEP.

## Command Mode

EXEC

## Example

```
Switch#clear ethernet cfm linktrace mdnf string x manf string x mepid 1
```

## Related Command

None



### 35.2.4 Setting the Size of the Linktrace Result Table

#### Syntax

To set the size of the linktrace result table (that is, the number of linktraces which can be conducted concurrently), run the following command.

```
ethernet cfm linktrace table-size <1-16>
```

#### Parameters

Parameters	Description
<i>table-size</i>	<b>Stands for the size of the linktrace result table.</b>

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#ethernet cfm linktrace table-size 1
```

#### Related Command

None

### 35.2.5 Setting the Number of Entries in the Linktrace Result Table

#### Syntax

To set the maximum number of entries that are received each time by the linktrace result table, run the following command.

```
ethernet cfm linktrace entry-number <2-4095>
```

#### Parameters

Parameters	Description
<i>entry-number</i>	<b>Stands for the number of the entries in the linktrace result table.</b>

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#ethernet cfm linktrace entry-number 2009
```

#### Related Command

None

### 35.2.6 Setting the aging time of the linktrace result table

#### Syntax

To set the maximum number of entries that are received each time by the linktrace result table(Unit:min), run the following command.

```
ethernet cfm linktrace hold-time <1-29>
```

#### Parameters

Parameters	Description
<i>hold-time</i>	<b>Stands for the aging time of the linktrace result table. Unit: minute</b>

#### Command Mode

Global configuration mode

#### Example

```
Switch_config#ethernet cfm linktrace hold-time 10
```

#### Related Command

None

### 35.2.7 Deleting the MEP Statistics Data

#### Syntax

To delete the statistics data of a designated MEP, run the following command.

```
ethernet cfm mep clear mdnf {string} <char_string> manf {string} <char_string> mepid <1-8191>
```

#### Parameters

Parameters	Description
<i>mdnf</i>	<b>Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. &lt;char_string&gt; is the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.</b>
<i>manf</i>	<b>Stands for the format of the name of the maintenance association. At present only the char-string format is supported. &lt;char_string&gt; is the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.</b>
<i>mepid</i>	<b>Stands for the MEPID of a designated MEP.</b>

#### Command Mode

Physical interface mode

#### Example

```
Switch_config_g0/1#ethernet cfm mep clear mdnf string x manf string x mepid 1
```

## Related Command

None

### **35.4 CFM Control Commands**

#### *35.4.1 CFM Stack Control Command*

##### Syntax

To enable or disable the whole CFM protocol stack, run the following command.

```
ethernet cfm {enable | disable}
```

##### Parameters

None

##### Command Mode

Global configuration mode

##### Example

```
Switch_config#ethernet cfm enable
```

## Related Command

None

#### *35.4.2 CFM Interface Control Command*

##### Syntax

To enable or disable the CFM function of the current interface, run the following command.

```
ethernet cfm {enable | disable}
```

##### Parameters

None

##### Command Mode

Physical interface mode

##### Example

```
Switch_config_g0/1#ethernet cfm enable
```

## Related Command

None

#### *35.4.3 MIP Control Command*

##### Syntax

To enable or disable the MIP of a designated VLAN on the current interface, run the following command.

```
ethernet cfm mip {enable | disable} vlan <1-4094>
```

---

**Parameters**

None

**Command Mode**

Physical interface mode

**Example**

```
Switch_config_g0/1#ethernet cfm mip enable vlan 1
```

**Related Command**

None

## **35.4 CFM Query Commands**

### *35.4.1 Browsing the CFM Protocol Stack*

**Syntax**

To browse the CFM protocol stack, run the following command.

```
show ethernet cfm stack
```

**Parameters**

None

**Command Mode**

Non-user mode

**Example**

```
Switch_config#show ethernet cfm stack
```

**Related Command**

None

### *35.4.2 Browsing the CFM Interface*

**Syntax**

To check the relevant information of CFM interface, run the following command.

```
show ethernet cfm interface [<interface_name>]
```

**Parameters**

None

**Command Mode**

Non-user mode

**Example**

```
Switch_config#show ethernet cfm interface g0/1
```

## Related Command

None

### 35.4.3 Browsing the Locally Stored Information about the Remote MEP

#### Syntax

To browse the detailed or brief information about all remote MEPs, which together with a designated local MEP belong to the same maintenance association, or about a designated remote MEP, run the following command.

```
show ethernet cfm rmep mdnf {string} mdn <char_string> manf {string} man
<char_string> [mepid <1-8191>] [rmepid <1-8191>] [view {detail | brief}]
```

#### Parameters

Parameters	Description
<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
<i>mdn</i>	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
<i>man</i>	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>mepid</i>	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association.
<i>rmepid</i>	Stands for the MEPID of the to-be-browsed remote MEP
<i>view</i>	Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default.

#### Command Mode

Non-user mode

#### Example

```
Switch_config#show ethernet cfm rmep mdnf string mdn x manf string man x mepid 1
rmepid 2 view brief
```

#### Related Command

None

### 35.4.4 Browsing the LinkTrace Result Table

#### Syntax

To browse the linktrace result table which is carried out by a specified TID of a specific MEP, run the following command.

```
show ethernet cfm linktrace mdnf {string} mdn <char_string> manf {string} man
<char_string> mepid <1-8191> tid <0-4294967295>
```

### Parameters

Parameters	Description
<i>mdnf</i>	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
<i>mdn</i>	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
<i>man</i>	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>manf</i>	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
<i>man</i>	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
<i>mepid</i>	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association.
<i>tid</i>	Stands for the TID that is returned during linktrace.

### Command Mode

Non-user mode

### Example

```
Switch_config#show ethernet cfm linktrace mdnf string mdn x manf string man x mepid 1 tid
19830719
```

```
**** [RESULT FOR READING LINKTRACE REPLY] ****

=====
ID :0x12E97BF (19830719) 【Event ID of the presently running LT】
TTL :0x0000004(4) 【TTL value of the presently running LT】
TOTAL LTRs:1 【LTRs returned by the remote terminal of the result table】
MAX LTRs:100 【receiving at most 100 LTRs】
NEXT ORDER:2 【The next expected LTR order ID】

【The total information of one Linktrace is shown above】
===== LTRs =====

order:1 【Order ID of this LTR】
TTL:3 【TTL value in the responded LTRs】
FwdYes:NO 【Whether the local node forwards LTM】
TerminalMEP:NO 【Whether the local node is the terminal MEP】
Last Egress ID:0 - 00:E0:0F:DC:02:11 【MAC of the previous hop】
Next Egress ID:0 - 00:00:00:00:00:00 【MAC of the next hop, and if the result is 0 it means there is no
next hop】

Relay Action:(1)HIT 【Field of the Relay action: HIT means just hitting successively】
Ingress Action:OK(1) 【state of the ingress port: OK】
Ingress MAC Address:00:E0:0F:81:11:1C 【MAC of the ingress port】
Ingress Port ID format:MAC-ADDRESS(3) 【ID format of the ingress port: MAC format】
Ingress Port ID (hex):00 E0 0F 81 11 1C 【Identifier of the ingress port: 00 E0 0F 81 11 1C】
```

### Related Command

None

### *35.4.5 Browsing the whole running status of CFM*

#### Syntax

To browse the whole running status of CFM, run the following command.

**show ethernet cfm running-info**

#### Parameters

None

#### Command Mode

All modes except the user mode

#### Example

```
Switch_config#show ethernet cfm running-info
```

### Related Command

None

## Chapter 36 DHCP-relay Snooping Configuration Commands

The DHCP-relay snooping configuration commands include:

- ip dhcp-relay snooping
- ip dhcp-relay snooping vlan
- ip dhcp-relay snooping database-agent
- ip dhcp-relay snooping db-file
- ip verify source vlan
- ip arp inspection vlan
- ip source binding
- arp inspection trust
- dhcp snooping trust
- ip-source trust
- show ip dhcp-relay snooping
- show ip dhcp-relay snooping binding
- debug ip dhcp-relay snooping
- debug ip dhcp-relay event
- debug ip dhcp-relay binding

### 36.1.1 *ip dhcp-relay snooping*

#### Syntax

To enable or disable the DHCP-relay snooping function in a VLAN, run `ip dhcp-relay snooping`. To resume the corresponding default settings, run `no dhcp-relay snooping`.

**ip dhcp-relay snooping**

**no ip dhcp-relay snooping**

#### Parameters

None

#### Default Value

The dhcp-relay snooping function is disabled by default.

#### Usage Guidelines

None

#### Example

The following example shows how to enable the DHCP snooping function:

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#
```

### 36.1.2 *ip dhcp-relay snooping vlan*

#### Syntax

**ip dhcp-relay snooping vlan *vlan\_id***

**no ip dhcp-relay snooping vlan *vlan\_id***

#### Parameters

Parameters	Description
<i>vlan_id</i>	Stands for the ID of a VLAN. Value range: 1-4094

#### Default Value

None

#### Usage Guidelines

This command is used to configure the VLAN of DHCP snooping.

#### Example

The following example shows how to enable snooping detection for DHCP packets on VLAN 2.

```
Switch_config#ip dhcp-relay snooping vlan 2
```



Switch\_config#

### 36.1.3 ip dhcp-relay snooping vlan vlan\_id max-client

#### Syntax

**ip dhcp-relay snooping vlan** *vlan\_id* **max-client** *number*

**no ip dhcp-relay snooping vlan** *vlan\_id* **max-client**

#### Parameters

Parameters	Description
<i>vlan_id</i>	<b>Stands for the ID of a VLAN. Value range: 1-4094</b>
<i>number</i>	<b>Allowable maximum number of users: 0-65535</b>

#### Default Value

The default maximum number of users is 65535.

#### Usage Guidelines

You can use this command to set the maximum users in a VLNA of DHCP snooping. During this settings, the principle “first come and first be distributed” will be followed. When the number of users in the VLAN reaches the maximum value, new clients are then forbidden to distribute.

#### Example

The following example shows that snooping check will be conducted towards the DHCP packets in VLAN2 and the allowable maximum number of users is 3.

```
Switch_config#ip dhcp-relay snooping vlan 2 max-client 3
```

```
Switch_config#
```

### 36.1.4 ip dhcp-relay snooping database-agent

#### Syntax

To bind DHCP snooping to standby TFTP server, run **ip dhcp-relay snooping database-agent** *A.B.C.D*.

**ip dhcp-relay snooping database-agent** *A.B.C.D*

**no ip dhcp-relay snooping database-agent** *A.B.C.D*

#### Parameters

Parameters	Description
<i>A.B.C.D</i>	<b>Means the IP address of the TFTP server.</b>

#### Default Value

There is no standby servers by default.

## Usage Guidelines

If the address of the TFTP server is not configured, the binding backup is not conducted.

## Example

The following example shows how to set the address of a server of backing up DHCP snooping binding to 192.168.1.1.

```
Switch_config#ip dhcp-relay snooping database-agent 192.168.1.1
Switch_config#
```

### 36.1.5 ip dhcp-relay snooping db-file

#### Syntax

**ip dhcp-relay snooping db-file** *name* [*timestamp*]

**no ip dhcp-relay snooping db-file** [*timestamp*]

#### Parameters

Parameters	Description
<i>Name</i>	File name which is saved during DHCP snooping binding backup.
<i>timestamp</i>	Timestamp which is the file name of the binding backup.

#### Default Value

There is no file.

#### Usage Guidelines

If the file name is not configured, the binding backup is not conducted.

## Example

The following example shows how to set the file name of binding backup to dhcp\_binding.txt.

```
Switch_config#ip dhcp-relay snooping db-file dhcp_binding.txt
Switch_config#
```

### 36.1.6 ip dhcp-relay snooping write-time

#### Syntax

**ip dhcp-relay snooping write-time** *num*

**no ip dhcp-relay snooping write-time**

#### Parameters

Parameters	Description
<i>Num</i>	Stands for the interval of backing up the DHCP snooping binding (2-1440).

### Default Value

The default value of the interval is 30 minutes.

### Usage Guidelines

The binding update will be checked during interval configuration. If the binding is updated, the binding information need be backed up.

### Example

The following example shows how to set the interval of backing up the binding to 60 minutes.

```
Switch_config#ip dhcp-relay snooping write-time 60
Switch_config#
```

### *36.1.7 ip dhcp-relay snooping write-immediately*

#### Syntax

```
ip dhcp-relay snooping write-immediately
no ip dhcp-relay snooping write-immediately
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

If there is entry update, it will write into the entry database immediately. It is recommended that the function is not enabled when there is plenty of entries. Otherwise, the performance may be affected.

### Example

The following example shows how to backup the binding entry after the configuration is updated.

```
Switch_config#ip dhcp-relay snooping write-immediately
Switch_config#
```

### *36.1.8 ip dhcp-relay snooping log*

#### Syntax

```
ip dhcp-relay snooping log
no ip dhcp-relay snooping log
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

After the log function is enabled, the syslog will report if there is packets of dhcp server on non-trust port, which indicates that there is illegal dhcp server on the port reporting syslog.

#### Example

The following example shows how to enable the DHCP-relay snooping function:

```
Switch_config#ip dhcp-relay snooping log
```

```
Switch_config#
```

### *36.1.9 ip dhcp-relay snooping rapid-refresh-bind*

#### Syntax

To enable rapid update of DHCP snooping, run `ip dhcp-relay snooping rapid-refresh-bind`.

```
ip dhcp-relay snooping rapid-refresh-bind
```

```
no ip dhcp-relay snooping rapid-refresh-bind
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

After this function is enabled, the DHCP attack of fake MAC will be closed; when the client is allowed to change the access port, the IP address can be directly acquired without waiting for the expiration of the IP lease.

If the client change the access port after the function is disabled, the device enabling snooping will take it as dhcp packet attack of fake mac and the dhcp packet will be dropped.

#### Example

None

### *36.1.10 dhcp-relay snooping information option*

#### Syntax

```
ip dhcp-relay snooping information option [ format snmp-ifindex | manual | cm-type | hn-type [host] ]
```

```
no ip dhcp-relay snooping information option [ format snmp-ifindex | manual | cm-type | hn-type [host] ]
```

## Parameters

Parameters	Description
<i>format snmp-ifindex</i>	Fills in option 82 in SNMP ifindex mode (optional).
<i>format manual</i>	Uses the manual configuration to fill in option82 (optional).
<i>format cm-type</i>	Uses cm-type to fill in option82 (optional)
<i>format hn-type [host]</i>	Uses the Cisco format to enter option82 (optional). Host means the configuration device is the master switch.

## Default Value

Option 82 will not be added to or removed from the report by default.

## Usage Guidelines

This command is used to set whether DHCP option82 can be handled when a switch is conducting DHCP snooping. If *format snmp-ifindex* is specified, you should use SNMP ifindex to fill in option82; if *format manual* is specified, you should use the character string, which is set by the command “*dhcp snooping information circuit-id string*” on all ports, to fill in the circuit-id option of option82; in other cases, fill in option82 according to the rules of RFC3046.

## Example

The following example shows how to fill in option 82 in SNMP ifindex mode.

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping information option format snmp-ifindex
```

The following example shows how to fill in option 82 in manual mode.

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping vlan [WORD] //[WORD] stands for the vlan name for start up the snooping function.
```

```
Switch_config# ip dhcp-relay snooping information option format manual
```

### 36.1.11 ip verify source vlan

## Syntax

```
ip verify source vlan vlanid
```

```
no ip verify source vlan vlanid
```

## Parameters

Parameters	Description
<i>vlan id</i>	Stands for the ID of a VLAN. Value range: 1-4094

### Default Value

None

### Usage Guidelines

This command is used to configure a VLAN for monitoring the source IP address. The “no” form of this command is used to cancel this VLAN. If the source IP address and source MAC address of the IP packet is not the client’s legal address, which is distributed by the DHCP server and listened by DHCP snooping, the vlan in which IP source address will take the kind of packets as illegal ones and drop them.

### Example

The following example shows how to conduct source IP address monitoring to the packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
Switch_config#ip verify source vlan 2
```

```
Switch_config#
```

### 36.1.12 ip arp inspection vlan

#### Syntax

```
ip arp inspection vlan vlanid
```

```
no ip arp inspection vlan vlanid
```

#### Parameters

Parameters	Description
<i>vlanid</i>	Stands for the ID of a VLAN. Value range: 1-4094

### Default Value

None

### Usage Guidelines

This command is used to configure a VLAN for monitoring the source address of the ARP packet. The “no” form of this command is used to cancel this VLAN. In the VLAN where monitoring the source address of the ARP packets is enabled, if SIP and SMAC of a ARP packet, which correspond to the IP address and MAC address of the client that the DHCP server distributes to the client, are unsuitable, the ARP packet will be dropped.

### Example

The following example shows how to conduct source address monitoring to the ARP packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
Switch_config#ip arp inspection vlan 2
```

```
Switch_config#
```

### 36.1.13 ip source binding

#### Syntax

To add MAC-to-IP binding to an interface, run `ip source binding xx-xx-xx-xx-xx-xx A.B.C.D interface name vlan vlan-id`

**ip source binding** `xx:xx:xx:xx:xx:xx A.B.C.D interface name vlan vlan-id`

**no ip source binding** `xx:xx:xx:xx:xx:xx A.B.C.D vlan vlan-id`

#### Parameters

Parameters	Description
<code>xx:xx:xx:xx:xx:xx</code>	<b>MAC地址</b>
<code>A.B.C.D</code>	<b>IP address</b>
<code>Name</code>	<b>Means a name of an interface.</b>
<code>vlan-id</code>	<b>Stands for VLAN ID.</b>

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to bind MAC address 08:00:3e:00:00:01 to IP address 192.168.1.2 on interface GigaEthernet0/1.

```
Switch_config#ip source binding 08:00:3e:00:00:01 192.168.1.2 interface GigaEthernet0/1
Switch_config#
```

### 36.1.14 arp inspection trust

#### Syntax

**arp inspection trust**

**no arp inspection trust**

#### Parameters

None

#### Default Value

The default interface is a distrusted one.

#### Usage Guidelines

The ARP monitoring is not conducted to the ARP-trusted interface. The “no” form of this command is used to configure the default value of this interface.

### Example

The following example shows how to set interface GigaEthernet 0/1 to an ARP-trusted interface.

```
Switch_config_g0/1#arp inspection trust
```

#### *36.1.15 dhcp snooping trust*

### Syntax

**dhcp snooping trust**

**no dhcp snooping trust**

### Parameters

None

### Default Value

The default interface is a distrusted one.

### Usage Guidelines

DHCP snooping is not conducted to the DHCP-trusted interface. The “no” form of this command is used to resume the default value of this interface.

### Example

The following example shows how to set interface GigaEthernet 0/1 to an DHCP-trusted interface.

```
Switch_config_g0/1#dhcp snooping trust
```

#### *36.1.16 dhcp snooping deny*

### Syntax

**dhcp snooping deny**

**no dhcp snooping deny**

### Parameters

None

### Default Value

Snooping monitoring is allowed on the default interface.

### Usage Guidelines

After this command is configured, DHCP snooping trust, IP-sourcetrust and ARP inspection trust are automatically enabled. The “no” form of this command is used to configure the default value of this interface.



## Example

The following example shows how to disable DHCP snooping on interface GigaEthernet0/1.

```
Switch_config_g0/1#dhcp snooping deny
```

### 36.1.17 dhcp snooping information circuit-id

#### Syntax

```
dhcp snooping information circuit-id {string STRING | hex xx-xx-xx-xx-xx-xx}
```

#### Parameters

Parameters	Description
<i>string STRING</i>	Stands for the character string carried by the sub-option of option82 circuit-id.
<i>hex xx-xx-xx-xx-xx-xx</i>	Stands for the hexadecimal character string carried by the sub-option of option82 circuit-id.

#### Default Value

None

#### Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set optio82 need be opened. See the command, ip dhcp-relay snooping information option format manual)

#### Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3.

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3#dhcp snooping information circuit-id string group1
```

### 36.1.18 dhcp snooping information remote-id string

#### Syntax

```
dhcp snooping information remote-id {string STRING | hex xx-xx-xx-xx-xx-xx}
```

#### Parameters

Parameters	Description
<i>string STRING</i>	Stands for the character string carried by option82 remote-id.

<i>hex xx-xx-xx-xx-xx-xx</i>	<b>Stands for the hexadecimal character string carried by the sub-option of option82 remote-id.</b>
------------------------------	---

### Default Value

None

### Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set optio82 need be opened. See the command, ip dhcp-relay snooping information option format manual)

### Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3.

```
Switch_config# ip dhcp-relay snooping
Switch_config# ip dhcp-relay snooping vlan 1
Switch_config#ip dhcp-relay snooping information option format manual
Switch_config#interface g0/3
Switch_config_g0/3# dhcp snooping information remote-id string group1
```

### 36.1.19 dhcp snooping information vendor-specific

#### Syntax

**dhcp snooping information vendor-specific** {string *STRING* | hex *xx-xx-xx-xx-xx-xx*}

#### Parameters

Parameters	Description
<i>string STRING</i>	<b>Stands for the character string carried by option82 vendor-specific.</b>
<i>hex xx-xx-xx-xx-xx-xx</i>	<b>Stands for the hexadecimal character string carried by the sub-option of option82 vendor-specific.</b>

### Default Value

None

### Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set optio82 need be opened. See the command, ip dhcp-relay snooping information option format manual)

### Example

The following example shows how to use the hexadecimal 00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34 to set option82 option vendor-specific (suboption 9)

```
Switch_config# ip dhcp-relay snooping
```

```
Switch_config# ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3# dhcp snooping information vendor-specific hex 00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
```

### 36.1.20 dhcp snooping information append

#### Syntax

**dhcp snooping information append**

**dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* | hostname | vlanip }**

**dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* | hostname | vlanip }**

**no dhcp snooping information append**

**no dhcp snooping information append first-subop9-param**

**no dhcp snooping information append second-subop9-param**

#### Parameters

Parameters	Description
<i>first-subop9-param hex [xx-xx-xx-xx-xx-xx]</i>	<b>Stands for the Hex system of the first parameter carried by option82 vendor-specific (suboption9).</b>
<i>second-subop9-param hex [xx-xx-xx-xx-xx-xx]</i>	<b>Stands for the Hex system of the second parameter carried by option82 vendor-specific (suboption9).</b>
<i>hostname</i>	<b>Option82 vendor-specific (suboption9) Stands for the parameter of the suboption is the host name</b>
<i>vlanip</i>	<b>Option82 vendor-specific (suboption9) Stands for the parameter of the suboption is IP of interface vlan</b>

#### Default Value

None

#### Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping.

This command without parameters acts as a switch command. When append is enabled, the information of this command will be added to suboption9 of option82. The added information is first-subop9-param and second-subop9-param.

## Example

The following example shows how to enrich dhcp packets with option82 on interface g0/3 and set suboption 9 added parameter 1 with the hexadecimal 61-62-63-61-62-63.

```
Switch_config_g0/3# dhcp snooping information append
```

```
Switch_config_g0/3#dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
```

Here 61-62-63-61-62-63 is the Hex system of the to-be-added parameter.

### *36.1.21 dhcp snooping information drop*

#### Syntax

**dhcp snooping information drop**

**no dhcp snooping information drop**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command can be set on each port that connects the client.

After this command is set, the request packets that contain option82 will be dropped on the stipulated port.

## Example

The following example shows how to drop dhcp packets with option82 on g0/3.

```
Switch_config_g0/3# dhcp snooping information drop
```

### *36.1.22 ip-source trust*

#### Syntax

**ip-source trust**

**no ip-source trust**

#### Parameters

None

#### Default Value

The default interface is a distrusted one.

#### Usage Guidelines

Source IP address snooping is not conducted to the source-IP-trusted interface. The “no” form of this command is used to resume the default value of this interface.

## Example

The following example shows how to set interface GigaEthernet0/1 to a source-ip-trusted interface.

```
Switch_config_g0/1#ip-source trust
```

### *36.1.23 show ip dhcp-relay snooping*

#### Syntax

```
show ip dhcp-relay snooping
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to display the information about DHCP-snooping configuration.

## Example

The following example shows how to display the information about DHCP-relay snooping.

```
Switch_config#show ip dhcp-relay snooping
```

### *36.1.24 show ip dhcp-relay snooping binding*

#### Syntax

```
show ip dhcp-relay snooping binding [all]
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to display the binding information about DHCP-relay snooping.

If the all parameter is in the command sentence, all binding information about DHCP-relay snooping will be displayed.

## Example

The following example shows how to display the information about DHCP-relay snooping binding.

```
Switch_config#show ip dhcp-relay snooping binding
```

### *36.1.25 debug ip dhcp-relay snooping*

#### Syntax

**debug ip dhcp-relay snooping**

**no debug ip dhcp-relay snooping**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to enable or disable the debugging switch of DHCP-relay snooping.

#### Example

The following example shows how to enable the debugging switch of DHCP-relay snooping.

```
Switch#debug ip dhcp-relay snooping
```

```
Switch#
```

### *36.1.26 debug ip dhcp-relay event*

#### Syntax

**debug ip dhcp-relay event**

**no debug ip dhcp-relay event**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to enable or disable the event debugging switch of DHCP-relay.

#### Example

The following example shows how to enable the debugging switch of DHCP-relay event.

```
Switch#debug ip dhcp-relay event
```

```
Switch#
```

### *36.1.27 debug ip dhcp-relay binding*

#### Syntax

**debug ip dhcp-relay binding**

**no debug ip dhcp-relay binding**

Parameters	Default Value
None	None

**Usage Guidelines**

This command is used to enable or disable the debugging switch of DHCP-relay snooping binding.

**Example**

The following example shows how to enable the debugging switch of DHCP-relay snooping binding.

```
Switch#debug ip dhcp-relay binding
```

**Chapter 37 MACFF Configuration Commands**

MACFF is to isolate downlink ports of the same VLAN in a switch from exchanging inter-access packets, enabling these packets to be allocated to the default gateway of client through DHCP server and then to downlink ports. By capturing the ARP packets between downlink ports, MACFF can prevent downlink ports from learn ARPs; MACFF replies the gateway's MAC address, enabling all inter-access packets among all downlink ports to pass through the gateway.

Note: MACFF needs the support of DHCP-relay snooping, so before enabling MACFF you have to make sure that DHCP-relay snooping works normally. ICMP redirection on the gateway is disabled by default. The VLAN management address must be configured for MACFF-enabled switch.

MACFF configuration commands include:

- `macff enable`
- `macff vlan vlan_id enable`
- `macff vlan vlan_id default-ar A.B.C.D`
- `macff vlan vlan_id other_ar A.B.C.D`
- `debug macff`

**37.1 macff enable****Syntax**

To enable or disable the MACFF function globally, run the following command. To return to the default setting, use the `no` form of this command.

**macff enable**

**no macff enable**

Parameters	Default Value
None	MACFF function is disabled by default.

## Usage Guidelines

None

## Example

The following example shows how to enable the MACFF function.

```
Switch_config#macff enable
```

```
Switch_config#
```

### **37.2 macff vlan vlan\_id enable**

#### Syntax

```
macff vlan vlan_id enable
```

```
no macff vlan vlan_id enable
```

#### Parameters

Parameters	Description
<i>vlan id</i>	Stands for the ID of a VLAN. Value range: 1-4094

#### Default Value

None

## Usage Guidelines

The command is used to send MAC-Based VLAN.

## Example

The following example shows how to enable MACFF on VLAN 2 and the default gateway address is 192.168.1.1.

```
Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed vlan 2
```

```
Switch_config#macff vlan 2 enable
```

```
Switch_config#
```

### **37.3 macff vlan vlan\_id default-ar A.B.C.D**

#### Syntax

To bind DHCP snooping to standby TFTP server, run ip dhcp-relay snooping database-agent A.B.C.D.

```
macff vlan vlan_id default-ar A.B.C.D
```

```
no macff vlan vlan_id default-ar A.B.C.D
```

#### Parameters

Parameters	Description
------------	-------------



<i>A.B.C.D</i>	IP address of the default gateway
----------------	-----------------------------------

### Default Value

None

### Usage Guidelines

This command is used when you set the IP address of the client host and the default gateway manually. Of course, you also need to add the DHCP snooping binding table manually.

### Example

The following example shows how to set the address of MACFF binding gateway in vlan1 to 192.168.1.1 and the client's address to 192.168.1.10.

```
Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed vlan 1
Switch_config#ip source binding 6c:62:6d:59:18:b6 192.168.1.10 interface GigaEthernet0/1
Switch_config# macff vlan 1 default-ar 192.168.1.1
Switch_config#
```

## 37.4 *macff vlan vlan\_id other\_ar A.B.C.D*

### Syntax

**macff vlan** *vlan\_id* **other\_ar** *A.B.C.D*

**no macff vlan** *vlan\_id* **other\_ar** *A.B.C.D*

### Parameters

Parameters	Description
<i>A.B.C.D</i>	Stands for the IP address of service AR.

### Default Value

None

### Usage Guidelines

When the network segment where the client host is has other service ARs and these ARs are only accessed by the client directly without the need of gateway to forwarding packets, this command can be used to add these service ARs.

### Example

The following example shows how to set an AR with its IP being 192.168.2.254 and its MAC being 00:e0:0f:23:02:fc on port g0/1 in vlan1.

```
Switch_config#arp 192.168.2.254 00:e0:0f:23:02:fc vlan 1
Switch_config#interface g0/1
```

```
Switch_config_g0/1# dhcp snooping trust
Switch_config_g0/1#exit
Switch_config#macff vlan 1 other_ar 90.1.1.1
```

### **37.5 macff disable**

#### Syntax

**macff disable**

**no macff disable**

#### Parameters

None

#### Default Value

A specified port is allowed to enable MACFF.

#### Usage Guidelines

Though MACFF is enabled in a VLAN, MACFF can be disabled on one of the ports in this VLAN. The DHCP snooping functionality is not affected on this port after disabled its MACFF functionality.

#### Example

The following example shows how to disable MACFF on port g0/1.

```
Switch_config_g0/1#macff disable
Switch_config_g0/1#
```

### **37.6 debug macff**

#### Syntax

**debug macff**

**no debug macff**

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to enable or disable the MACFF debugging switch.

#### Example

The following example shows how to enable the debugging switch of MACFF.

```
Switch_config#debug macff
Switch_config#
```

## Chapter 38 L2 Channel Configuration Commands

### 38.1 L2 Channel Configuration Commands

The following is a L2 tunnel monitoring command:

- `l2protocol-tunnel`
- `no spanning-tree`

#### 38.1.1 L2 protocol-tunnel

##### Syntax

To configure the layer-2 (L2) protocol tunnel, run the following command.

**[no] l2protocol-tunnel [stp]**

##### Parameters

None

##### Default Value

By default, the tunnel function of any L2 protocol is not enabled on the port of the switch.

When the tunnel function is enabled, the tunnel function of all supported L2 protocols is enabled if no specific L2 protocol is designated.

##### Usage Guidelines

Currently only STP supports the tunnel function in our switches.

##### Example

The following example shows how to enable the tunnel function of the STP (including STP/PVST) on interface `g0/2`.

```
Switch_config# interface g0/2
Switch_config_g0/2# l2protocol-tunnel stp
```

#### 38.1.2 no spanning-tree

##### Syntax

To disable the STP of a port, run the following command.

**no spanning-tree**

##### Parameters

None

##### Default Value

STP can be enabled on all switch's ports by default.

##### Usage Guidelines

This command is used to disable STP on the port of a tunnel entrance, preventing this port from influencing the devices that access the tunnel by sending the STP packets.

### Example

The following example shows how to disable STP on port g0/2:

```
Switch_config# interface g0/2
```

```
Switch_config_g0/2# no spanning-tree
```

## Chapter 39 Loopback Detection Configuration Commands

Loopback Detection Configuration Commands include:

- loopback-detection
- loopback-detection enable
- loopback-detection vlan-control
- loopback-detection hello-time
- loopback-detection recovery-time
- loopback-detection control
- loopback-detection dest-mac
- loopback-detection existence
- loopback-detection frames-threshold
- loopback-detection frames-monitor
- show loopback-detection
- show loopback-detection interface

### 39.1 *loopback-detection Syntax*

To enable global loopback detection, run the following command. To return to the default setting, use the no form of this command.

```
[no] loopback-detection
```

#### Parameters

None

#### Default Value

Loopback detection is globally disabled by default.

#### Command Mode

Global configuration mode

#### Usage Guidelines

None

## Example

```
Switch#config
Switch_config#
Switch_config#loopback-detection
```

### 39.2 *loopback-detection enable Syntax*

To enable or disable loopback detection on a port, run the following command.

**[no] loopback-detection enable**

#### Parameters

None

#### Default Value

Loopback detection is disabled on a port by default.

#### Command Mode

Port configuration mode

#### Usage Guidelines

This command can be used to enable or disable loopback detection on a specified port. However, this settings takes effect only after loopback detection is enabled globally.

## Example

```
Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection enable
```

### 39.3 *loopback-detection vlan-control Syntax*

To set a port to perform loopback detection toward a specified VLAN, run the following command.

**[no] loopback-detection vlan-control *vlan-list***

#### Parameters

Parameters	Description
<i>vlan-list</i>	Stands for a VLAN specified by a port. It ranges from 1 to 4094, and up to 10 VLANs can be specified.

#### Default Value

None

#### Command Mode

Port configuration mode

## Usage Guidelines

After loopback detection is configured on a specified VLAN, the port transmits multiple detection packets of specified VLAN tag regularly and the number of these detection packets transmitted by this port can be up to 10.

## Example

```
Switch_config#interface g0/1
```

```
Switch_config_g0/1#loopback-detection vlan-control 1-5
```

### 39.4 loopback-detection hello-time Syntax

To set the transmission period of loopback detection packets, run the following command.

```
[no] loopback-detection hello-time hello-time
```

#### Parameters

Parameters	Description
<i>hello-time</i>	Stands for the transmission period of loopback packets, whose unit is second.

#### Default Value

3 seconds

#### Command Mode

Port configuration mode

#### Usage Guidelines

None

#### Example

None

### 39.5 loopback-detection recovery-time Syntax

To set the recovery time of a port after being controlled, run the following command.

```
[no] loopback-detection recovery-time recovery-time
```

#### Parameters

Parameters	Description
<i>recovery-time</i>	Stands for the recovery time of a port after being controlled, whose unit is second.

#### Default Value

10 seconds

#### Command Mode

Port configuration mode

### Usage Guidelines

None

### Example

None

## 39.6 *loopback-detection control Syntax*

To set a port to be controlled, run the following command.

```
[no] loopback-detection control { block|learning|shutdown}
```

### Parameters

Parameters	Description
<i>block</i>	<b>Sets a port to be blocked.</b>
<i>learning</i>	<b>Sets a port to be learning.</b>
<i>shutdown</i>	<b>Sets a port to be shutdown.</b>

### Default Value

None

### Command Mode

Port configuration mode

### Usage Guidelines

When a port detects loopback exists in its network, you can perform corresponding control actions to this port by setting control functions. The controlled states of a port include block, nolearn, shutdown and trap. When a controlled state is configured and loopback exists on a port, the trap message be transmitted. It is not configured by default.

After loopback detection is enabled globally, the port on which loopback detection is enabled transmits the loopback detection packets and receives the already transmitted loopback detection packets. Four control actions are conducted on the port:

**block** : This means to block the port. When loopback is found, this port will be isolated from other ports and the packets going into this port cannot be forwarded to other ports. This port is then in protocol down state and its MAC address table ages.

**nolearn**: This means forbidding this port to learn MAC addresses. Upon the discovery of loopback on a port, this port will not learn MAC addresses and at the same time age its MAC address table.

**Shutdown**: Disable the port. When detecting the loopback, the port forwards trap warning information, ages the MAC address table and automatically disables the port (error-disable). Thus, the port cannot forward the packet until the error-disable-recover time.

trap: It means that the port only reports alarms. When loopback is discovered, the port will only report alarms and age its MAC address table.

When a port is blocked, the packets entering into this port cannot be forwarded by this port and this port will go on transmitting loopback detection packets at the same time; when loopback disappears, the port will recover itself automatically. Loopback disappearance takes place if the port has not received loopback detection packets within 10 seconds. In block state the port protocol is down, while in shutdown state the port's link is down directly.

### Example

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection control block
```

### 39.7 loopback-detection dest-mac Syntax

To set the destination MAC address of loopback detection packets on a port, run the following command.

**[no] loopback-detection dest-mac *mac-addr***

#### Parameters

Parameters	Description
<i>mac-addr</i>	Stands for the MAC address that corresponds to a MAC VLAN entry.

#### Default Value

The default destination MAC address is 01-80-C2-00-00-0a.

#### Command Mode

Port configuration mode

#### Usage Guidelines

None

### Example

```
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection dest-mac 1111.1111.1111
```

### 39.8 loopback-detection existence Syntax

To set a standard to judge whether loopback exists on a port when this port is enabled or its link state is UP, run the following command.

**[no] loopback-detection existence**

#### Parameters



None

#### Default Value

Loopback is nonexistent by default.

#### Command Mode

Port configuration mode

#### Usage Guidelines

This command is mainly used to solve the problem that loopback exists on a port or not when this port is up and its loopback detection function takes effect. When the controlled action of this port is set to shutdown, it is improper to regard that loopback exists on this port for a shutdown port has already not forwarded packets. There is no loopback by default.

#### Example

None

### 39.9 *loopback-detection frames-threshold Syntax*

To configure the upper threshold the loop detection frame received every minute, run the following command.

```
[no] loopback-detection frames-threshold frames-threshold
```

#### Parameters

Parameters	Description
<i>frames-threshold</i>	The upper threshold the loop detection frame received every minute (100-200)

#### Default Value

The default upper threshold is 10.

#### Command Mode

Port configuration mode

#### Usage Guidelines

None

#### Example

```
Switch_config#interface g0/1
```

```
Switch_config_g0/1#loopback-detection frames-threshold 20
```

### 39.10 *loopback-detection frames-monitor Syntax*

To configure enable or disable frame number detection function, run the following commands.

```
[no] loopback-detection frames-monitor
```

**Parameters**

None

**Default Value**

Disabled.

**Command Mode**

Port configuration mode

**Usage Guidelines**

None

**Example**

```
Switch#config Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection frames-monitor
```

**39.11 show loopback-detection Syntax**

To display the configuration details of loopback detection, run the following command.

```
show loopback-detection
```

**Parameters**

None

**Default Value**

None

**Command Mode**

EXEC mode, Global configuration mode or interface mode

**Usage Guidelines**

This command is used to display the global or port's loopback detection configurations and port status.

**Example**

```
Switch#show loopback-detection
Loopback-detection is enable
Interface state information
Port   Status dest MacAddress Control  VLAN
-----
G0/1   UP     1234.5678.9abc BLOCK    1-5
G0/2   UP     0180.c200.000a WARNING
G0/3   UP     0180.c200.000a BLOCK
```

```
G0/4  UP    0180.c200.000a WARNING
G0/5  UP    0180.c200.000a WARNING
G0/6  UP    0180.c200.000a WARNING 1-8
G0/7  UP    0180.c200.000a WARNING
G0/8  UP    0180.c200.000a WARNING
G0/9  UP    0180.c200.000a WARNING
G0/10 UP    0180.c200.000a WARNING
G0/11 UP    0180.c200.000a WARNING
G0/12 UP    0180.c200.000a WARNING
G0/13 UP    0180.c200.000a WARNING
G0/14 UP    0180.c200.000a WARNING
G0/15 UP    0180.c200.000a WARNING
G0/16 UP    0180.c200.000a WARNING
```

### **39.12 show loopback-detection Syntax**

To display the information about the loopback detection port, run the following command.

```
show loopback-detection intf-id
```

#### **Parameters**

#### **Default Value**

None

#### **Command Mode**

EXEC mode, Global configuration mode or interface mode

#### **Usage Guidelines**

This command is mainly used to display the status of the loopback detection port.

#### **Example**

```
Switch#show loopback-detection interface g0/1
```

```
Receive Packets :0
```

```
Transmit Packets: 20
```

```
Discard Packets:0
```

```
HelloTimeOut:10
```

```
RecoverTimeOut:26
```

## Chapter 40 QoS Configuration Commands

### 40.1 QoS Configuration Commands

QoS configuration commands include:

- `cos default`
- `cos map`
- `dscp map`
- `scheduler weight bandwidth`
- `scheduler policy`
- `policy-map`
- `classify`
- `action`
- `qos policy`
- `show policy-map`
- `trust`

#### 40.1.1 `cos default`

##### Syntax

To configure the default COS value, run `cos default cos`.

**`cos default` *cos***

**`no cos default`**

##### Parameters

Parameters	Description
<code>cos</code>	The COS value ranges between 0 and 7.

##### Default Value

The default COS value is 0.

##### Usage Guidelines

This command is run in layer-2 interface configuration mode or in global configuration mode.

If this command is run in global configuration mode, default CoS in all ports are affected.

If this command is run on a layer-2 interface, the CoS on this interface will be affected.

##### Example

The following example shows how to set the CoS value of the untagged frame received by interface g0/1 to 4.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1#cos default 4
```

### 40.1.2 cos map

#### Syntax

To set the CoS priority queues, use the cos map command.

```
cos map quid cos1..cosn
```

```
no cos map
```

#### Parameters

Parameters	Description
<i>quid</i>	Stands for the ID of the CoS priority queue, 1 to 8.
<i>cos1..cosn</i>	CoS value defined by IEEE802.1p, ranging between 0 and 7

#### Default Value

CoS Value	S Priority Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

#### Usage Guidelines

This command is run in layer-2 interface configuration mode or in global configuration mode.

If this command is run in global configuration mode, CoS priority queues in all ports are affected.

If this command is run on a layer-2 interface, the CoS priority queues on this interface will be affected.

#### Example

The following example shows how to map CoS 0-2 to CoS priority queue 1 and CoS 3 to CoS priority queue 2.

```
Switch_config # cos map 1 0 1 2
```

```
Switch_config # cos map 2 3
```

### 40.1.3 dscp map

#### Syntax

To set the CoS priority queues according to dscp, use the cos map command.

```
dscp map word { cos cos-value }
```

```
no dscp map
```

#### Parameters

Parameters	Description
<i>word</i>	Dscp range table, for instance, (1,3,5,7), (1, 3-5,7), (1-7).
<i>cos cos-value</i>	The priority cos of Dscp mapping, 0-7.

#### Default Value

None

#### Usage Guidelines

This command is run in global configuration mode.

#### Example

The following example shows how to map dscp 0-2 to Cos priority queue.

```
Switch_config#dscp map 0-2 cos 1
```

### 40.1.4 scheduler weight bandwidth

#### Syntax

To set the bandwidth of the CoS priority queue, run the following command.

```
scheduler weight bandwidth weight1...weightn
```

```
no scheduler weight bandwidth
```

#### Parameters

Parameters	Description
<i>weight1...weight8</i>	Values of eight CoS priority queues WRR/WFQ, ranging between 0 and 127.

#### Default Value

The weight value of each CoS priority queue is same. All weight values of eight CoS priority queues are 1.

### Usage Guidelines

This command is run in layer-2 interface configuration mode or in global configuration mode.

If this command is run, the bandwidth of all priority queues on all interfaces are affected. Before the command is run, only the bandwidth of the priority queue will be affected. This command validates only when the queue schedule mode is set to WRR/WFQ. This command decides the bandwidth weight value of the CoS priority queue when the WRR/WFQ schedule policy is used.

The weight of the queue after the third queue can be configured to 0. Once the weight of a queue is configured to 0, the queue after that is compelled to 0, then the hybrid mode will be applied.

### Example

The following example shows how to set the weight values of eight CoS priority queues to 1, 2, 3, 4, 5, 6, 7 and 8 respectively.

```
Switch_config # scheduler weight bandwidth 1 2 3 4 5 6 7 8
```

#### 40.1.5 scheduler policy

### Syntax

To set CoS priority queue debug policy, use the scheduler policy command.

```
scheduler policy { sp | wrr | wfq | fcfs }
```

```
no scheduler policy
```

### Parameters

Parameters	Description
<i>sp</i>	Uses the SP schedule policy.
<i>wrr</i>	Uses the WRR schedule policy.
<i>wfq</i>	Uses the WFQ schedule policy.
<i>fcfs</i>	Uses the FCFS schedule policy.

### Default Value

The SP schedule policy is used by default.

### Usage Guidelines

This command can be used in layer-2 interface configuration mode or in global configuration mode.

If this command is run, the port queue schedule policy on all interfaces are affected. Before the command is run, only the belonging port queue schedule policy will be affected. No fcfs command for the interface.

After this command is configured, the schedule mode of the interface is set to the designated value.

### Example

The following example shows how to send transmission schedule mode to WRR.

```
Switch_config # scheduler policy wrr
```

### 40.1.6 policy-map

#### Syntax

To set the QoS policy map, run `policy-map name`.

**policy-map** *name*

**no policy-map** *name*

#### Parameters

Parameters	Description
<i>name</i>	Name of the QoS policy map, consisting of 1 to 20 characters.

#### Default Value

None

#### Usage Guidelines

Global Configuration mode

After the command is entered, the system enters the QoS policy mapping configuration mode. In this mode, the following commands are used:

- **classify**: Used to set the QoS flow.
- **description**: Used to describe the QoS policy map.
- **exit**: Used to exit from the QoS policy mapping configuration mode.
- **no**: Used to cancel the previously-entered command.
- **action**: Used to define the QoS action.

### Example

The following example shows how to set the QoS policy map.

```
Switch_config # policy-map myqos
```

### 40.1.7 classify

#### Syntax



To configure the match up data flow of the QoS policy map, run the following command. To return to the default setting, use the no form of this command.

```
classify {any | cos cos | icos icos | vlan vlanid | ivlan ivlanid | ethernet-type ethernet-type | precedence precedence-value | dscp dscp-value | tos tos-value | diffserv diffserv-value | ip ip-access-list | ipv6 ipv6-access-list | mac mac-access-list}
```

```
no classify {cos | icos | vlan | ivlan | ethernet-type | precedence | dscp | tos | diffserv | ip | ipv6 | mac}
```

Parameters	Description
<i>any</i>	Matches up with any packet.
<i>cos cos</i>	Configures the matching COS value; the valid range is 0 to 7
<i>icos icos</i>	Configures the matching interior tag COS value; the valid range is 0 to 7.
<i>vlan vlanid</i>	Configures the matching VLAN; the valid range is 1 to 4094
<i>ivlan ivlanid</i>	Configures interior tag vlan id. 1-4094.
<i>ethernet-type ethernet-type</i>	Configures the packet type, 0x0600-0xFFFF
<i>precedence precedence-value</i>	The priority field in tos of ip packet (5-7 of tos), 0-7.
<i>dscp dscp-value</i>	Dscp field in tos of ip packet (2-7 of tos), 0~63.
<i>tos tos-value</i>	tos in the ip packet represents delay, throughput, reliability and cost field (1-4 of tos), 0~15.
<i>diffserv diffserv-value</i>	All tos field in Ip packet: 8, 0-255.
<i>ip ip-access-list</i>	Configures the name of the matched IP access list.. The name has 1 to -20 characters.
<i>ipv6 ipv6-access-list</i>	Configures the name of the matched IPV6 access list. The name has 1 to 20 characters.
<i>mac mac-access-list</i>	Configures the name of the matched MAC access list. The name has 1 to 20 characters.

## Default Value

Any packet is matched by default.

## Usage Guidelines

QoS policy map configuration mode

All data flows in a QoS policy map must have the same mask value. The port number in the IP access list must be a definite value, not a value range.

The IP access list and the MAC access list which are used to match up with the data flows can be configured no more than 16 regulations, or the configuration will fail. When the action in the regulation is permit, the regulation is used to differentiate the data flows; when the action in the regulation is deny, the regulation has no function.

When the QinQ mode is enabled, that is, when the dot1q-tunnel command is configured, the ivlan and icos commands need be configured when the vlan or the cos value of the source packet is matched.

### Example

```
Switch-policy-map#classify vlan 4
```

#### 40.1.8 action

### Syntax

To configure the data flow policy of a QoS policy map, run the following commands.

```
action{bandwidth max-band | cos cos | drop | dscp dscp-value | precedence precedence-value | forward | icos icos | ivlanID { add addvlanid | ivlanid} | monitor session-value | quequ quequ-value | redirect interface-id | stat-packet | stat-byte | vlanID { add addvlanid | vlanid} | copy-to-cpu}
```

```
no action {bandwidth | cos | drop | dscp | precedence | forward | | icos | ivlanID | monitor | quequ | redirect | stat-packet | stat-byte | vlanID | copy-to-cpu}
```

### Parameters

Parameters	Description
<i>bandwidth max-band</i>	Maximum bandwidth to a class, the range is 1 to 163840. Unit: 64Kbps.
<i>cos cos</i>	Sets the matched COS field to cos-value 0-7.
<i>drop</i>	Drops the matched packets.
<i>dscp dscp-value</i>	Sets the matched DSCP field to dscp-value 0~63.
<i>precedence precedence-value</i>	Configures interior tag vlan id. 1-4094.
<i>ethernet-type ethernet-type</i>	Configures the packet type, 0x0600-0xFFFF
<i>precedence precedence-value</i>	The priority field in tos of ip packet (5~7 of tos). 0-7.
<i>forward</i>	Conducts no operations to the matched packets.
<i>icos icos</i>	Sets the matched COS field to cos-value 0-7.
<i>ivlan {add ivlanid} ivlanid</i>	Sets replacing or adding interior vlanid; the range is 1-4094.
<i>monitor session-value</i>	Sends the packets to monitor interface; the range is 1-4.
<i>quequ quequ-value</i>	Sets the queue mapping value 1-8.
<i>redirect interface-id</i>	Redirects the egress port of the matched flow.
<i>stat-packet</i>	Calculates the number of packets.
<i>stat-byte</i>	Calculates the number of bytes.
<i>vlanID {add vlanid} vlanid</i>	Sets replacing or adding exterior vlanid; the range is 1-4094.
<i>copy-to-cpu</i>	Sets forwarding the packet to CPU.

**Default Value**

None

**Usage Guidelines**

QoS policy map configuration mode

After enabling dot1q function, vlan and cos on the downlink port takes effect only when ivlan and icos are configured.

When Monitor is applied to the egress, an independent policymap must be configured. Otherwise, the result may turn to abnormal.

In igress direction, the action of vlan and ivlan conflicts with dscp, precedence, bandwidth, cir, mirror, stat or redirect. They cannot be configured simultaneously.

In igress direction, the action of cos and ivlan conflicts with dscp, precedence, bandwidth, cir, mirror, stat or redirect. They cannot be configured simultaneously.

In egress direction, the action of cos and ivlan conflicts with dscp, precedence, bandwidth, cir, mirror, stat or redirect. They cannot be configured simultaneously.

**Example**

```
Switch-policy-map#action redirect g0/1
```

**40.1.9 qos policy****Syntax**

To configure the QoS policy of a port, run the following command.

```
[no] qos policy name {ingress}
```

**Parameters**

Parameters	Description
<i>name</i>	<b>Stands for the name of QoS policy mapping.</b>
<i>ingress</i>	<b>Functions on the ingress port.</b>

**Default Value**

None

**Usage Guidelines**

This command can be used in layer-2 interface configuration mode or in global configuration mode.

The flow of most actions in the igress direction can be correctly matched up when they are known unicasts.

**Example**

The following example shows how to configure the pmap QoS policy on interface g0/1.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1# qos policy pmap ingress
```

### 40.1.10 show policy-map

#### Syntax

To display all or some designated QoS policy maps, run the following command.

```
show policy-map {policy-map-name | interface [interface-id] | global}
```

#### Parameters

Parameters	Description
<i>policy-map-name</i>	<b>Stands for the name of a QoS policy map.</b>
<i>interface</i> [ <i>interface-id</i> ]	<b>Stands for the policy of interface application</b>
<i>global</i>	<b>Stands for the policy of global configuration</b>

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to display all QoS policy maps.

```
Switch_config#show policy-map
```

```
policy-map 1
```

```
classify any
```

```
action redirect g0/1
```

```
policy-map 11
```

```
classify any action
```

```
Switch_config#
```

### 40.1.11 trust

#### Syntax

To show how to set the trust mode, run the following command.

```
[no]qos trust { cos | dscp | untrust }
```

#### Parameters

Parameters	Description
<i>cos</i>	<b>Stands for the trust mode.</b>
<i>dscp</i>	<b>The trust mode.</b>
<i>untrust</i>	<b>The untrust mode.</b>

#### Default Value

None

## Usage Guidelines

The command is applicable in the global configuration mode.

## Example

The following example shows how to set the trust mode cos.

```
Switch_config#qos trust cos
```

# Chapter 41 DoS-Attack Prevention Configuration Commands

## 41.1. DoS-Attack Prevention Configuration Commands

DoS-Attack Prevention Configuration Commands include:

- dos enable
- show dos

### 41.1.1. dos enable

#### Syntax

```
dos enable {all | icmp icmp-value | ip | l4port | mac | tcpflags | tcpfrag  
tcpfrag-value | tcpsmurf | icmpsmurf | ipsmurf}
```

```
no dos enable { all | icmp icmp-value | ip | l4port | mac | tcpflags | tcpfrag  
tcpfrag-value | tcpsmurf | icmpsmurf | ipsmurf }
```

#### Parameters

Parameters	Description
<i>all</i>	Enables to prevent all kinds of DoS attacks.
<i>icmp icmp-value</i>	Enables detection ICMP packet. <i>icmp-value</i> is the maximum length of the ICMP packet. The ICMP packet and ICMPv6 packet whose length is larger than <i>icmp-value</i> will be dropped.
<i>ip</i>	Prevents those DoS attack packets whose source IP addresses are equal to the destination IP addresses.
<i>l4port</i>	Starts to check the L4 packets whose source port is equal to the destination port.
<i>mac</i>	Prevents those packets whose source MACs equal to destination MACs.
<i>tcpflags</i>	Starts to check the TCP packets with illegal flags.
<i>tcpfrag</i> <i>tcpfrag-value</i>	Starts to check the DoS attack packet of TCP fragment. Here, the <i>tcpfrag-value</i> parameter means the minimum TCP header, whose default value is 20.
<i>tcpsmurf</i>	Prevents those TCP packets whose destination addresses equal to broadcast addresses.
<i>icmpsmurf</i>	Prevents those ICMP packets whose destination addresses equal to broadcast addresses.
<i>ipsmurf</i>	Prevents those ICMP packets whose destination addresses equal to broadcast addresses.

## Default Value

DoS attack prevention is disabled by default.

DoS attack prevention is configured in global mode.

The DoS IP sub-function can drop those IP packets whose source IPs are equal to the destination IPs. Prevents LAND attack.

The DoS ICMP sub-function can drop the following two kinds of packets: 1. ICMP ping packets whose size is larger than icmp-value; 2. ICMP packets, ICMPv6 packets. Prevents PING attack.

The DoS l4port sub-function can drop those TCP/UDP packets whose source port is equal to the destination port.

The DoS mac sub-function can check packet MAC address and prevents those packets whose source MAC addresses equal to destination MAC address.

The DoS tcpflags sub-function can drop the following 4 kinds of TCP packets: 1. TCP SYN flag=1 & source port<1024; 2. TCP control flags = 0 & sequence = 0; 3. TCP FIN URG PSH =1 & sequence = 0; 4. TCP FIN SYN =1.

The DoS tcpfrag sub-function can drop the following two kinds of TCP packets: 1. The TCP header is smaller than the first TCP fragment of tcpfrag-value; 2. TCP fragments whose offset values are 1. Prevents tear drop attack.

The DoS tcpsmurf sub-function can prevent tcpsmurf attack and those TCP packets whose destination addresses are broadcast addresses.

The DoS icmpsmurf sub-function can prevent icmpsmurf attack and those ICMP packets whose destination addresses are broadcast addresses.

The DoS icmpsmurf sub-function can prevent icmpsmurf attack and those IP packets whose destination addresses are broadcast addresses.

## Example

The following example shows how to set the global DoS attack prevention function to prevent those IP packets whose source IPs are destination IP addresses.

```
Switch_config#dos enable ip
```

The following example shows how to detect illegal TCPflag packets.

```
Switch_config#dos enable tcpflags
```

### 41.1.2. *show dos*

#### Syntax

To show all DoS attack prevention functions that users have set, run this command.

```
show dos
```

#### Parameters

None

### Default Value

None

### Usage Guidelines

EXEC mode

### Example

The following example shows how to display all DoS attack prevention functions.

```
Switch_config#dos enable all
```

```
Switch_config#show dos
```

```
dos enable icmp
```

```
dos enable ip
```

```
dos enable l4port
```

```
dos enable mac
```

```
dos enable tcpflags
```

```
dos enable tcpfrag
```

```
dos enable tcpsmurf
```

```
dos enable icmpsmurf
```

```
dos enable ipsmurf
```

```
Switch_config#
```

The following example shows how to set dos enable ip to display the sub-function that users have set.

```
Switch_config#dos enable ip
```

```
Switch_config#show dos
```

```
dos enable ip
```

## Chapter 42 Anti-Attack Configuration Commands

### 42.1 Anti-Attack Configuration Commands

#### 42.1.1 filter period

To configure the attack checkup period, run the following command.

```
filter period time
```

To configure the attack checkup period, run the following command.

```
no filter period
```

Parameters

Parameters	Description
<i>time</i>	Stands for the attack-proof checkup period whose unit is second. If the number of packets transmitted by the attack source exceeds the designated number in the checkup period, the attack source is thought to trigger attacks. Value range: 1-600 second(s)

#### Default Value

The default time is 10 seconds.

#### Command Mode

Global configuration mode

#### Example

```
Switch_config# filter period 15
```

#### Related Command

filter threshold

#### 42.1.2 filter threshold

To configure the threshold value which is exceeded before the system thinks an attack, run the following command. Vary your configuration in terms of the packet type.

To return to the default setting, use the no form of this command.

**filter threshold** *type value*

**no filter threshold** *type*

#### Parameters

Parameters	Description
<i>type</i>	Packet type, including ARP, BPDU, DHCP, IGMP, ICMP, and IP.
<i>value</i>	Stands for the number of the packets received in an attack-proof checkup period before the system thinks it as an attack. Value range: 5-2000

#### Default Value

The default value is 1000 packets.

#### Command Mode

Global configuration mode

#### Example

```
Switch_config# filter threshold ip 1500
```



## Related Command

filter period

### 42.1.3 filter block-time

To configure the time to block attack resource, use the filter block-time value command. To return to the default setting, use the no form of this command.

**filter block-time** *value*

**no filter block-time**

## Parameters

Parameters	Description
<i>value</i>	<b>Stands for the time of blocking the attack source after the attack is detected. Its unit is second. Value range: 1-86400</b>

## Default Value

The default value is 300 seconds.

## Command Mode

Global configuration mode

## Example

```
Switch_config# filter block-time 600
```

## Related Command

filter period

filter threshold

### 42.1.4 filter polling period

To configure the period of the attack source polling check in the hybrid mode, run the following command. To return to the default setting, use the no form of this command.

**filter polling period** *time*

**no filter polling period**

## Parameters

Parameters	Description
<i>time</i>	<b>The period of the polling attack after blocking the attack source. Unit: second Value range: 1-600</b>

## Default Value

The default time is 10 seconds.

## Command Mode

Global configuration mode

## Example

```
Switch_config# filter polling period 20
```

## Related Command

filter polling threshold

filter polling auto-fit

### 42.1.5 filter polling threshold

To configure the filter polling threshold in the hybrid mode, run the following command. Vary your configuration in terms of the packet type. To return to the default setting, use the no form of this command.

**filter polling threshold** *type value*

**no filter polling threshold** *type*

## Parameters

Parameters	Description
<i>type</i>	Packet type, including ARP, BPDU, DHCP, IGMP and ICMP.
<i>value</i>	The attack source is taken as existed if 1-2000 packets are received within any polling period. Value range: 1-2000

## Default Value

The default value is 750 packets.

## Command Mode

Global configuration mode

## Example

```
Switch_config# filter polling threshold ip 1500
```

## Related Command

filter polling period

filter polling auto-fit

### 42.1.6 filter polling auto-fit

To configure auto-fit the polling detect period and threshold, run the following command. The command is efficient by default. The polling period equals with the attack filter period and the polling packet threshold equals to 3/4 of the attack filter packet threshold. To resume to the default setting, use the no form of this command.

**filter polling auto-fit**

**no filter polling auto-fit****Parameters**

None

**Command Mode**

Global configuration mode

**Example**

```
Switch_config# filter polling auto-fit
```

**Related Command**

filter polling period

filter polling threshold

**42.1.7 filter igmp**

To enable detect ICMP attack, run the following command.

To disable ICMP attack detection, run the no form of this command.

**filter igmp****no filter igmp****Parameters**

None

**Command Mode**

Global configuration mode

**Example**

```
Switch_config# filter igmp
```

**Related Command**

filter enable

**42.1.8 filter ip source-ip**

To enable IP attack detection, run this command. To disable IP attack detection, run the no form of this command.

**filter ip source-ip****no filter ip source-ip****Parameters**

None

**Command Mode**

Global configuration mode and physical port configuration mode.

---

The command is efficient when both the global port and the physical port are configured.

### Example

```
Switch_config# filter ip source-ip
Switch_config# interface g0/1
switch_config_g0/1# filter ip source-ip
```

### Related Command

filter enable

#### ***42.1.9 filter icmp***

To enable ICMP attack detection, run the following command. To disable ICMP attack detection, run the no form of the following command.

**filter icmp**

**no filter icmp**

### Parameters

None

### Command Mode

Global configuration mode and physical port configuration mode.

The command is efficient when both the global port and the physical port are configured.

### Example

```
Switch_config# filter icmp
Switch_config# interface g0/1
switch_config_g0/1# filter icmp
```

### Related Command

filter enable

#### ***42.1.10 filter dhcp***

To enable ICMP attack detection, run the following command. To disable DHCP attack detection, run the no form of this command.

**filter dhcp**

**no filter dhcp**

### Parameters

None

### Command Mode

Global configuration mode and physical port configuration mode.

The command is efficient when both the global port and the physical port are configured.

### Example

```
Switch_config# filter dhcp
Switch_config# interface g0/1
switch_config_g0/1# filter dhcp
```

### Related Command

filter enable

#### **42.1.11 filter arp**

To enable the ARP attack detection, run this command. To disable ARP attack detection, run the no form of the following command.

**filter arp**

**no filter arp**

### Parameters

None

### Command Mode

Physical interface configuration mode

### Example

```
Switch_config_g0/1# filter arp
```

### Related Command

filter enable

#### **42.1.12 filter bpdu**

To enable the BPDU attack detection, run this command. To disable BPDU attack detection, run this command.

**filter bpdu**

**no filter bpdu**

### Parameters

None

### Command Mode

Physical interface configuration mode

### Example

```
Switch_config_g0/1# filter bpdu
```

### Related Command

filter enable

#### 42.1.13 filter mode

To configure the filter mode, run the following command.

**filter mode [ raw | hybrid ]**

Parameters

Parameters	Description
<i>raw</i>	To configure Filter as Raw mode.
<i>hybrid</i>	To configure Filter as Hybrid mode.

Default Value

Hybrid mode

Command Mode

Global configuration mode

Example

```
Switch_config# filter mode raw
```

Related Command

filter enable

#### 42.1.14 filter enable

To enable the attack detection function, run this command in global mode. To return to the default setting, use the no form of this command.

**filter enable**

**no filter enable**

Parameters

None

Command Mode

Global configuration mode

Example

```
Switch_config# filter enable
```

Related Command

None

### 42.1.15 show filter

To display the working state of the attack-proof function of the current switch, run this command. To display working state of the anti-attack feature of the current switch, use the show filter command.

#### show filter

#### show filter summary

#### Parameters

None

#### Command Mode

Non-user mode

#### Example

```
Switch#show filter
```

```
Filter period 600 seconds, polling interval 600 seconds
```

Filter thresholds:

Filter type(major code)	Minor code	Threshold	Polling
arp	A	5	3
bpdu	B	1000	750
dhcp	D	1000	750
ip	I	1000	750
icmp	I	1000	750
igmp	I	1000	750

Filters blocked:

Cause	Address	Seconds	Discard	Rate	Polling	Interface
arp	0000.abcd.1234	7.41	0	0/0	592.59	G0/1

Filters counting:

Cause	Address	Seconds	Count	Interface
arp	0000.abcd.1234	15.59	1	G0/1

Filters blocked: indicates MAC address of the blocked attack source, blocked time and source interface.

Filters counting: indicates MAC address of the attack source, counting time, the number of the receiving packets and the source interface.

## Chapter 43 IP Address Configuration Commands

### 43.1 IP Address Configuration Commands

IP Address Configuration Commands include:

- arp arp
- arp max-gw-retries
- arp retry-allarp
- arp send-gratuitous
- arp timeout
- clear arp-cache
- ip address
- ip host
- show arp
- show hosts
- show ip interface

#### 43.1.1 arp

##### Syntax

To add a static and permanent entry in the Address Resolution Protocol (ARP) cache, use the `arp` command in global configuration mode. To remove an entry from the ARP cache, use the `no` form of this command.

**arp** *ip-address hardware-address vlan [alias]*

**no arp** *ip-address [vlan]*

##### Parameters

Parameters	Description
<i>ip-address</i>	IP address corresponding to the local data-link address.
<i>hardware-address</i>	Physical address of local data-link address
<i>vlan</i>	The vlan interface belongs to the static arp
<i>alias</i>	(optional) switch responds to ARP requests as if it were the interface of the specified address.

##### Default Value

No entries are permanently installed in the ARP cache.

##### Command Mode

Global configuration mode



## Usage Guidelines

The common host all supports dynamic ARP analysis, so user doesn't need to configure static ARP entries for host.

Usually to delete static arp, run `no arp ip_address vlan`. If the vlan interface belongs to a static arp is deleted, delete the static arp by running `no arp ip_address`.

## Example

The following example shows that the MAC address of the host with IP address 1.1.1.1 is set to 00:12:34:56:78:90.

```
arp 1.1.1.1 00:12:34:56:78:90 vlan1
```

## Related Command

```
clear arp-cache
```

### 43.1.2 arp max-gw-retries

#### Syntax

To set the maximum retransmissions of the Re-Detect packets, run the following command. To return to the default setting, use the no form of this command.

```
arp max-gw-retries number
```

```
no arp max-gw-retries
```

#### Parameters

Parameters	Description
<i>number</i>	Sets the maximum retransmissions of the Re-Detect packets.

#### Default Value

3

#### Command Mode

Global configuration mode

#### Usage Guidelines

The ARP entries, which the routing entry gateway depends on, require being redetected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. This command is here used for setting the maximum ARP retransmissions in the redetection process. The bigger its value is, the greater chance the detection has.

## Example

The following example shows how to set the maximum retransmissions of the Re-Detect packets to 5:

```
arp max-gw-retries 5
```

## Related Command

show arp

### 43.1.3 arp retry-allarp

#### Syntax

To set whether to carry on redetection at the aging of ARP entries (not just meaning the gateway-related ARP entries), run the following command:

**arp retry-allarp**

**no arp retry-allarp**

#### Parameters

None

#### Command Mode

Global configuration mode

#### Usage Guidelines

By default, redetection is conducted only to the aging ARPs, which the routing entry gateway depends on. However, if this command is enabled, redetection will be conducted towards all types of aging ARP entries.

#### Example

The following example shows how to enable redetection to be carried out to all aging ARP entries.

```
arp retry-allarp
```

## Related Command

show arp

### 43.1.4 arp timeout

#### Syntax

To configure the exist time that a dynamic ARP entry remains in the Address Resolution Protocol (ARP) cache, use the arp timeout. To restore the default value, use the no form of this command or default arp timeout command.

**arp timeout seconds**

**no arp timeout default**

**arp timeout**

#### Parameters

Parameters	Description
<i>seconds</i>	<b>Time in seconds that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.</b>

### Default Value

14400 seconds (4 hours)

### Command Mode

Interface configuration mode

### Usage Guidelines

This command is ignored when it is not configured on interfaces using ARP. The `show interface` command displays the ARP timeout value, as seen in the following example from the `show interfaces` command:

```
ARP type: ARPA, ARP timeout 04:00:00
```

### Example

The following example sets the ARP timeout to 900 seconds on interface `vlan 10` to allow entries to time out more quickly than the default.

```
interface vlan 10
arp timeout 900
```

### Related Command

`show interface`

## 43.1.5 *arp send-gratuitous*

### Syntax

To configure ARP send-gratuitous function, use the `arp send-gratuitous` command.

```
arp send-gratuitous [ interval value ]
```

```
no arp send-gratuitous
```

### Parameters

Parameters	Description
<i>interval</i>	Set the intervals of <code>arp send-gratuitous</code>
<i>value</i>	Set time interval, the default is 120 seconds. The range is 15 to 600 seconds

### Command Mode

Port configuration mode

### Example

The following example start `arp send-gratuitous` on Interface `Vlan 1`, and set the send interval as 3 minutes.

```
switch_config_v1#arp send-gratuitous interval 180
```

## Related Command

arp

### 43.1.6 clear arp-cache

#### Syntax

To clear all dynamic entries from the ARP cache, use the clear arp-cache command.

```
clear arp-cache [ ip-address [ mask | vlan vlanid ] ]
```

#### Parameters

Parameters	Description
<i>ip-address</i>	<b>IP or subnets</b>
<i>mask</i>	<b>Subnet mask</b>
<i>vlanid</i>	<b>vlan ID</b>

## Command Mode

EXEC

## Example

The following example shows how to clear all dynamic ARP cache.

```
clear arp-cache
```

## Related Command

arp

### 43.1.7 ip address

#### Syntax

To set an IP address and mask for an interface, use the ip address command. Currently, there is no strict regulation to distinguish A.B.C IP address. But multicast address and broadcast address can not be used( all host section is '1'). Other than the Ethernet,multiple interfaces of other types can be connected to the same network. Other than the unnumbered interface, the configured network range of the Ethernet interface can not be the same as the arbitrary interfaces of other types. Usually one interface usually can configure one master address and numerous secondary addresses. You should configure the primary address before configuring the secondary address. IP packets generated by the system, if the upper application does not specify the source address, the switch will use the IP address configured on the sending interface that on the same network range with the gateway as the source address of the packet. If the IP address is uncertain (like interface route), the switch will use the primary address of the sending interface. If the ip address is not configured on an interface, also it is not the unnumbered interface, and then this interface will not deal with any IP packet.

To remove an IP address or disable IP processing, use the no form of this command.

**ip address** *ip-address mask* [secondary]

**no ip address** *ip-address mask*

**no ip address**

#### Parameters

Parameters	Description
<i>ip-address</i>	<b>IP address</b>
<i>mask</i>	<b>Mask of the IP network</b>
<i>secondary</i>	<b>(optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</b>

#### Default Value

No IP address is defined for the interface.

#### Command Mode

Interface configuration mode

#### Usage Guidelines

If any switch on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet.

When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

#### Example

In the following example, 202.0.0.1 is the primary address, 255.255.255.0 is the mask and 203.0.0.1 and 204.0.0.1 are secondary addresses for EthernetVLAN 10.

```
interface vlan 10
ip address 202.0.0.1 255.255.255.0
ip address 203.0.0.1 255.255.255.0 secondary
ip address 204.0.0.1 255.255.255.0 secondary
```

#### 43.1.8 ip host

##### Syntax

To define the name-address mapping of the static host, run `ip host name hostname address`. To delete the name-address mapping of the static host, run `no ip host name hostname`.

**ip host** *name address*

**no ip host** *name*

##### Parameters

Parameters	Description
<i>name</i>	Name of the host
<i>Address</i>	IP address

### Default Value

No mapping is configured.

### Command Mode

Global configuration mode

### Example

The following example shows how to set the name of the host with IP address 202.96.1.3 to dns-server.

```
ip host dns-server 202.96.1.3
```

### 43.1.9 show arp

#### Syntax

To display the entries in the Address Resolution Protocol (ARP) table, including the ARP mapping of interface IP address, the static ARP mapping that user configures and the dynamic ARP mapping, use the show arp command.

#### show arp

#### Parameters

The command has no parameters or keywords.

#### Command Mode

EXEC

#### Usage Guidelines

Shown information include:

<i>Protocol</i>	Protocol, the type of physical address mapping, for instance, IP
<i>Address</i>	Address, the network address mapping the physical address, for instance, IP address.
<i>Age</i>	Time to Live, from generating ARP entries to now. Unit: min. The value will not be affected if the switch uses the ARP entry.
<i>Hardware Address</i>	physical address, the address corresponding to the network address. The entry has not resolved is empty.
<i>Type</i>	Type, means the encapsulation type the interface uses, such as ARPA and SNAP.
<i>Interface</i>	Interface, the interface connects to the network address.

## Example

The following example shows ARP cache

```
switch#show arp
```

Protocol	IP Address	Age(min)	Hardware Address	Type	Interface
IP	192.168.20.77	11	00:30:80:d5:37:e0	ARPA	vlan 10
IP	192.168.20.33	0	Incomplete		
IP	192.168.20.22	-	08:00:3e:33:33:8a	ARPA	vlan 10
IP	192.168.20.124	0	00:a0:24:9e:53:36	ARPA	vlan 10
IP	192.168.0.22	-	08:00:3e:33:33:8b	ARPA	vlan 11

### 43.1.10 show hosts

#### Syntax

To show all entries in host name-address cache, run this command.

#### show hosts

#### Parameters

The command has no parameters or keywords.

#### Command Mode

EXEC

#### Example

The command shows all host name/address mapping:

```
show hosts
```

#### Related Command

None

### 43.1.11 show ip interface

#### Syntax

To show IP configuration of the interface, run this command.

```
show ip interface [type number | brief ]
```

#### Parameters

Parameters	Description
<i>type</i>	(Optional) interface type
<i>number</i>	(Optional) interface number
<i>brief</i>	(Optional) Shows ip protocol brief of all vlan interfaces.

## Command Mode

EXEC

## Usage Guidelines

If the link layer of an interface can effectively transmit and receive the data, the interface is available, whose state is Protocol Up. If an IP address is configured on the interface, the switch will add an direct-through route to the routing table. If the link-layer protocol is disabled, that is, if the link-layer protocol is Protocol Down, the direct-through route will be deleted. If the interface type and the number of the interface is specified, only the information about the specified interface is displayed. Otherwise, the information about the IP configuration of all interfaces is displayed.

## Example

The following example shows the IP configuration of interface VLAN 10.

```
switch#show ip interface vlan 10
vlan 10 is up, line protocol is up
IP address : 192.168.20.167/24
Broadcast address : 192.168.20.255
Helper address : not set
MTU : 1500(byte)
Forward Directed broadcast : OFF
Multicast reserved groups joined:
224.0.0.9 224.0.0.6 224.0.0.5 224.0.0.2
224.0.0.1
Outgoing ACL : not set
Incoming ACL : not set IP fast switching : ON
IP fast switching on the same interface : OFF
ICMP unreachable : ON
ICMP mask replies : OFF
ICMP redirects : ON
```

## Description

Domain	Description
<i>vlan 10 is up</i>	<b>If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.</b>
<i>line protocol is up</i>	<b>If the interface can provide two-way communication, the line protocol is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.</b>



<i>IP address</i>	<b>IP address and mask for interface</b>
<i>Broadcast address</i>	<b>Displays broadcast address</b>
<i>MTU</i>	<b>Displays the MTU value set on the interface.</b>
<i>Helper address</i>	<b>Displays helper address</b>
<i>Directed broadcast forwarding</i>	<b>Forwards the directed broadcast packets.</b>
<i>Multicast reserved groups joined</i>	<b>Multicast groups added to the interface</b>
<i>Outgoing ACL</i>	<b>Outgoing access control list used by the interface</b>
<i>Incoming ACL</i>	<b>Incoming access control list used by the interface</b>
<i>IP fast switching</i>	<b>Enables fast switching on the interface by the switch.</b>
<i>Proxy ARP</i>	<b>Enables the proxy ARP on the interface.</b>
<i>ICMP redirects</i>	<b>Forwards the ICMP redirect packet on the interface.</b>
<i>ICMP unreachable</i>	<b>Forwards the ICMP-unreachable packet on the interface.</b>
<i>ICMP mask replies</i>	<b>Forwards the ICMP-mask-replies packet on the interface.</b>

## Chapter 44 DHCP Client Configuration Commands

### 44.1 DHCP Client Configuration Commands

DHCP Client Configuration Commands include:

- `ip address dhcp`
- `ip dhcp client`
- `ip dhcp-server`
- `show dhcp lease`
- `show dhcp server`
- `debug dhcp`

The chapter describes the DHCP configuration commands. These commands are used to configure and monitor the DHCP running on the switch.

#### 44.1.1 `ip address dhcp`

##### Syntax

To obtain an IP address for the interface through the dynamic host configuration protocol (DHCP), run this command. To delete the obtained IP address, run `no ip address dhcp`.

**`ip address dhcp`**

**`no ip address dhcp`**

Parameters

None

### Default Value

None

### Command Mode

Interface configuration mode

### Usage Guidelines

The `ip address dhcp` command allows an interface to obtain an IP address through DHCP, which is very useful to dynamically connecting ISP through the Ethernet interface.

When the dynamic IP address is obtained and the `ip address dhcp` command is configured, the switch sends the DHCPDISCOVER message to the DHCP server in the network.

When the dynamic IP address is obtained and the `no ip address dhcp` command is configured, the switch sends the DHCPRELEASE message.

### Example

The following example shows that the VLAN11 interface obtains the IP address through the DHCP protocol.

```
!
interface vlan11
ip address dhcp
```

### Related Command

**ip dhcp client**

**ip dhcp-server**

**show dhcp lease**

**show dhcp server**

#### 44.1.2 ip dhcp client

### Syntax

To configure parameters at the DHCP client server of the local switch, run this command.

```
ip dhcp client { bootfileaddmac | minlease seconds | retransmit count | select seconds |
class_identifier WORD | client_identifier hrd_ether | retry_interval <1-1440> |
tftpdownload | timeout_shut }
```

```
no ip dhcp client { bootfileaddmac | minlease | retransmit | select | class_identifier |
client_identifier | retry_interval | tftpdownload | timeout_shut }
```

### Parameters

Parameters	Description
<i>bootfileaddmac</i>	<b>(optional)</b> Enables bootfile name to add client mac.

<i>minlease seconds</i>	<b>Stands for the acceptable minimum lease time, which ranges from 60 to 86400 seconds and an optional parameter.</b>
<i>retransmit count</i>	<b>Stands for the retransmission times of the protocol packets, which ranges from 1 to 10 and is an optional parameter.</b>
<i>select seconds</i>	<b>(Optional) Stands for the interval of SELECT, which ranges from 5 to 30 and is an optional parameter.</b>
<i>class_identifier WORD</i>	<b>(Optional) Sets the class ID belongs to the client</b>
<i>client_identifier hrd_ether</i>	<b>(Optional) Sets the type of client ID to Ethernet</b>
<i>retry_interval &lt;1-1440&gt;</i>	<b>(Optional) Sets retry interval</b>
<i>tftpdownload</i>	<b>(Optional) Enable TFTP download function</b>
<i>timeout_shut</i>	<b>(Optional) Enable up/down on the interface when the leasing time outs.</b>

### Default Value

The default value of the minlease parameter is 60 seconds.

The default value of the retransmit parameter is 4 times.

The default value of the select parameter is 5 seconds.

*class\_identifier* no parameter default value

*client\_identifier* the parameter default value is the character string

*retry\_interval* the default value is 1 minute

*timeout\_shut* no parameter default value

### Command Mode

Global configuration mode.

### Usage Guidelines

You can adjust these parameters according the requirements of the network structure and the DHCP server.

If the negative forms of these commands are set, these parameter will resume their default values.

### Example

The following example shows how to set the acceptable minimum lease time of the DHCP client on the switch to 100 seconds:

```
ip dhcp client minlease 100
```

The following example shows how to set the retransmission times of the protocol packets on the DHCP client of the switch to 3:

```
ip dhcp client retransmit 3
```

The following example shows, on the DHCP client of the switch, how to set the interval of SELECT to 10 seconds:

```
ip dhcp client select 10
```

#### Related Command

```
ip address dhcp
```

```
ip dhcp-server
```

```
show dhcp lease
```

```
show dhcp server
```

### 44.1.3 *ip dhcp-server*

#### Syntax

To specify a familiar DHCP server, you can use `ip dhcp-server` to designate the IP address of the DHCP server.

```
ip dhcp-server ip-address
```

```
no ip dhcp-server ip-address
```

#### Parameters

Parameters	Description
<i>ip-address</i>	<b>IP address of the DHCP server</b>

#### Default Value

There is no default IP address of the DHCP server.

#### Command Mode

Global configuration mode.

#### Usage Guidelines

You can designate an IP address for a DHCP server by using this command, which will not replace the previously designated IP address of the DHCP server.

But the previously designated IP address of the DHCP server can be removed by the negative form of this command.

#### Example

The following example shows how to specify on the switch a server, whose IP address is 192.168.20.1, to be the DHCP server:

```
ip dhcp-server 192.168.20.1
```

#### Related Command

```
ip address dhcp
```

**ip dhcp client****show dhcp lease****show dhcp server****44.1.4 show dhcp lease****Syntax**

To browse the distribution information of the DHCP server, which is used by the current switch, run show dhcp lease.

**Show dhcp lease****Parameters**

None

**Default Value**

None

**Command Mode**

EXEC

**Usage Guidelines**

You can use this command to browse the distribution information of the DHCP server of the current switch.

**Example**

The following example shows how to display the DHCP distribution information of the switch:

```
switch#show dhcp lease
```

```
Temp IP addr: 192.168.20.3 for peer on Interface: vlan11
```

```
Temp sub net mask: 255.255.255.0
```

```
DHCP Lease server: 192.168.1.3, state: 4 Rebinding
```

```
DHCP transaction id: 2049
```

```
Lease: 86400 secs, Renewal: 43200 secs, Rebind: 75600 secs
```

```
Temp default-gateway addr: 192.168.1.2
```

```
Next timer fires after: 02:34:26
```

```
Retry count: 1      Client-ID: router-0030.80bb.e4c0-v11
```

**Related Command****ip address dhcp****ip dhcp client****ip dhcp-server**

**show dhcp server**

**debug dhcp**

#### *44.1.5 show dhcp server*

**Syntax**

To display the known information of the DHCP server, run show dhcp server.

**show dhcp server**

**Parameters**

None

**Default Value**

None

**Command Mode**

EXEC

**Usage Guidelines**

This command is used to display the known information of the DHCP server.

**Example**

The following example shows how to display the already known information about the DHCP server.

```
switch#show dhcp sever
```

```
DHCP server: 255.255.255.255
```

```
Leases: 0
```

```
Discovers: 62   Requests: 0   Declines: 0   Releases: 0
```

```
Offers:      0   Acks:      0   Naks: 0     Bad:  0
```

```
Subnet: 0.0.0.0,      Domain name:
```

**Related Command**

**ip address dhcp**

**ip dhcp client**

**ip dhcp-server**

**show dhcp lease**

#### *44.1.6 debug dhcp*

**Syntax**

To browse the processing of DHCP when DHCP is run on the switch, run the following command.

**debug dhcp [detail]****no debug dhcp [detail]**

Parameters

Parameters	Description
<i>detail</i>	Means to display the content of the DHCP packet.

Default Value

Relative information is not shown.

Command Mode

EXEC

Usage Guidelines

The following example shows some key information about DHCP processing:

switch#debug dhcp

switch#2000-4-22 10:50:40 DHCP: Move to INIT state, xid: 0x7

2000-4-22 10:50:40 DHCP: SDISCOVER attempt # 1, sending 277 byte DHCP packet

2000-4-22 10:50:40 DHCP: B'cast on vlan11 interface from 0.0.0.0 2000-4-22 10:50:40  
DHCP: Move to SELECTING state, xid: 0x7

2000-4-22 10:50:46 DHCP: SDISCOVER attempt # 2, sending 277 byte DHCPpacket

2000-4-22 10:50:46 AM DHCP: B'cast on vlan11 interface from 0.0.0.0

2000-4-22 10:50:54 AM DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket

Related Command

**show dhcp lease**

## Chapter 45 IPv6 Configuration Commands

### 45.1 IP Service Configuration Commands

IP Service Configuration Commands include:

- clear tcp
- clear tcp statistics
- debug arp
- debug ip icmp
- debug ip packet
- debug ip raw
- debug ip tcp packet

- debug ip tcp transactions
- debug ip udp
- ip mask-reply
- ip mtu
- ip source-route
- ip tcp synwait-time
- ip tcp window-size
- ip unreachable
- show ip sockets
- show ip traffic
- show tcp
- show tcp brief
- show tcp statistics
- show tcp tcb

#### 45.1.1 clear tcp

##### Syntax

To delete a TCP connection, run the following command:

```
clear tcp {local host-name port remote host-name port | tcb address}
```

##### Parameters

Parameters	Description
<i>local host-name port</i>	IP address and TCP port of the local host
<i>remote host-name port</i>	IP address and TCP port of the remote host
<i>tcb address</i>	Address of the transmission control block (TCB) for the to-be-deleted TCP connection. TCB is an internal identifier of the TCP connection, which can be obtained through the show tcp brief command.

##### Command Mode

EXEC

##### Usage Guidelines

The clear tcp command is mainly used to delete the terminated TCP connection. The clear tcp command is mainly used to delete the terminated TCP connection. The TCP connection has no communication, so the system does not know that the TCP connection is already closed. In this case, the clear tcp command is used to close the invalid TCP connection. The clear tcp local host-name port remote host-name port command is used to close the TCP



connection between the IP address or port of the local host and the IP address or port of the remote host. The `clear tcp tcb address` command is used to close the TCP connection identified by the designated TCB address.

### Example

The following example shows that the TCP connection between 192.168.20.22:23 (local) and 192.168.20.120:4420 (remote). The `show tcp brief` command is used to display the information of the local and remote hosts of the current TCP connection.

```
switch#show tcp brief
```

TCB	Local Address	Foreign Address	State
0xE85AC8	192.168.20.22:23	192.168.20.120:4420	ESTABLISHED
0xEA38C8	192.168.20.22:23	192.168.20.125:1583	ESTABLISHED

```
switch#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
```

```
switch#show tcp brief
```

TCB	Local Address	Foreign Address	State
0xEA38C8	192.168.20.22:23	192.168.20.125:1583	ESTABLISHED

The following example shows how to clear the TCP connection whose TCB address is 0xea38c8. The `show tcp brief` command displays the TCB address of the TCP connection.

```
switch#show tcp brief
```

TCB	Local Address	Foreign Address	State
0xEA38C8	192.168.20.22:23	192.168.20.125:1583	ESTABLISHED

```
switch#clear tcp tcb 0xea38c8
```

```
switch#show tcp brief
```

TCB	Local Address	Foreign Address	State
-----	---------------	-----------------	-------

### Related Command

**show tcp**

**show tcp brief**

**show tcp tcb**

#### 45.1.2 clear tcp statistics

##### Syntax

To clear the statistics data about TCP, run the following command:

```
clear tcp statistics
```

##### Parameters

The command has no parameters or keywords.

## Command Mode

EXEC

## Example

The following example shows how to delete the TCP statistics information:

```
switch#clear tcp statistics
```

## Related Command

**show tcp statistics**

### 45.1.3 debug arp

## Syntax

To display the ARP interaction information, such as ARP request transmitting, ARP response receiving, ARP request receiving and ARP response transmitting, run `debug arp`. When the switch and host cannot communicate with each other, you can run the command to analyze the ARP interaction information. You can run `no debug arp` to stop displaying the ARP interaction information. To disable displaying the ARP interaction information, run this command.

**debug arp [ *packet* | *delete* ]**

**no debug arp**

## Parameters

Parameters	Description
<i>packet</i>	The debug information of ARP packet and entry
<i>delete</i>	The deleted debug information of ARP entry

## Command Mode

EXEC

## Example

```
switch#debug arp
```

```
switch#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10
IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:
```

```
00:00:00:00:00, wrong cable, vlan 11
```

```
IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10
```

```
IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10
```

```
IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10
```

The first information line shows that the switch receives an ARP request from Ethernet vlan 10. The ARP is sent from a host whose IP address is 192.168.20.116 and MAC address is

00:90:27:a7:a9:c2 and received by a host whose IP address is 192.168.20.111. The ARP request requires the MAC address of the destination host.

```
IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10
```

The second information line shows that the switch receives an ARP address request with IP 192.168.20.139 from interface Ethernet vlan 11. However, according to the interface configuration of the switch, the interface is not in the network claimed by the host. The reason may lie in the incorrect host configuration. If the switch creates an ARP cache according to the information, it cannot communicate with a host having the same address though the host connects an interface normally.

```
IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:00:00:00:00, wrong cable, vlan 11
```

The third line shows that, before the switch resolves the MAC address of host 192.168.20.77, an incomplete ARP item must be created in the ARP cache for the host; after the ARP response is received, the MAC address is entered. According to the configuration of the switch, the host connects interface Ethernet vlan 10.

```
IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10
```

The fourth information shows that the switch transmits the ARP request from interface Ethernet vlan 10, the IP address of the switch is 192.168.20.22, the MAC address of the interface is 08:00:3e:33:33:8a and the IP address of the requested host is 192.168.20.77. The fourth information line has connection with the third information line.

```
IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10
```

The fifth information line shows the switch receives the ARP response which is transferred from host 192.168.20.77 to the switch's interface 192.168.20.22 on interface Ethernet 1/0, telling that the MAC address is 00:30:80:d5:37:e0. The fifth information line has connection with the third and fourth information lines.

```
IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10
```

#### *45.1.4 debug ip icmp*

##### Syntax

To display the interaction information about ICMP, run the following command. To disable the debugging output, run `no debug ip icmp`.

```
debug ip icmp
```

```
no debug ip icmp
```

##### Parameters

The command has no parameters or keywords.

##### Command Mode

EXEC

##### Usage Guidelines

The command is used to display the received and transmitted ICMP packets, helping to resolve the end-to-end connection problem. To understand the detailed meaning of the debug ip icmp command, see RFC 792, "Internal Control Message Protocol".

### Example

```
switch#debug ip icmp
```

```
switch#ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
```

```
ICMP: rcvd echo from 192.168.20.125, len 40
```

```
ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40
```

```
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
```

```
ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36
```

```
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
```

```
ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36
```

```
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
```

```
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36
```

The first information line is explained as follows:

```
ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
```

Domain	Description
<i>ICMP</i>	<b>Displays the information about (ICMP)</b>
<i>Sent</i>	<b>Transmits the ICMP packets.</b>
<i>pointer indicating</i>	<p><b>Type of the ICMP packet, which shows the original IP packet is incorrect and specifies the incorrect domain. Other types of ICMP packet include:</b></p> <p><b>echo reply (echo reply)</b></p> <p><b>dst unreachable including:</b></p> <ul style="list-style-type: none"> <li>---net unreachable(net unreachable)</li> <li>---host unreachable (host unreachable)</li> <li>---protocol unreachable (protocol unreachable)</li> <li>---port unreachable (port unreachable)</li> <li>---fragmentation needed and DF set (fragmentation needed and DF set)</li> <li>---source route failed (source route failed)</li> <li>---net unknown (net unknown)</li> <li>---destination host unknown (destination host unknown)</li> <li>---source host isolated(source host isolated)</li> <li>---net prohibited (net prohibited)</li> <li>---host prohibited (host prohibited)</li> <li>---net tos unreachable (net tos unreachable)</li> <li>---host tos unreachable (host tos unreachable) source quench (source quench) redirect(redirect), including:</li> <li>---net redirect(net redirect)</li> <li>---host redirect(host redirect)</li> </ul>

	<p>---net tos redirect(redirection for the service type and the network)          ---host tos redirect(redirection for the service type and the host) echo (echo request)          router advertisement          router solicitation          time exceeded (timeout), including :          ---ttl exceeded (ttltimeout)          ---reassembly timeout (reassembly timeout)          parameter problem (parameter problem), including :          ---pointer indicating (point error parameter)          ---option missed (option missed)          ---bad length (bad length)          timestamp (timestamp)          timestamp reply (timestamp reply)          information request (information request)          information reply (information reply)          mask request (mask request)          mask reply (mask reply)          If it is the unknown ICMP type, the system will display the ICMP type and its code.</p>
<i>to 192.168.20.124</i>	The destination address of the ICMP packet is <b>192.168.20.124</b> , which is also the source address, of the original packet triggering the ICMP packet.
<i>(dst was 192.168.20.22)</i>	The destination address of the original packet leading to the ICMP packet is <b>192.168.20.22</b> .
<i>len 48</i>	The length of the ICMP packet is 48bytes, the length of IP header excluded.

The second information line is explained as follows:

ICMP: rcvd echo from 192.168.20.125, len 40

Domain	Description
<i>rcvd</i>	Receives the ICMP packet.
<i>echo</i>	ICMPICMP packet type, Request response packet
<i>from 192.168.20.125</i>	The source address of the ICMP packet is <b>192.168.20.125</b> .

The third information line is explained as follows:

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

Domain	Description
<i>src 192.168.20.22</i>	The source address of the ICMP packet is <b>192.168.20.125</b> .
<i>dst 192.168.20.125</i>	The destination address of the ICMP packet is <b>192.168.20.125</b> .

Different types of ICMP packets have different formats when the ICMP packet is generated.

For example, the ICMP redirect packet adopts the following format:

```
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
```

```
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
```

The first information line shows that the redirect ICMP packet from host 192.168.20.77 is received and gateway 192.168.20.26 is recommended to forward the packet to destination host 22.0.0.3; the length of the ICMP packet is 36 bytes.

The second information line shows the redirect ICMP packet is sent to host 192.168.20.124. The redirect ICMP packet notifies the host of using gateway 192.168.20.77 to send packets to host 22.0.0.5. The length of the ICMP packet is 36 bytes.

For the DST unreachable ICMP packet, the following format is adopted for printing:

```
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
```

```
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36
```

The first information line shows that, because the switch cannot route a certain IP packet, the source host 192.168.20.124 sends the unreachable ICMP packet to the destination host (202.96.209.133). The length of the ICMP packet is 36 bytes.

The second information line shows that the switch receives an ICMP packet from host 192.168.20.26, notifying that the destination host 2.2.2.2 cannot be reached. The length of the ICMP packet is 36 bytes.

#### 45.1.5 debug ip packet

##### Syntax

To display the information about IP interaction, run `debug ip raw`. To disable displaying the IP interaction information, use the `no` form of this command.

```
debug ip packet [detail] [access-group ip-access-list-name] [interface type number]
```

```
no debug ip packet
```

##### Parameters

Parameters	Description
<i>detail</i>	(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and ICMP packet type.
<i>ip-access-list-name</i>	(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.
<i>interface</i>	(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.

##### Command Mode

EXEC

## Usage Guidelines

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.

The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets
- Receiving IP fragments
- Transmitting packets
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the switch at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

## Command Mode

EXEC

### Example

```
switch#debug ip packet
```

```
switch#IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60,  
redirected
```

```
IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending
```

IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, forward

IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd

Domain	Description
<i>IP</i>	Means that the information is about the IP packet.
<i>s=192.168.20.120 (vlan 10)</i>	Source address of the IP packet and the name of the interface receiving the packet
<i>d=19.0.0.9 (vlan 10)</i>	Destination address of the IP packet and the name of the interface transmitting the packet (if the routing succeeds)
<i>g=192.168.20.1</i>	Destination address of the next hop of the IP packet, which may be the gateway address or the destination address
<i>len</i>	Length of the IP packet
<i>redirected</i>	<p>Means the switch will send the ICMP redirected packet to the source host of the ICMP packet. The following are other cases:</p> <p>Forward—the packet is forwarded.</p> <p>forward directed broadcast—Packets are forwarded as the directed broadcast and packets will be transformed as the physical broadcast on the transmission interface</p> <p>unroutable—The addressing of the packet fails and the packet will be dropped.</p> <p>source route—Source route</p> <p>rejected source route—Because the system does not support the source route, the packets with the IP source route are rejected.</p> <p>Bad options—the IP option is incorrect and the packet will be dropped.</p> <p>need frag but DF set—The local packet need be fragmented; however, the DF is reset.</p> <p>rcvd—the packet is received by the local host.</p> <p>rcvd fragment—The fragment of the packet is received.</p> <p>sending—The locally-generated packet is being sent.</p> <p>sending broad/multicast—The locally-generated broadcast/multicast packet is being sent.</p> <p>sending fragment—The locally-fragmented IP packet is being sent.</p> <p>denied by in acl—The packet is denied by the ACL of the receiver interface.</p> <p>denied by out acl—The packet is denied by the transmitter interface.</p> <p>unknown protocol—unknown protocol</p> <p>encapsulation failed—the protocol encapsulation fails in the Ethernet. When the to-be-transmitted packet is dropped on the Ethernet interface because of ARP resolution failure, the information appears.</p>

The first information line shows that the switch has received an IP packet; its source address is 192.168.20.120 and destination address is 19.0.0.9; it is from the network segment connected by interface vlan 10; the transmitter interface determined by the routing table is interface vlan 10; the gateway's address is 192.168.20.1 and the length of



the packet is 60 bytes. The gateway and the source host which transmits the IP packet are connected on the same network, that is, the network connected by interface vlan 10 of the switch. Hence, the switch transmits the ICMP redirect packet.

```
IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, redirected
```

The second information line describes the transmission of the ICMP redirect packet. The source address is the local address 192.168.20.22 and the destination address is the source address of the previous packet, that is, 192.168.20.120. The ICMP redirect packet is transmitted from interface vlan 10 to the destination directly, so the address of the gateway is the destination address 192.168.20.120. The length of the ICMP redirect packet is 56 bytes.

```
IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending
```

The third information line shows that the IP layer receives an IP packet. The source address of the packet is 192.168.20.120; the transmitter interface is interface vlan 10; the destination address of the packet is 19.0.0.9. Through the routing table, the packet is found to forward to interface VLAN 10; the address of the gateway is 192.168.20.77 and the length of the packet is 60 bytes. This information shows the packet displayed when forwarding the first information after the system sends ICMP redirection packets.

```
IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.77, len=60, forward
```

The fourth information line shows that the IP layer receives an IP packet. The source address is 192.168.20.81 and the receiver interface is VLAN 10; the destination address is 192.168.20.22, which is an IP address configured on interface VLAN 10 of the switch; the length of the packet is 56 bytes.

```
IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd
```

The output of the debug ip packet detail command is described in the following. Only newly-added parts are described.

```
switch#debug ip packet detail
```

```
switch#IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP:
src=68, dst=67
```

```
IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89
```

```
IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code
= 0
```

```
IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending,
TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK
```

Domain	Description
<i>UDP</i>	<b>Protocol name, such as UDP, ICMP or TCP. Other protocols are presented with the protocol number.</b>
<i>type, code</i>	<b>Type and code of the ICMP packet</b>
<i>src, dst</i>	<b>Source port and destination port of the UDP/TCP packet</b>
<i>seq</i>	<b>Sequence number of the TCP packet</b>
<i>ack</i>	<b>Acknowledge number of the TCP packet</b>

<i>win</i>	<b>Windows value of the TCP packet</b>
<i>ACK</i>	<b>ACK in the control bit of the TCP packet is reset, indicating that the acknowledge number is valid. Other control bits include SYN, URG, FIN, PSH and RST.</b>

The first information line shows that the UDP packet is received. The source port is 68 and the destination port is 67.

```
IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP: src=68, dst=67
```

The second information line shows that the protocol number of the received packet is 89.

```
IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89
```

The third information line shows that the ICMP packet is received. Both the packet type and the code are 0.

```
IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code = 0
```

The fourth information line shows that the TCP packet is transmitted. The source port is 1024, the destination port is 23, the sequence number is 75098622, the acknowledge number is 161000466, the size of the receiver window is 17520 and the ACK bit is reset. For the meanings of these domains, see RFC 793 — TRANSMISSION CONTROL PROTOCOL.

```
IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK
```

The following describes how to use the ACL. For example, to display the information about the packet whose source address is 192.168.20.125, you need to define the abc ACL and then allow the IP packets whose source address is 192.168.20.125. At last, you can use the ACL in the debug ip packet command.

```
switch#config
switch_config#ip access-list standard abc
switch_config_std_nacl#permit 192.168.20.125
switch_config_std_nacl#exit
switch_config#exit
switch#debug ip packet access-group abc
switch#IP: s=192.168.20.125 (vlan 101), d=192.168.20.22 (vlan 101), len=48, rcvd
```

In the previous commands, the standard ACL is used. However, the expanded ACL can also be used.

### Related Command

```
debug ip tcp packet
```

### 45.1.6 debug ip raw

#### Syntax

To display the information about IP interaction, run `debug ip raw`. To disable displaying information about IP interaction, run `no debug ip raw`.

**debug ip raw [detail] [access-group access-list-group] [interface type number]**

**no debug ip raw**

#### Parameters

Parameters	Description
<i>detail</i>	<b>(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and ICMP packet type.</b>
<i>access-list-group</i>	<b>(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.</b>
<i>interface</i>	<b>(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.</b>

#### Command Mode

EXEC

#### Usage Guidelines

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.

The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets
- Receiving IP fragments
- Transmitting packets

- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the switch at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

### Example

It is the same with `debug ip packet`, so it is omitted here.

### Related Command

`debug ip tcp packet`

#### *45.1.7 debug ip tcp packet*

### Syntax

To display the information about receiving and transmitting the TCP packet, run `debug ip tcp packet`. To disable displaying relative information, run `no debug ip tcp packet`.

**debug ip tcp packet**

**no debug ip tcp packet**

### Parameters

The command has no parameters or keywords.

### Command Mode

EXEC

### Example

```
switch#debug ip tcp packet
```

```
switch#tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460
```

```
DATA 1 ACK 3130379810 PSH WIN 4380
```

```
tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810
```

```
DATA 2 ACK 50659460 PSH WIN 16372
```

```
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461
```

```
DATA 50 ACK 3130379812 PSH WIN 4380
```

```

tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511
      ACK 3130379812 FIN WIN 4380
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659511 WIN 16321
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659512 WIN 16321
tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659512 FIN WIN 16321
tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512
      ACK 3130379813 WIN 4380
tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318
      DATA 2 ACK 8057944 PSH WIN 17440
tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944 RST

```

Domain	Description
<i>tcp:</i>	Information about the TCP packets
<i>O</i>	Transmits the TCP packets.
<i>ESTABLISHED</i>	TCP Current state of the TCP connection For the description of the TCP connection's state, see the description of the debug ip tcp transactions command.
<i>192.168.20.22:23</i>	The source address of the packet is 192.168.20.22 and the source port is 23.
<i>192.168.20.125:3828</i>	The destination address of the packet is 192.168.20.125 and the destination port is 3828.
<i>seq 50659460</i>	The sequence number of the packet is 50659460.
<i>DATA 1</i>	Means that the packet contains only one effective byte.
<i>ACK 3130379810</i>	The acknowledgment number of the packet is 3130379810.
<i>PSH</i>	PSH is reset in the control bit of the packet. Other control bytes include ACK, FIN, SYN, URG and RST.
<i>WIN 4380</i>	Window domain of the packet used to notify the peer end to receive the cache size, which is 4380 bytes currently 4380 bytes
<i>I</i>	Receives the TCP packet.

If a domain of the previous domains does not appear, the domain has no effective value in the TCP packet.

#### Related Command

**debug ip tcp transactions**

### 45.1.8 debug ip tcp transactions

#### Syntax

To display the important interaction information about TCP, such as the state change of the TCP connection, run `debug ip tcp transactions`. To disable displaying relative information, run `no debug ip tcp transactions`.

**debug ip tcp transactions**

**no debug ip tcp transactions**

#### Parameters

The command has no parameters or keywords.

#### Command Mode

EXEC

#### Example

```

switch#debug ip tcp transactions

switch#TCP: rcvd connection attempt to port 23

TCP: TCB 0xE88AC8 created

TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]

TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]

TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]

TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0:0]

TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]

TCP: TCB 0xE923C8 deleted TCP: TCB 0xE7DBC8 created

TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to SYN_SENT

TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]

TCP: state was SYN_SENT -> ESTABLISHED [1022 -> 192.168.20.124:513]

TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]

TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]

TCP: sending FIN [1022 -> 192.168.20.124:513]

TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]

TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]

TCP: TCB 0xE7DBC8 deleted

```

Domain	Description
TCP:	Displays the TCP interaction information.

<i>rcvd connection attempt to port 23</i>	Receives the connection request from the peer port23 ( that is, the TELNET port.
<i>TCB 0xE88AC8 created</i>	Generates a new control block for the TCP connection, which is identified as 0xE88AC8.
<i>state was LISTEN -&gt; SYN_RCVD</i>	<p>Means that the TCP state machine changes from LISTEN to SYN_RCVD.</p> <p>The states of the TCP include:</p> <p><b>LISTEN</b>—waiting for the TCP connection request from any remote host</p> <p><b>SYN_SENT</b>—Sending out the connection request to trigger the TCP connection negotiation and then waiting for the peer's response</p> <p><b>SYN_RCVD</b>—receiving the connection request from the peer, sending out the acknowledgment response and also sending out its connection request, and waiting for the connection request acknowledgment from the peer</p> <p><b>ESTABLISHED</b>---means that the connection is created; the connection is in the data transmission phase; the data of the upper-layer application can be received and transmitted.</p> <p><b>FIN_WAIT_1</b>—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited.</p> <p><b>FIN_WAIT_2</b>—Means that the connection termination request has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited.</p> <p><b>CLOSE_WAIT</b>—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request.</p> <p><b>CLOSING</b>—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request.</p> <p><b>LAST_ACK</b>—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited.</p> <p><b>TIME_WAIT</b>—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped.</p> <p><b>CLOSED</b>—Means that there is no connection or the connection has been completed shut down.</p> <p>For more detailed information, see RFC 793, TRANSMISSION CONTROL PROTOCOL.</p>
<i>[23-&gt; 192.168.20.125:3828]</i>	The content in the bracket is explained as follows: The first domain (23) stands for the local TCP port. The second domain (192.168.20.125) stands for the remote IP address.

	<b>The third domain(3828) stand for the remote TCP port.</b>
<i>sending SYN</i>	<b>Transmits a connection request out (the SYN of the control bit in the TCP header is reset). Other TCP control bits include SYN, ACK, FIN, PSH, RST and URG.</b>
<i>seq 50658312</i>	<b>The sequence number of the transmitted packet is 50658312.</b>
<i>ack 3130379657</i>	<b>The acknowledgement number of the transmitted packet is 3130379657.</b>
<i>rcvd FIN</i>	<b>Means that the connection termination request is received (FIN in the control bit of the TCP header is reset).</b>
<i>connection closed by user</i>	<b>Means that the upper-layer application requires disabling the TCP connection.</b>
<i>connection timed out</i>	<b>Means that the connection is closed because it times out.</b>

### Related Command

**debug ip tcp packet**

#### 45.1.9 debug ip udp

#### Syntax

To display the interaction information about UDP, run the following command. To stop displaying the information about UDP interaction, run no debug ip udp.

**debug ip udp**

**no debug ip udp**

#### Parameters

The command has no parameters or keywords.

#### Command Mode

EXEC

#### Example

```
switch#debug ip udp
```

```
switch#UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32
```

```
UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008
```

Domain	Description
<i>UDP:</i>	<b>Means that the information is about the UDP packet.</b>
<i>rcvd</i>	<b>Receiving the packets</b>
<i>sent</i>	<b>Means that the packet is transmitted.</b>
<i>src</i>	<b>Stands for the source IP address and UDP port of the UDP packet.</b>
<i>dst</i>	<b>Stands for the destination IP address and UDP port of the UDP packet.</b>



<i>len</i>	<b>Stands for the length of UDP packet.</b>
------------	---

The first information shows that the UDP packet is received. Its source address is 192.168.20.99 and its source port is port 520; its destination address is 192.168.20.255 and its destination port is port 520; the length of the packet is 32 bytes.

The second information shows that the UDP packet is transmitted. Its source address is 192.168.20.22 and its source port is port 20001; its destination address is 192.168.20.43 and its destination port is port 1001; the length of the packet is 1008 bytes.

#### 45.1.10 *ip mask-reply*

##### Syntax

To enable the switch to answer the request of the IP mask on the designated interface, run `ip mask-reply`. To disable this function, run `no ip mask-reply`.

**ip mask-reply**

**no ip mask-reply**

**default ip mask-reply**

##### Parameters

The command has no parameters or keywords.

##### Default Value

The IP mask request is not answered.

##### Command Mode

Interface configuration mode

##### Example

```
interface vlan 11
```

```
ip mask-reply
```

#### 45.1.11 *ip mtu*

##### Syntax

To set the MTU of the IP packet transmitted from an interface, run `ip mtu bytes`. To reuse the default value of MTU, run `no ip mtu`.

**ip mtu bytes**

**no ip mtu**

##### Parameters

Parameters	Description
<i>bytes</i>	<b>Maximum IP transmission length which is counted with bytes</b>

### Default Value

The physical media of the interfaces are different, while the MTU on the interfaces are same.

Sixty-eight bytes is the minimum MTU.

### Command Mode

Interface configuration mode

### Usage Guidelines

If the length of the IP message exceeds IP MTU configured on the interface, the switch fragments the message. All devices connecting on the same physical media need be configured the same MTU. The MTU affects the IP MTU. If the value of IP MTU is the same as that of the MTU, the value of IP MTU automatically changes to the new value of the MTU when the MTU value changes. The change of the IP MTU does not affect the MTU.

The minimum value of IP MTU is 68 bytes and the maximum value of IP MTU cannot exceed the MTU value configured on the interface.

### Example

The following example shows that IP MTU on interface vlan 10 is set to 200:

```
interface vlan 10
ip mtu 200
```

### Related Command

**mtu**

#### *45.1.12 ip source-route*

### Syntax

To enable the switch to handle the IP packet with the source IP route option, run `ip source-route`. To enable the switch to drop the IP packet with the source IP route option, run `no ip source-route`.

**ip source-route**

**no ip source-route**

### Parameters

None

### Default Value

The IP packet with the source IP route option is handled.

### Command Mode

Global configuration mode

### Example

The following example shows how to enable the switch to handle the IP packet with the source IP route option.

```
ip source-route
```

#### Related Command

**ping**

#### 45.1.13 ip tcp synwait-time

##### Syntax

To set the timeout time for the switch to wait for the successful TCP connection, run `ip tcp synwait-time`. To resume the default timeout time, run `no ip tcp synwait-time`.

**ip tcp synwait-time** *seconds*

**no ip tcp synwait-time**

##### Parameters

Parameters	Description
<i>seconds</i>	<b>Time for the TCP connection, whose unit is second. The valid vale ranges between 5 and 300 seconds. The default value is 75.</b>

##### Default Value

75 seconds

##### Command Mode

Global configuration mode

##### Usage Guidelines

When the switch triggers the TCP connection and if the TCP connection is not established in the designated wait time, the switch views that the connection fails and then sends the result to the upper-layer program. You can set the wait time for creation of the TCP connection. The default value of the wait time is 75 seconds. The option has no relation with the TCP connection packet which is forwarded through the switch, but has relation with the TCP connection of the switch itself.

##### Example

The following example shows how to set the wait time of creating TCP connection to 30 seconds:

```
switch_config#ip tcp synwait-time 30
```

#### 45.1.14 ip tcp window-size

##### Syntax

To resume the default size of the TCP window, run `no ip tcp window-size`.

**ip tcp window-size** *bytes*

## no ip tcp window-size

### Parameters

Parameters	Description
<i>bytes</i>	<b>Size of the window The maximum window size is 65535 bytes. The default window size is 2000 bytes.</b>

### Default Value

2000 bytes

### Command Mode

Global configuration mode

### Usage Guidelines

Do not change the window size at will unless you have a definite purpose.

### Example

The following example shows how to set the size of the TCP window to 6000 bytes.

```
switch_config#ip tcp window-size 6000
```

## 45.1.15 ip unreachable

### Syntax

To enable the switch to transmit the ICMP unreachable packet, run `ip unreachable`. To enable the switch to stop transmitting this packet, run `no ip unreachable`.

### ip unreachable

### no ip unreachable

### Parameters

The command has no parameters or keywords.

### Default Value

ICMP unreachable packets are sent by default.

### Command Mode

Interface configuration mode

### Usage Guidelines

When the switch forwards the IP packet, the packet may be dropped because there is no relative route in the routing table. In this case, the switch can send the ICMP unreachable packet to the source host, notifying the source host and enabling it to detect the host timely and correct the fault rapidly.

### Example

The following example shows how to enable the ICMP unreachable packet to be transmitted on interface vlan 10:

```
interface vlan 10
```

```
ip unreachable
```

#### 45.1.16 show ip sockets

##### Syntax

To display the socket information, run this command.

```
show ip sockets [ socketid ]
```

##### Parameters

Parameters	Description
<i>socketid</i>	Displays some socket information.

##### Command Mode

EXEC

##### Example

```
switch#show ip sockets
```

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590

Domain	Description
<i>Proto (Protocol)</i>	IP Protocol ID 17 is UDP and 6 is TCP
<i>Remote (Remote)</i>	Remote address
<i>Port (Port)</i>	Remote port
<i>Local(local)</i>	Local address
<i>Port (Port)</i>	Local port
<i>In(receive)</i>	Total number of the received bytes
<i>Out(send)</i>	Total number of the received bytes

### 45.1.17 *show ip traffic*

#### Syntax

To display the flow statistics information, run the following command:

```
show ip traffic
```

#### Parameters

The command has no parameters or keywords.

#### Command Mode

EXEC

#### Example

```
switch#show ip traffic
```

IP statistics:

Rcvd: 0 total, 0 local destination, 0 delivered

0 format errors, 0 checksum errors, 0 bad ttl count

0 bad destination address, 0 unknown protocol, 0 discarded

0 filtered, 0 bad options, 0 with options

Opts: 0 loose source route, 0 record route, 0 strict source route

0 timestamp, 0 router alert, 0 others

Frag: 0 fragments, 0 reassembled, 0 dropped

0 fragmented, 0 fragments, 0 couldn't fragment

Bcast: 0 received, 0 sent

Mcast: 0 received, 0 sent

Sent: 230 generated, 0 forwarded

0 filtered, 0 no route, 0 discarded ICMP statistics:

Rcvd: 0 total, 0 format errors, 0 checksum errors

0 redirect, 0 unreachable, 0 source quench

0 echos, 0 echo replies, 0 mask requests, 0 mask replies

0 parameter problem, 0 timestamps, 0 timestamp replies

0 time exceeded, 0 router solicitations, 0 router advertisements

Sent: 0 total, 0 errors

0 redirects, 0 unreachable, 0 source quench

0 echos, 0 echo replies, 0 mask requests, 0 mask replies

0 parameter problem, 0 timestamps, 0 timestamp replies

0 time exceeded, 0 router solicitations, 0 router advertisements

UDP statistics:

Rcvd: 28 total, 0 checksum errors, 22 no port, 0 full sock

Sent: 0 total

TCP statistics:

Rcvd: 0 total, 0 checksum errors, 0 no port

Sent: 3 total

IGMP statistics:

Rcvd: 0 total, 0 format errors, 0 checksum errors

0 host queries, 0 host reports

Sent: 0 host reports

ARP statistics:

Rcvd: 8 total, 7 requests, 1 replies, 0 reverse, 0 other

Sent: 5 total, 5 requests, 0 replies (0 proxy), 0 reverse

Domain	Description
<i>format errors(format errors)</i>	<b>Error of the packet's format, such as incorrect IP header length</b>
<i>bad hop count(TTLerror)</i>	<b>If the routing switch finds that the TTL value of the packet decreases to zero when it forwards the packet, the packet will be dropped.</b>
<i>no route(no route)</i>	<b>Means that the switch has no corresponding route.</b>

#### 45.1.18 show tcp

Syntax

To display all status information of TCP connection, run the following command.

**show tcp**

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

```
switch#show tcp
```

```
TCB 0xE9ADC8
```

```
Connection state is ESTABLISHED, unread input bytes: 934
```

```
Local host: 192.168.20.22, Local port: 1023
```

```
Foreign host: 192.168.20.124, Foreign port: 513
```

```
Enqueued bytes for transmit: 0, input: 934 mis-ordered: 0 (0 packets)
```

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

```
iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520
```

```
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380
```

```
SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
```

```
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms
```

```
Datagrams (max data segment is 1460 bytes):
```

```
Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
```

```
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61
```

Domain	Description
<i>TCB 0xE77FC8</i>	<b>Internal identifier of the control block for the TCP connection</b>
<i>Connection state is ESTABLISHED</i>	<p><b>Current state of the TCP connection</b> The TCP connection may be in one of the following states:</p> <p><b>LISTEN---</b>Means the TCP connection request from any remote host is being waited.</p> <p><b>SYN_SENT---</b>Means that the response from the peer is being waited after the connection request is transmitted to the peer.</p> <p><b>SYN_RCVD---</b>receiving the connection request from the peer, sending out the acknowledgment response and also sending out its connection request, and waiting for the connection request acknowledgment from the peer</p> <p><b>ESTABLISHED---</b>means that the connection is created; the connection is in the data transmission phase; the</p>



	<p>data of the upper-layer application can be received and transmitted.</p> <p><b>FIN_WAIT_1</b>—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited.</p> <p><b>FIN_WAIT_2</b>—Means that the connection termination request has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited.</p> <p><b>CLOSE_WAIT</b>—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request.</p> <p><b>CLOSING</b>—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request.</p> <p><b>LAST_ACK</b>—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited.</p> <p><b>TIME_WAIT</b>—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped.</p> <p><b>CLOSED</b>—Means that there is no connection or the connection has been completed shut down.</p> <p>For more detailed information, see RFC 793, <b>TRANSMISSION CONTROL PROTOCOL</b>.</p>
<i>unread input bytes:</i>	Data that is submitted to but not yet received by the upper-layer application after the lower-layer TCP handles
<i>Local host:</i>	Local IP address
<i>Local port:</i>	Local TCP port
<i>Foreign host:</i>	Remote IP address
<i>Foreign port:</i>	Remote TCP port.
<i>Enqueued bytes for transmit:</i>	Bytes in the transmission queue, including the transmitted but unacknowledged data bytes and not-yet-transmitted data bytes
<i>input:</i>	Data in the receiver queue which is waiting for being received by the upper-layer application after sorting
<i>mis-ordered:</i>	Number of bytes and number of packets in the mis-ordered queue. These data can enter the receiver queue in order and be received by the upper-layer application after other data is received. For example, if packets 1, 2, 4, 5 and 6 are received, packets 1 and 2 can enter the receiver queue, while packets 4, 5 and 6 have to enter

	the mis-ordered queue to wait for the arrival of packet 3.
--	--

The information about the currently-displayed timer will then be displayed, including start-up times, timeout times and next timeout time (0 means the timer doesn't work currently). Each connection has its independent timers. The timeout times of the timer are generally less than the start-up times of the timer because the timer may be reset when it is running. For example, if the system receives the peer's acknowledgment of all transmitted data when the re-sending timer runs, the re-sending timer will stop running.

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

Domain	Description
<i>Timer</i>	<b>Name of the timer</b>
<i>Starts</i>	<b>Start-up times of the timer</b>
<i>Wakeups</i>	<b>Timeout times of the timer</b>
<i>Next(ms)</i>	<b>Time before next timeout occurs (unit: millisecond)0 means that the timer is not running.</b>
<i>Retrans</i>	<b>Retransmission timer which is used to retransmit the data. The timer is restarted after the data is transmitted. If the data is not acknowledged by the peer during the timeout time, the data will be resent.</b>
<i>TimeWait</i>	<b>Time-wait timer which is used to ensure that the peer receives the acknowledgement of the connection termination request.</b>
<i>SendWnd</i>	<b>Timer of the transmission timer, used to ensure that the receiver window resumes the normal size after the TCP acknowledgment is lost.</b>
<i>KeepAlive</i>	<b>KeepAlive timer used to ensure that the communication link is normal and the peer is still in the connection state. It will trigger the transmission of the test packet to detect the state of the communication link and the peer's state.</b>

The sequence number of the TCP connection will then be displayed. The reliable and ordered data transmission is guaranteed through the sequence number. The local/remote host conducts flow control and transmission acknowledgment through the sequence number.

```
iss: 29139463  snduna: 29139525  sndnxt: 29139525  sndwnd: 17520
irs: 709124039  rcvnxt: 709205436  rcvwnd: 4380
```

Domain	Description
--------	-------------

<i>iss:</i>	<b>Initial transmission sequence number</b>
<i>snduna:</i>	<b>Transmission sequence number of the first byte in the data which has been transmitted but the peer's acknowledgment is not received</b>
<i>sndnxt:</i>	<b>Transmission sequence number of the first byte in the data which will be transmitted next time</b>
<i>sndwnd:</i>	<b>Size of the TCP window of the remote host.</b>
<i>irs:</i>	<b>Initial reception sequence number, that is, initial transmission sequence number of the remote host</b>
<i>rcvnxt:</i>	<b>Recently-acknowledged acceptance sequence number</b>
<i>rcvwnd:</i>	<b>Size of the TCP window of the local host</b>

The transmission time recorded by the local host is then displayed. The system can adapt to different networks according to the data.

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

<b>Domain</b>	<b>Description</b>
<i>SRTT:</i>	<b>Round-trip time after smooth handle</b>
<i>RXT:</i>	<b>Retransmission timeout time</b>
<i>RTV:</i>	<b>Change value of the round-trip time</b>
<i>MinRXT:</i>	<b>Allowable minimum retransmission timeout</b>
<i>MaxRXT:</i>	<b>Allowable maximum retransmission timeout</b>
<i>ACK hold:</i>	<b>Maximum latency time for delaying the acknowledgment and enabling it to be transmitted together with the data</b>

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

<b>Domain</b>	<b>Description</b>
<i>max data segment is</i>	<b>Maximum data-segment length allowed by a connection</b>
<i>Rcvd:</i>	<b>Number of packets received by the local host through the connection and the number of mis-ordered packets</b>
<i>with data:</i>	<b>Number of packets which contains valid data</b>
<i>total data bytes:</i>	<b>Total data bytes contained in the packet</b>
<i>Sent</i>	<b>Total number of packets transmitted by the local host during the connection and the number of resent packets</b>
<i>with data:</i>	<b>Number of packets which contains valid data</b>
<i>total data bytes:</i>	<b>Total data bytes contained in the packet</b>

## Related Command

`show tcp brief``show tcp tcb`*45.1.19 show tcp brief*

## Syntax

To display the brief information about the TCP connection, run the following command:

`show tcp brief [all]`

## Parameters

Parameters	Description
<i>all</i>	(optional) Displays all ports. If the keyword is not entered, the system will not display the port in listening mode.

## Command Mode

EXEC

## Example

switch#show tcp brief

TCB	Local Address	Foreign Address	State
0xE9ADC8	192.168.20.22:1023	192.168.20.124:513	ESTABLISHED
0xEA34C8	192.168.20.22:23	192.168.20.125:1472	ESTABLISHED

Domain	Description
<i>TCB</i>	TCP Internal identifier of the TCP connection
<i>Local Address</i>	Local address and local TCP port
<i>Foreign Address</i>	IP address and TCP port of the remote host.
<i>State</i>	State of the connection For details, see the show tcp command.

## Related Command

`show tcp``show tcp tcb`*45.1.20 show tcp statistics*

## Syntax

To display the statistics data about TCP, run the following command.

`show tcp statistics`

## Parameters

The command has no parameters or keywords.

## Command Mode

EXEC

## Example

```
switch#show tcp statistics
```

```
Rcvd: 148 Total, 0 no port
```

```
0 checksum error, 0 bad offset, 0 too short
```

```
131 packets (6974 bytes) in sequence
```

```
0 dup packets (0 bytes)
```

```
0 partially dup packets (0 bytes)
```

```
0 out-of-order packets (0 bytes)
```

```
0 packets (0 bytes) with data after window
```

```
0 packets after close
```

```
0 window probe packets, 0 window update packets
```

```
0 dup ack packets, 0 ack packets with unsend data
```

```
127 ack packets (247 bytes)
```

```
Sent: 239 Total, 0 urgent packets
```

```
6 control packets
```

```
123 data packets (245 bytes)
```

```
0 data packets (0 bytes) retransmitted
```

```
110 ack only packets (101 delayed)
```

```
0 window probe packets, 0 window update packets
```

```
4 Connections initiated, 0 connections accepted, 2 connections established
```

```
3 Connections closed (including 0 dropped, 1 embryonic dropped)
```

```
5 Total rxmt timeout, 0 connections dropped in rxmt timeout
```

```
1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive
```

Domain	Description
<i>Rcvd:</i>	<b>Statistics data of the packets received by the switch</b>
<i>Total</i>	<b>Total number of the received packets</b>
<i>no port</i>	<b>Number of received packets which have no destination ports</b>
<i>checksum error</i>	<b>Number of received packets which have checksum error</b>

<i>bad offset</i>	Number of received packets which have offset error
<i>too short</i>	Number of received packets whose length is less than the valid effective length
<i>packets in sequence</i>	Number of packets received in order
<i>dup packets</i>	Number of received duplicate packets
<i>partially dup packets</i>	Number of some duplicate packets received
<i>out-of-order packets</i>	Number of packets received out of order
<i>packets with data after window</i>	Number of received packets whose data exceeds the received window of the switch
<i>packets after close</i>	Number of packets received after the connection is closed
<i>window probe packets</i>	Number of received packets about window detection
<i>window update packets</i>	Number of received packets about window update
<i>dup ack packets</i>	Number of packets which are re-acknowledged after received
<i>ack packets with unsent data</i>	Number of packets which are received but not sent
<i>ack packets</i>	Number of acknowledgement packets
<i>Sent</i>	Statistics data of the packets transmitted by the switch
<i>Total</i>	Total number of the transmitted packets
<i>urgent packets</i>	Number of transmitted urgent packets
<i>control packets</i>	Total number of control packets (SYN, FIN or RST) which have been transmitted
<i>data packets</i>	Number of transmitted urgent packets
<i>data packets retransmitted</i>	Number of resent data packets
<i>ack only packets</i>	Number of transmitted acknowledgment packets
<i>window probe packets</i>	Number of transmitted packets about window detection
<i>window update packets</i>	Number of transmitted packets about window update
<i>Connections initiated</i>	Number of locally-initiated connections
<i>connections accepted</i>	Number of locally-accepted connections
<i>connections established</i>	Number of locally-established connections
<i>Connections closed</i>	Number of locally-closed connections
<i>Total rxmt timeout</i>	Total number of re-transmission timeouts
<i>Connections dropped in rxmit timeout</i>	Number of disconnected connections because of re-transmission timeout
<i>Keepalive timeout</i>	Number of keepalive timeouts
<i>keepalive probe</i>	Number of transmitted packets about keepalive detection
<i>Connections dropped in keepalive</i>	Number of connections which are disconnected because of Keepalive

## Related Command

`clear tcp statistics`

### 45.1.21 `show tcp tcb`

## Syntax

To display the state of a TCP connection, run the following command:

`show tcp tcb address`

## Parameters

Parameters	Description
<i>address</i>	Address of the transmission control block (TCB) for the to-be-displayed TCP connection. TCB is an internal identifier of the TCP connection, which can be obtained through the <code>show tcp brief</code> command.

## Command Mode

EXEC

## Example

The following information is displayed after the `show tcp` command is run:

```
switch_config#show tcp tcb 0xea38c8
```

```
TCB 0xEA38C8
```

```
Connection state is ESTABLISHED, unread input bytes: 0
```

```
Local host: 192.168.20.22, Local port: 23
```

```
Foreign host: 192.168.20.125, Foreign port: 1583
```

```
Enqueued bytes for transmit: 0, input: 0 mis-ordered: 0 (0 packets)
```

Timer	Starts	Wakeups	Next(ms)
Retrans	4	0	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	+5	0	6633000

```
iss: 10431492 snduna: 10431573 sndnxt: 10431573 sndwnd: 17440
```

```
irs: 915717885 rcvnxt: 915717889 rcvwnd: 4380
```

SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):

Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3

Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80

### Related Command

**show tcp**

**show tcp brief**

## 45.2 ACL Configuration Commands

ACL configuration commands include:

- deny
- ip access-group
- ip access-list
- permit
- show ip access-list

### 45.2.1 deny

#### Syntax

To configure the deny regulations in IP ACL configuration mode, run `deny source [source-mask]` or `deny protocol source source-mask destination destination-mask [tos tos]`. To remove a deny regulation from an IP ACL, run `no deny source [source-mask]` or `no deny protocol source source-mask destination destination-mask [tos tos]`.

**deny source** *[source-mask]* [**log**] [**location**]

**no deny source** *[source-mask]* [**log**]

**deny protocol source source-mask destination destination-mask** [[**precedence** precedence] [**tos tos** ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**tll**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

**no deny protocol source source-mask destination destination-mask** [[**precedence** precedence] [**tos tos** ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**tll**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

For the Internet Control Message Protocol (ICMP), use the following command syntax.

**deny icmp source source-mask destination destination-mask [icmp-type] [**precedence** precedence] [**tos tos**] [**log**]**



For the Internet Group Management Protocol (IGMP), run the following command syntax.

```
deny igmp source source-mask destination destination-mask [igmp-type] [precedence precedence] [tos tos] [log]
```

For the Transmission Control Protocol (TCP), use the following command syntax.

```
deny tcp source source-mask [operator port] destination destination-mask [operator port] [established] [precedence precedence] [tos tos] [log]
```

For the User Datagram Protocol (UDP), use the following command syntax.

```
deny udp source source-mask [operator port] destination destination-mask [operator port] [precedence precedence] [tos tos] [log]
```

### Parameters

Parameters	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igmp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
<i>source</i>	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>source-mask</i>	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>destination</i>	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
<i>destination-mask</i>	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
<i>precedence precedence</i>	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This parameter is optional.
<i>tos tos</i>	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
<i>icmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
<i>igmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
<i>operator</i>	((Optional) Compares the source or destination ports.) The operations include lt, gt, eq and neq. If the operator symbol is behind source and source-mask, it must match

	up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
<i>Port</i>	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535. The name of the TCP port is listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
<i>established</i>	An optional parameter for the TCP protocol, representing an established connection. If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
<i>log</i>	An optional parameter, meaning the logs can be recorded
<i>location</i>	Insert the rule to designated num

## Command Mode

IP ACL configuration commands

## Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the match-up occurs, the expanded access control list will not be checked again. The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's access path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

### Note:

After an access control list is originally established, (ny added content is) put at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Bgp、ftp、ftp-data、login、pop2、pop3、smtp、telnet、www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Domain, snmp, syslog, tftp

## Example

The following example shows how to forbid network segment 192.168.5.0.

```
ip access-list standard filter deny 192.168.5.0 255.255.255.0
```

**Note:**

The IP access control list ends with a connotative deny regulation.

**Related Command**

```
ip access-group
```

```
ip access-list
```

```
permit
```

```
show ip access-list
```

**45.2.2 ip access-group****Syntax**

To control and access an interface, run `ip access-group`. To delete the designated access group, run `no ip access-group {access-list-name}{in | out}`.

```
ip access-group {access-list-name}{in | out}
```

```
no ip access-group {access-list-name}{in | out}
```

**Parameters**

Parameters	Description
<i>access-list-name</i>	<b>Stands for the name of an access control list. This is a character string with up to 20 characters.</b>
<i>In</i>	<b>Uses the access control list on the incoming interface.</b>
<i>out</i>	<b>Uses the access control list on the outgoing interface.</b>

**Command Mode**

Interface configuration mode

**Usage Guidelines**

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

For the standard access list of the out interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the expanded access control list, the switch will also check the access control list at the receiver terminal. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

If the designated access control list does not exist, all packets are allowed to pass through.

## Example

The following example shows how to apply the filter list on the egress port of Ethernet interface vlan1.

```
interface vlan 1
ip access-group filter out
```

## Related Command

**ip access-list**

**show ip access-list**

### 45.2.3 ip access-list

## Syntax

After this command is run, the system enters the IP ACL configuration mode. In this mode, you can add and delete the access regulations. You can run exit to return the configuration mode. You can run no ip access-list to delete the IP access control list.

**ip access-list {standard | extended} name**

**no ip access-list {standard | extended} name**

## Parameters

Parameters	Description
<i>standard</i>	Designates a standard access control list.
<i>extended</i>	Designates an extended access control list.
<i>name</i>	Stands for the name of an access control list. It is a character string with up to 20 characters.

## Default Value

No IP access control list is defined by default.

## Command Mode

Global configuration mode

## Usage Guidelines

This command is used to enter the IP ACL configuration mode and then you can use the deny command and the permit command to configure the access regulation.

## Example

The following example shows how to configure a standard IP access control list.

```
ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any
```

## Related Command

**deny****ip access-group****permit****show ip access-list****45.2.4 permit**

## Syntax

To configure the permit regulation in IP ACL configuration mode, run **permit**. To cancel the permit regulation, run **no permit**.

```
permit source [source-mask] [log] [location]
```

```
no permit source [source-mask] [log]
```

```
permit protocol source source-mask destination destination-mask [[precedence
precedence] [tos tos] [log] [offset-zero] [totalen] [time-range] [location] [t
ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-
zero] [log ]]
```

```
no permit protocol source source-mask destination destination-mask [[precedence
precedence] [tos tos] [log] [offset-zero] [totalen] [time-range] [location] [t
ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-
zero] [log ]]
```

For the Internet Control Message Protocol (ICMP), use the following command syntax.

```
permit icmp source source-mask destination destination-mask [icmp-type] [precedence
precedence] [tos tos] [log]
```

For the Internet Group Management Protocol (IGMP), run the following command syntax.

```
permit igmp source source-mask destination destination-mask [igmp-type] [precedence
precedence] [tos tos] [log]
```

For the Transmission Control Protocol (TCP), use the following command syntax.

```
permit tcp source source-mask [operator port] destination destination-mask [operator
port] [established] [precedence precedence] [tos tos] [log]
```

For the User Datagram Protocol (UDP), use the following command syntax.

```
permit udp source source-mask [operator port [port]] destination destination-mask
[operator port] [precedence precedence] [tos tos] [log]
```

## Parameters

Parameters	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be <b>icmp</b> , <b>igmp</b> , <b>igrp</b> , <b>ip</b> , <b>ospf</b> , <b>tcp</b> or <b>udp</b> , or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including

	ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
<i>source</i>	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>source-mask</i>	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>destination</i>	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
<i>destination-mask</i>	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
<i>precedence precedence</i>	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This parameter is optional.
<i>tos tos</i>	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
<i>icmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
<i>igmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
<i>operator</i>	((Optional) Compares the source or destination ports.) The operations include lt, gt, eq and neq. If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
<i>Port</i>	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535. The name of the TCP port is listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
<i>established</i>	An optional parameter for the TCP protocol, representing an established connection. If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
<i>log</i>	An optional parameter, meaning the logs can be recorded

## Command Mode

IP ACL configuration commands

## Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again.

The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's access path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

### Note:

After an access control list is originally established, (ny added content is) put at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Bgp, ftp, ftp-data, login, pop2, pop3, smtp, telnet, www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Domain, snmp, syslog, tftp

## Example

The following example shows how to allow network segment 192.168.5.0.

```
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
```

### Note:

The IP access control list deny ends with a connotative deny regulation.

## Related Command

**deny**

**ip access-group**

**ip access-list**

**show ip access-list**

*45.2.5 show ip access-list*

## Syntax

To display the content of the current IP access control list, run the following command.

```
show ip access-list [access-list-name]
```

### Parameters

Parameters	Description
<i>access-list-name</i>	<b>Stands for the name of an access control list. It is a character string with up to 20 characters.</b>

### Default Value

This command is used to display all standard and extended IP access control lists.

### Command Mode

EXEC

### Usage Guidelines

The command helps you to designate a specific access control list.

### Example

The following information is displayed when the show ip access-list command is run in case an IP access control list is designated.

```
Switch# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

The following information is displayed when the show ip access-lists bbb command is run in case that an access control list is designated.

```
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

### **45.3 IP ACL based on physical port**

The commands for configuring the IP Access Control List (ACL) are:

- deny
- ip access-group
- ip access-list
- permit



- show ip access-list

### 45.3.1 deny

#### Syntax

To configure the deny regulations in IP ACL configuration mode, run `deny source [source-mask] or deny protocol source source-mask destination destination-mask [tos tos]`. To remove a deny regulation from an IP ACL, run `no deny source [source-mask] or no deny protocol source source-mask destination destination-mask [tos tos]`.

**deny source** [*source-mask*] [**log**] [**location**]

**no deny source** [*source-mask*] [**log**]

**deny protocol source source-mask destination destination-mask** [[**precedence** precedence] [**tos** tos] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

**no deny protocol source source-mask destination destination-mask** [[**precedence** precedence] [**tos** tos ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

For the Internet Control Message Protocol (ICMP), use the following command syntax.

**deny icmp** source source-mask destination destination-mask [*icmp-type*] [**tos** tos]

For the Internet Group Management Protocol (IGMP), run the following command syntax.

**deny igmp** source source-mask destination destination-mask [*igmp-type*] [**tos** tos] For the Transmission Control Protocol (TCP), use the following command syntax.

**deny tcp** source source-mask [*operator port*] destination destination-mask [*operator port*] [**tos** tos]

For the User Datagram Protocol (UDP), use the following command syntax.

**deny udp** source source-mask [*operator port*] destination destination-mask [*operator port*] [**tos** tos]

#### Parameters

Parameters	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igmp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
<i>source</i>	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>source-mask</i>	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.

<i>destination</i>	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
<i>destination-mask</i>	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
<i>tos tos</i>	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
<i>icmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
<i>igmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
<i>operator</i>	((Optional) Compares the source or destination ports.) The operations include eq, gt, lt and portrange. If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
<i>Port</i>	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535.

## Command Mode

IP ACL configuration commands

## Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again. The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's access path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

### Note:

After an access control list is originally established,(ny added content is)put at the end of the list.

## Example

The following example shows how to forbid network segment 192.168.5.0.

```
ip access-list standard filter
```

```
deny 192.168.5.0 255.255.255.0
```

**Note:**

The IPaccess control listdenyends with a connotative deny regulation.

**Related Command**

**ip access-group**

**ip access-list**

**permit**

**show ip access-list**

**45.3.2 ip access-group****Syntax**

To control and access an interface, run `ip access-group {access-list-name}{in | out}`. To delete the designated access group, run `no ip access-group {access-list-name}{in | out}`.

**[no] ip access-group** [*access-list-name*]

**Parameters**

Parameters	Description
<i>access-list-name</i>	<b>Stands for the name of an access control list. This is a character string with up to 20 characters.</b>

**Command Mode**

Interface configuration mode

**Usage Guidelines**

The access control list is used on the incoming interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

If the designated access control list does not exist, all packets are allowed to pass through.

**Example**

The following example shows how to apply the filter list on the ingress port of Ethernet interface g0/10:

```
interface g0/10
```

```
ip access-group filter
```

**Related Command**

**ip access-list**

**show ip access-list**

### 45.3.3 *ip access-list*

#### Syntax

After this command is run, the system enters the IP ACL configuration mode. In this mode, you can add and delete the access regulations. You can run `exit` to return the configuration mode. You can run `no ip access-list` to delete the IP access control list.

**ip access-list** {standard | extended} *name*

**no ip access-list** {standard | extended} *name*

#### Parameters

Parameters	Description
<i>standard</i>	Designates a standard access control list.
<i>extended</i>	Designates an extended access control list.
<i>name</i>	Stands for the name of an access control list. It is a character string with up to 20 characters.

#### Default Value

No IP access control list is defined by default.

#### Command Mode

Global configuration mode

#### Usage Guidelines

This command is used to enter the IP ACL configuration mode and then you can use the `deny` command and the `permit` command to configure the access regulation.

#### Example

The following example shows how to configure a standard IP access control list.

```
ip access-list standard filter
```

```
deny 192.168.1.0 255.255.255.0
```

```
permit any
```

#### Related Command

**deny**

**ip access-group**

**permit**

**show ip access-list**

### 45.3.4 *permit*

#### Syntax

To configure the permit regulations in IP ACL configuration mode, run `permit`. To cancel the permit regulations, run `no permit`.

**permit source** [*source-mask*] [**log**] [**location**]

**no permit source** [*source-mask*] [**log**]

**permit protocol source** *source-mask* **destination** *destination-mask* [[**precedence** *precedence*] [**tos** *tos*] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log**]]

**no permit protocol source** *source-mask* **destination** *destination-mask* [[**precedence** *precedence*] [**tos** *tos*] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log**]]

For the Internet Control Message Protocol (ICMP), use the following command syntax.

**permit icmp source** *source-mask* **destination** *destination-mask* [*icmp-type*] [**tos** *tos*]

For the Internet Group Management Protocol (IGMP), run the following command syntax.

**permit igmp source** *source-mask* **destination** *destination-mask* [*igmp-type*] [**tos** *tos*]

For the Transmission Control Protocol (TCP), use the following command syntax.

**permit tcp source** *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**tos** *tos*]

For the User Datagram Protocol (UDP), use the following command syntax.

**permit udp source** *source-mask* [**operator** *port* [*port*]] **destination** *destination-mask* [**tos** *tos*]

## Parameters

Parameters	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be <code>icmp</code> , <code>igmp</code> , <code>igrp</code> , <code>ip</code> , <code>ospf</code> , <code>tcp</code> or <code>udp</code> , or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the <code>ip</code> keyword. Some protocols allow further limitations as described below.
<i>source</i>	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword <code>any</code> is used as the shortened forms of the source and the source mask of <code>0.0.0.0 0.0.0.0</code> .
<i>source-mask</i>	Stands for the source address of the network mask. The keyword <code>any</code> is used as the shortened forms of the source and the source mask of <code>0.0.0.0 0.0.0.0</code> .
<i>destination</i>	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword <code>any</code> is used as the shortened forms of the destination and the destination mask of <code>0.0.0.0 0.0.0.0</code> .

<i>destination-mask</i>	Stands for the destination address of the network mask. The keyword <b>any</b> is used as the shortened forms of the destination address and the destination mask of <b>0.0.0.0 0.0.0.0</b> .
<i>tos tos</i>	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
<i>icmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
<i>igmp-type</i>	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
<i>operator</i>	((Optional) Compares the source or destination ports.) The operations include <b>eq, gt, lt</b> and <b>portrange</b> . If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
<i>Port</i>	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535.

## Command Mode

### IP ACL configuration commands Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the match-up occurs, the expanded access control list will not be checked again.

The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's access path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

#### Note:

After an access control list is originally established, (ny added content is) put at the end of the list.

#### Example

The following example shows how to allow network segment 192.168.5.0.

```
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
```

#### Note:

The IP access control list deny ends with a connotative deny regulation.

#### Related Command

**deny**

**ip access-group****ip access-list****show ip access-list**

### 45.3.5 show ip access-list

#### Syntax

To display the content of the current IP access control list, run the following command.

```
show ip access-lists [access-list-name [config-list | merge-list | both-list]]
```

#### Parameters

Parameters	Description
<i>access-list-name</i>	Stands for the name of an access control list. It is a character string with up to 20 characters.
<i>config-list</i>	Displays the original config list.
<i>merge-list</i>	Displays the merge list.
<i>both-list</i>	Displays the config list and the merge list.

#### Default Value

This command is used to display all standard and extended IP access control lists.

#### Command Mode

EXEC

#### Usage Guidelines

The command helps you to designate a specific access control list.

#### Example

The following information is displayed when the show ip access-list command is run in case an IP access control list is designated.

```
Switch# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```

The following information is displayed when the show ip access-lists bbb command is run in case that an access control list is designated.

```
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```

## Chapter 46 IP ACL Application Configuration Commands

### 46.1 IP ACL Application Configuration Commands

IP ACL Application Configuration Commands include:

- ip access-group
- ipv6 access-group

#### 46.1.1 ip access-group

To control and access an interface, run ip access-group. To cancel the designated access group, run no ipv6 access-group.

Use it on the interface

**[no] ip access-group *name***

To apply the established IP access list to an interface or in the global mode or cancel a IP access list which is already applied to an interface or in the global mode, run the following command.

Use it in the global mode

**[no] ip access-group *name* [vlan {*word* | add *word* | remove *word*}]**

Parameters

Parameters	Description
<i>name</i>	Name of the IP access control list
<i>Vlan</i>	THE ACCESS LIST IS APPLIED IN INGRESS.
<i>Word</i>	VLAN RANGE TABLE
<i>add</i>	ADD VLAN RANGE TABLE
<i>remove</i>	DELETE VLAN RANGE TABLE

Command Mode

Global configuration mode or interface configuration mode

Usage Guidelines

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

**Note:**

The IPv4 standard ACL supports the following rules:

any: means any source IP address.



source-addr source-mask : means matching up the source address.

reverse-mask source-addr source-mask: means to use the reverse source address for match-up.

The IPv4 extended ACL supports the following rules:

any: means any IP address.

ip-protocol: means the IP protocol ID. ip –IP protocol

reverse-mask: means the reverse configuration of varied protocols eq/gt/lt/src-portrange/

dst-portrange: means TCP/UDP port ID match-up. gre: GRE protocol ID match-up

icmp: ICMP protocol ID match-up icmp: IGMP protocol ID match-up

ospf: OSPF routing protocol ID match-up

Though tcp/udp port ID can enable the source port ID match-up and the destination port ID simultaneously, only the destination port ID match-up takes effect. Here is an exception when the match-up is configured to eq. In such case, the source port ID match-up and the destination port ID match-up takes effect simultaneously.

### Example

The following example shows how to apply the ACL filter at the ingress direction of interface g0/1.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1# ip access-group filter
```

#### 46.1.2 ipv6 access-group

To designate an access group, run the ipv6 access-group. To cancel the designated access group, run no ipv6 access-group.

Use it on the interface

**[no] ipv6 access-group name**

Use it in the global mode

To apply or delete a created IPv6 ACL on a port or in global mode, run this command.

**[no] ipv6 access-group name [vlan {word | add word | remove word}]**

#### Parameters

Parameters	Description
<i>name</i>	Name of the ip access control list
<i>vlan</i>	The access list is applied in ingress.
<i>word</i>	vlan range table
<i>add</i>	Add vlan range table
<i>remove</i>	Delete vlan range table

## Command Mode

Global configuration mode or interface configuration mode

## Usage Guidelines

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

### Note:

The IPv6 ACL supports the following rules:

any: means any IP address.

IPv6-addr/ host IPv6-addr : means IPv6 address match-up. ip-protocol: means the IPv6 protocol ID.

eq/gt/lt/src-portrange/ dst-portrange: means TCP/UDP port ID match-up.

dscp/flow-label: means field match-up.

Though tcp/udp port ID can enable the source port ID match-up and the destination port ID simultaneously, only the destination port ID match-up takes effect. Here is an exception when the match-up is configured to eq. In such case, the source port ID match-up and the destination port ID match-up takes effect simultaneously.

## Example

The following example shows how to apply the ACL filter at the ingress direction of interface g0/1.

```
Switch_config#inter g0/1
```

```
Switch_config_g0/1# ipv6 access-group filter
```

## Chapter 47 IPv6 Configuration Commands

### 47.1 IPv6 Configuration Commands

IPv6 configuration commands include:

- `ipv6 address`
- `ipv6 address anycast`
- `ipv6 address autoconfig`
- `ipv6 address eui-64`
- `ipv6 address link-local`
- `ipv6 enable`
- `show ipv6 interface`

#### 47.1.1 `ipv6 address`

##### Syntax

To set an IPv6 address in port configuration mode and meanwhile enable IPv6 on a port, run `ipv6 address { ipv6-address/prefix-length | general-prefix prefix-name sub-bits/prefix-length }`. To delete the IPv6 address on a port, run `no ipv6 address [ ipv6-address/prefix-length | general-prefix prefix-name sub-bits/prefix-length ]`.

**ipv6 address** { *ipv6-address/prefix-length* | **general-prefix** *prefix-name sub-bits/prefix-length* }

**no ipv6 address** [ *ipv6-address/prefix-length* | **general-prefix** *prefix-name sub-bits/prefix-length* ]

##### Parameters

Parameters	Description
<i>ipv6-address</i>	Means the to-be-added IPv6 address.
<i>/prefix-length</i>	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.
<i>Prefix-name</i>	Means a general prefix, defining the network part of the IPv6 address.
<i>Sub-bits</i>	Means the host part of the IPv6 address. It combines with the prefix, which is defined by <i>prefix-name</i> , to form an IPv6 address. This parameter must support the IPv6 address format regulated in RFC2373.

##### Default Value

No default IPv6 address exists on the VLAN port.

##### Command Mode

VLAN interface configuration mode

## Usage Guidelines

If you run `no ipv6 address`, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted.

## Example

The following example shows how to set an IPv6 address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port.

```
Switch_config_v1# ipv6 address 2001:0:0:0:0DB8:800:200C:417A/64
```

## Related Command

**ipv6 address anycast**

**ipv6 address eui-64**

**ipv6 address link-local**

**show ipv6 interface**

### 47.1.2 ipv6 address anycast

## Syntax

To set an anycast address, run `ipv6 address ipv6-prefix/prefix-length anycast` in interface configuration command. Meanwhile, the command can enable IPv6 protocol of the VLAN interface. To delete an anycast address, run `no ipv6 address [ ipv6-prefix/prefix-length anycast ]`.

**ipv6 address *ipv6-prefix/prefix-length* anycast**

**no ipv6 address [ *ipv6-prefix/prefix-length* anycast ]**

## Parameters

Parameters	Description
<i>ipv6-prefix</i>	Means the network part of the IPv6 address.
<i>/prefix-length</i>	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

## Default Value

The command is used to set as an anycast address on the VLAN port by default.

## Command Mode

VLAN interface configuration mode

## Usage Guidelines

If you run `no ipv6 address`, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted.

## Example

```
Switch_config_v1# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

### Related Command

**ipv6 address eui-64**

**ipv6 address link-local**

**show ipv6 interface**

### 47.1.3 ipv6 address autoconfig

#### Syntax

To use the stateless auto-configuration protocol to set an IPv6 address, run `ipv6 address autoconfig` in VLAN port configuration mode. Meanwhile, the command can enable IPv6 protocol of the VLAN interface. To delete the automatically configured address, run `no ipv6 address autoconfig`.

**ipv6 address autoconfig**

**no ipv6 address autoconfig**

#### Parameters

None

#### Default Value

By default, IPv6 address auto-configuration is not used.

#### Command Mode

VLAN interface configuration mode

#### Example

```
Switch_config_v1# ipv6 address autoconfig
```

### 47.1.4 ipv6 address eui-64

#### Syntax

To set an IPv6 address in VLAN port configuration mode, run `ipv6 address eui-64`. Meanwhile, the command can enable IPv6 protocol of the VLAN interface. To delete the configuration, run `no ipv6 address eui-64`.

**ipv6 address *ipv6-prefix/prefix-length* eui-64**

**no ipv6 address [ *ipv6-prefix/prefix-length* eui-64 ]**

#### Parameters

Parameters	Description
<i>ipv6-prefix</i>	Means the network part of the IPv6 address.
<i>/prefix-length</i>	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address.

## Default Value

The IPv6 address in the eui-64 form is not configured on the VLAN port.

## Command Mode

VLAN interface configuration mode

## Usage Guidelines

If you run no ipv6 address, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted.

If the prefix-length parameter is bigger than 64 bits, the prefix-length is prior to the length of the VLAN port ID.

## Example

```
Switch_config_v1# ipv6 address 2001:0:0:0:0DB8::/64 eui-64
```

## Related Command

```
ipv6 address link-local
```

```
show ipv6 interface
```

### 47.1.5 ipv6 address link-local

## Syntax

To set a link-local address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port, run the first one of the following two commands: To delete link-local address, run no ipv6 address [ ipv6-address link-local ].

```
ipv6 address ipv6-address link-local
```

```
no ipv6 address [ ipv6-address link-local ]
```

## Parameters

Parameters	Description
<i>ipv6-address</i>	<b>Means the to-be-added IPv6 address. The format of this address must abide by the definition in RFC 4291 strictly.</b>
<i>link-local</i>	<b>Means a link-local address. The link-local address designated by the ipv6-address command will automatically replace the configured link-local address.</b>

## Default Value

No default IPv6 link-local address exists on the VLAN port.

## Command Mode

VLAN interface configuration mode

## Usage Guidelines

If you run `no ipv6 address`, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted. If you run `ipv6 enable`, a link-local address will be automatically set. Of course you can set the link-local address manually, the command you will use is `ipv6 address link-local`.

### Example

The following example shows how to set a link-local address manually on the VLAN port:

```
Switch_config_v1# ipv6 address FE80::A00:3EFF:FE12:3457 link-local
```

### Related Command

**ipv6 address eui-64**

**show ipv6 interface**

### 47.1.6 *ipv6 enable*

#### Syntax

If the IPv6 address is not set on the VLAN port but users want to enable the IPv6 protocol on this port, run `ipv6 enable`. To disable IPv6, run `no ipv6 enable`.

**ipv6 enable**

**no ipv6 enable**

#### Parameters

None

#### Default Value

The IPv6 protocol is forbidden on the VLAN port.

#### Command Mode

VLAN interface configuration mode

#### Usage Guidelines

After the `ipv6 enable` command is run, the system will add a link-local address on the VLAN port automatically. At the same time, the communication range of the IPv6 protocol on the VLAN port is confined to the links that the VLAN port connects. If the IPv6 address has already configured on the VLAN port explicitly, you cannot forbid IPv6 processing on the VLAN port even though you use the `no ipv6 enable` command.

### Example

```
Switch_config# interface vlan 1
```

```
Switch_config_v1# ipv6 enable
```

### Related Command

**ipv6 address link-local**

**ipv6 address eui-64**

**show ipv6 interface***47.1.7 show ipv6 interface***Syntax**

To show the information about the VLAN port on which the IPv6 protocol is enabled, run the following command:

**show ipv6 interface** [ *interface-type interface-number* ] | [ **brief** ]

**Parameters**

Parameters	Description
<i>interface-type</i>	<b>Stands for the type of the VLAN interface port.</b>
<i>interface-number</i>	<b>Stands for the ID of the VLAN port.</b>

**Default Value**

Those VLAN ports on which the IPv6 protocol is enabled will all be displayed.

**Command Mode**

Global configuration mode

**Usage Guidelines**

This command can be used to display the state of IPv6 on the VLAN port, the configured IPv6 address and other IPv6 related parameters.

**Example**

The following example shows how to display the IPv6 state on port vlan1:

```
Switch# show ipv6 interface vlan 1
```

```
Vlan1 is up, line protocol is down
```

```
IPv6 is enabled, link-local address is FE80::A00:3EFF:FE12:3457 [TENTATIVE]
```

```
Global unicast address(es):
```

```
5678::111, subnet is 5678::/64 [TENTATIVE]
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::2
```

```
FF02::1:FF12:3457
```

```
FF02::1:FF00:111
```

```
MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled
```

```
ICMP unreachable are enabled
```



Field	Description
<i>Vlan1 is up(down/administratively down)</i>	Indicates whether the physical layer of the VLAN port is accessible or whether it can be shut down manageably.
<i>line protocol is up(down)</i>	Indicates whether the line protocol (the software layer) is accessible.
<i>IPv6 is enabled</i>	Enables the IPv6 protocol.
<i>link-local address</i>	Displays the link-local address of a port.
<i>Global unicast address(es):</i>	Displays the unicast address of a port.
<i>Joined group address(es)</i>	Displays the multicast address of a port.
<i>MTU</i>	Displays the MTU of a port.
<i>ICMP error messages</i>	Displays the transmission frequency of ICMPv6 error packets (the minimum interval).
<i>ICMP redirects</i>	Displays whether the redirection packet will be sent or not.
<i>ICMP unreachable</i>	Displays whether the destination unreachable packet will be enabled or shut down.

#### Related Command

None

## Chapter 48 IPv6 Configuration Commands

### 48.1 IPv6 Configuration Commands

IPv6 configuration commands include the following ones:

- clear ipv6 traffic
- debug ipv6 packet
- ipv6 mtu
- ipv6 redirect
- ipv6 access-group
- ipv6 unreachable
- ipv6 route default
- show ipv6 general-prefix
- show ipv6 pmtu
- show ipv6 traffic

#### 48.1.1 clear ipv6 traffic

##### Syntax

To delete the statistics information about the IPv6 flow, run the following command:

**clear ipv6 traffic****Parameters**

None

**Command Mode**

EXEC

**Usage Guidelines**

This command is used to delete all the statistics information about IPv6 flow.

**Example**

The following example shows how to delete the statistics information about IPv6 flow:

```
Switch# clear ipv6 traffic
```

```
Switch# show ipv6 traffic
```

```
IPv6 statistics:
```

```
Rcvd: 0 total, 0 local destination
```

```
    0 badhdrs, 0 badvers
```

```
    0 tooshort, 0 toosmall, 0 toomanyhdrs
```

```
    0 source-routed, 0 badscope
```

```
    0 badopts, 0 unknowopts, 0 exthdrtoolong
```

```
    0 fragments, 0 total reassembled
```

```
    0 reassembly timeouts, 0 reassembly failures
```

```
Sent: 0 generated, 0 forwarded, 0 cant forwarded
```

```
    0 fragmented into 0 fragments, 0 failed
```

```
    0 no route
```

```
Mcast: 0 received, 0 sent
```

```
ICMP statistics:
```

```
Rcvd: 0 total, 0 format errors, 0 checksum errors
```

```
    0 unreachable, 0 packet too big
```

```
    0 time exceeded, 0 parameter problem
```

```
    0 echos, 0 echo replies
```

```
    0 membership query, 0 membership report, 0 membership reduction
```

```
    0 Switch solicitations, 0 Switch advertisements
```

```
    0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
```

Sent: 0 total, 0 bandwidth limit

0 unreachable, 0 packet too big

0 time exceeded, 0 parameter problem

0 echos, 0 echo replies

0 membership query, 0 membership report, 0 membership reduction

0 Switch solicitations, 0 Switch advertisements

0 neighbor solicitations, 0 neighbor advertisements, 0 redirect

## Related Command

**show ipv6 traffic**

### 48.1.2 debug ipv6 packet

#### Syntax

To display the debug information about the IPv6 packet, run the first one of the following two commands: To disable the input of debug information, run `no debug ipv6 packet`.

**debug ipv6 packet** [ **interface** *interface-type interface-number* | **access-list**

[ *access-list-name* ] | **detail** ]

**no debug ipv6 packet**

#### Parameters

Parameters	Description
<i>Interface-type</i>	<b>(Optional)</b> The type of the VLAN port.
<i>Interface-number</i>	<b>ID of an interface (optional)</b>
<i>access-list-name</i>	<b>Name of ACL (optional)</b>

#### Default Value

The debug information is closed in default state.

#### Command Mode

EXEC

#### Example

The following example shows how to export the IPv6 debug information:

```
Switch# debug ipv6 packet
```

```
2002-1-1 05:07:16
```

```
IPv6: source FE80::A00:3EFF:FE12:3459, dest FF02::1
```

```
    plen 32, proto 58, hops 255
```

sending on Ethernet1/0

Field	Description
<i>source</i>	Source address in the IPv6 packet
<i>dest</i>	Destination address in the IPv6 packet
<i>plen</i>	Load length in the IPv6 packet
<i>proto</i>	Protocol for the next header encapsulation, which is presented by next-header in the IPv6 packet
<i>hops</i>	Value of hop-limit in the IPv6 packet
<i>sending (receiving , forwarding ) on Ethernet</i>	Displays packet transmission, reception and forwarding on an interface

### 48.1.3 ipv6 mtu

#### Syntax

To set the MTU of the VLAN port, run the first one of the following two commands: To return to the default setting, run `no ipv6 mtu`.

`ipv6 mtu bytes`

`no ipv6 mtu`

#### Parameters

Parameters	Description
<i>bytes</i>	Stands for MTU, whose unit is byte.

#### Default Value

The default value depends on the port type, but the minimum value of any port is 1280 bytes.

#### Command Mode

VLAN interface configuration mode

#### Usage Guidelines

When MTU is the default value, RA has the MTU option.

When a switch forwards packet, a packet will not be fragmented just because the MTU of the egress is smaller than the packet's length. But it will be fragmented only when the transmitted packet is generated.

#### Example

The following example shows how to set the MTU of a port:

```
Switch_config_v1# ipv6 mtu 1400
```

#### Related Command

```
show ipv6 interface
```

#### 48.1.4 ipv6 redirects

##### Syntax

To control whether to transmit a redirection packet after the packet is forwarded, run `ipv6 redirects`. To return to the default setting, use `no ipv6 redirects`.

##### ipv6 redirects

##### no ipv6 redirects

##### Parameters

None

##### Default Value

The redirection packet will be transmitted by default.

##### Command Mode

VLAN interface configuration mode

##### Usage Guidelines

The redirection packets are transmitted through the ICMPv6 protocol.

##### Example

The following example shows how to shut down a port to transmit the redirection packet.

```
Switch_config_v1# no ipv6 redirects
```

To observe whether redirection packets are forwarded, run command `show ipv6 interface`.

##### Related Command

```
show ipv6 interface
```

#### 48.1.5 ipv6 access-group

##### Syntax

To filter the receiving and forwarding packets of a port, run `ipv6 access-group`. To disable the function, run `no ipv6 access-group`.

```
ipv6 access-group access-list-name { in | out }
```

```
no ipv6 access-group { in | out }
```

##### Parameters

Parameters	Description
<i>access-list-name</i>	access list name
<i>In</i>	filtration direction, receiving packet
<i>Out</i>	filtration direction, forwarding packet

### Default Value

Filtration function is not configured by default.

### Command Mode

VLAN interface configuration mode

### Usage Guidelines

### Example

The following example shows how to use access list test to filter received packet on interface vlan 1.

```
Switch_config_v1# ipv6 access-group test in
```

### Related Command

Ipv6 access-list

Show ipv6 interface

### *48.1.6 ipv6 unreachable*

#### Syntax

To enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface, use the `ipv6 unreachable` command in interface configuration mode. To prevent the generation of unreachable messages, use the `no` form of this command.

**ipv6 unreachable**

**no ipv6 unreachable**

#### Parameters

None

#### Default Value

Allows IPv6 to transmit the destination unreachable packets.

#### Command Mode

VLAN interface configuration mode

#### Usage Guidelines

The destination unreachable packets are forwarded by ICMPv6 protocol.

#### Example

The following example shows how to shut down the VLAN port to transmit the redirection packet.

```
Switch_config_v1# no ipv6 unreachable
```

To observe whether destination unreachable packets are forwarded, run command `show ipv6 interface`.

#### Related Command

None

#### 48.1.7 *ipv6 route default*

##### Syntax

To set the default ipv6 gateway of the switch, run this command.

```
ipv6 route default [NULL | X:X:X:X::X]
```

```
no ipv6 route default [NULL | X:X:X:X::X]
```

##### Parameters

Parameters	Description
<i>NULL</i>	<b>NULL interface</b>
<i>X:X:X:X::X</i>	<b>Gateway's address</b>

##### Default Value

There is no default configuration.

##### Command Mode

Global configuration mode

##### Example

The following example shows how to set the address of 2008::1 to the route default of the switch.

```
route default
```

```
ipv6 route default 2008::1
```

##### Related Command

None

#### 48.1.8 *show ipv6 general-prefix*

##### Syntax

To show details of general-prefix, run the following command:

```
show ipv6 general-prefix
```

##### Parameters

None

## Command Mode

EXEC

## Example

```
Switch_config#show ipv6 general-prefix
```

IPv6 Prefix my-prefix, acquired via manual

2002::/64

Vlan1 (Address command)

Field	Usage Guidelines
<i>IPv6 Prefix</i>	User-defined IPv6 general prefix
<i>Acquire via</i>	Configuration mode of general-prefix Manual configuration and DHCP automatic acquisition are supported now.
<i>Vlan1 (Address command)</i>	Stands for a list of ports that use this general prefix.

## Related Command

**ipv6 general-prefix**

### 48.1.9 show ipv6 pmtu

## Syntax

IPv6 router supports path MTU (Refer to RFC 1981). To show MTU buffer item, run show ipv6 pmtu.

```
show ipv6 pmtu
```

## Parameters

None

## Command Mode

EXEC

## Example

```
Switch_config#show ipv6 pmtu
```

```

PMTU      Expired      Destination  Address
1300      00:04:00      2002:1::1
1280      12:01:00 AM   2001:2::2

```

Path MTU buffer saves the destination address used by path MTU. The forwarding packet will be fragmented if the forwarded packet of all switches greater than path MTU.

A record of path MTU will be created when the switch receives ICMPv6 "too-big" packet.



Field	Usage Guidelines
<i>MTU</i>	Path MTU value MTU included in ICMPv6 "too-big" packet
<i>Expired</i>	Timeout: Timer from receiving ICMPv6 "too-big" packet. Delete the record when expired is 0.
<i>Destination Address</i>	Destination address Address included in ICMPv6 "too-big" packet

## Related Command

### ipv6 mtu

#### 48.1.10 show ipv6 traffic

### Syntax

To show statistics about IPv6 traffic, use the show ipv6 traffic command.

### show ipv6 traffic

### Parameters

None

### Command Mode

EXEC

### Example

```
Switch#show ipv6 traffic
```

IPv6 statistics:

```
Rcvd: 0 total, 0 local destination
      0 badhdrs, 0 badvers
      0 tooshort, 0 toosmall, 0 toomanyhdrs
      0 source-routed, 0 badscope
      0 badopts, 0 unknowopts, 0 exthdrtoolong
      0 fragments, 0 total reassembled
      0 reassembly timeouts, 0 reassembly failures
Sent: 25 generated, 0 forwarded, 0 cant forwarded
      0 fragmented into 0 fragments, 0 failed
      0 no route
```

```
Mcast: 0 received, 25 sent
```

ICMP statistics:

Rcvd: 25 total, 0 format errors, 0 checksum errors

0 unreachable, 0 packet too big

0 time exceeded, 0 parameter problem

0 echos, 0 echo replies

0 membership query, 0 membership report, 0 membership reduction

0 Switch solicitations, 0 Switch advertisements

0 neighbor solicitations, 0 neighbor advertisements, 0 redirect

Sent: 0 total, 0 bandwidth limit

0 unreachable, 0 packet too big

0 time exceeded, 0 parameter problem

0 echos, 0 echo replies

0 membership query, 0 membership report, 0 membership reduction

0 Switch solicitations, 0 Switch advertisements

0 neighbor solicitations, 0 neighbor advertisements, 0 redirect

## Related Command

`clear ipv6 traffic`

## 48.2 Network Testing Tool Commands

IPv6 Network Testing Tool Commands

- ping6
- traceroute6

### 48.2.1 ping6

#### Syntax

To test host accessibility and network connectivity, run the following command. After the ping command is run, an ICMP request message is sent to the destination host, and then the destination host returns an ICMP response message.

`ping6 host [-a] [-l length] [-n number] [-v] [-w waittime] [-b internal]`

#### Parameters

Parameters	Description
<i>host</i>	The destination host address or the host name
<i>-a</i>	icmp echo request packets are forwarded continuously until the user stops it manually.
<i>-l length</i>	Sets the length of ICMP data in the message. Default: 56 bytes
<i>-n number</i>	Sets the total number of messages. Default: 5 messages

<i>-w waittime</i>	<b>Time for each message to wait for response Default: 2 seconds</b>
<i>-b interval</i>	<b>Sets the time interval of sending ping packet. Unit: 10ms; Value range: 0-65535; Default Value: 0.</b>

## Command Mode

EXEC and global configuration mode

## Usage Guidelines

Press the Q key to stop the ping command.

Simple output is adopted by default.

Parameters	Description
!	<b>A response message is received.</b>
.	<b>Response message is not received in the timeout time.</b>
U	<b>The message that the ICMP destination cannot be reached is received.</b>
R	<b>The ICMP redirection message is received.</b>
T	<b>The ICMP timeout message is received.</b>
P	<b>The ICMP parameter problem message is received.</b>

The statistics information is exported:

Parameters	Description
<i>packets transmitted</i>	<b>Number of transmitted messages</b>
<i>packets received</i>	<b>Number of received response messages, excluding other ICMPmessages</b>
<i>packet loss</i>	<b>Rate of messages that are not responded to</b>
<i>round-trip min/avg/max</i>	<b>Minimum/average/maximum time of a round trip (ms)</b>

The routing switch supports the destination address to be link-local address or the multicast address. When ping this address, the vlan port must be specified at the end and forward ICMP packets on the specified port. The routing switch is to export the addresses of all response hosts.

## Example

```
switch#ping6 2008::2 -l 10000 -n 30
```

```
PING 2008::2 (2008::2): 10000 data bytes
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
--- 2008::2 ping6 statistics ---
```

```
30 packets transmitted, 30 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0/1/20 ms
```

```
· ping multicast address :
```

```
switch#ping6 ff02::1 vlan 1 -n 2
```

```
PING 1 (FF02:1B::1): 56 data bytes
```

```
Reply to request 0 from FE80::2E0:FFF:FEDB:583F, <10 ms
```

```
Reply to request 0 from FE80::1EAF:F7FF:FE35:D02A, 10 ms
```

```
Reply to request 1 from FE80::2E0:FFF:FEDB:583F, <10 ms
```

```
Reply to request 1 from FE80::1EAF:F7FF:FE35:D02A, 10 ms
```

### 48.2.2 traceroute6

#### Syntax

To detect which routes have already reached the destination, run the following command.

You can transmit to the destination the UDP packets (or ICMP ECHO packets) of different TTLs to confirm which routes have come to the destination. Each router on this path has to deduct 1 from the TTL value before forwarding ICMP ECHO packets. Speaking from this aspect, TTL is an effective hop count. When the TTL value of a packet is deducted to zero, the router sends back to the source system the ICMP timeout message. Send the first response packet whose TTL is 1 and send TTL plus 1 subsequently until the target reaches to the max TTL.

By checking the ICMP timeout message sent back by inter medial routers, you can confirm the routers. At the arrival of the destination, the traceroute sends a UDP packet whose port ID is larger than 30000; the destination node hence can only transmit back a Port Unreachable ICMP message. This reception of this message means the arrival of destination.

```
traceroute6 host [-i source-ip-address] [-p port-number] [-q probe-count] [-t ttl] [-w waittime] [-x icmp]
```

#### Parameters

Parameters	Description
<i>host</i>	The destination host address or the host name
<i>-i source-ip-address</i>	Sets the source address.
<i>-p port-number]</i>	Sets the ID of destination port that transmits UDP packets. Default value: 33434 Default: 33434
<i>-q probe-count</i>	Sets the number of packets that you detect each time. Default: 3 messages
<i>-t ttl</i>	Sets IP TTL of the message to ttl. Default: the minimum and maximum TTLs are 1 and 30 respectively.
<i>-w waittime</i>	Time for each message to wait for response Default: 3 seconds
<i>-x icmp</i>	Sets the detection packet to be the ICMP ECHO packet. Default: UDP packet

#### Command Mode

EXEC and global configuration mode

### Usage Guidelines

The UDP packet is used for detection by default, but you can run `-x icmp` to replace it with ICMP ECHO for detection.

If you want to stop traceroute, press `q` or `Q`. By default, the simple output information is as follows.

Simple output is adopted by default.

Parameters	Description
<i>!N</i>	Receives ICMP destination unreachable packets (route unreachable, code: 0)
<i>!P</i>	Receives ICMP destination unreachable packets (management forbid, code: 1)
<i>!S</i>	Receives ICMP destination unreachable packets (not neighbor, code: 2)
<i>!A</i>	Receives ICMP destination unreachable packets (address unreachable, code: 3)
<i>!</i>	Receives ICMP destination unreachable packets (port unreachable, code: 4)

The statistics information is exported:

Parameters	Description
<i>hops max</i>	Means the maximum detection hops (the threshold of ICMP).
<i>byte datalen</i>	Stands for the size of each detection packet.

### Example

```
switch#traceroute6 2008::2
tracert6 to 2008::2 , 30 hops max, 12 byte datalen
1 2008::2 0 ms * 0 ms
```

## Chapter 49 MLD Multicast Configuration Commands

The MLD multicast configuration commands include:

- `ipv6 mld-snooping`
- `ipv6 mld-snooping solicitation`
- `ipv6 mld-snooping vlan vlan_id static X:X:X:X::X interface intf`
- `ipv6 mld-snooping timer router-age timer_value`
- `ipv6 mld-snooping timer response-time timer_value`
- `ipv6 mld-snooping vlan vlan_id mrouter interface inft_name`
- `ipv6 mld-snooping vlan vlan_id immediate-leave`
- `show ipv6 mld-snooping`
- `show ipv6 mld-snooping vlan vlan_id`
- `show ipv6 mld-snooping timer`
- `show ipv6 mld-snooping timer`
- `show ipv6 mld-snooping groups`
- `show ipv6 mld-snooping statistics`
- `show ipv6 mld-snooping mac`

### 49.1 *ipv6 mld-snooping*

#### Syntax

To enable MLD snooping, run `ipv6 mld-snooping`.

#### **ipv6 mld-snooping**

#### **ipv6 mld-snooping**

#### Parameters

None

#### Default Value

Enables MLD snooping multicast.

#### Usage Guidelines

After MLD snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the MLD-snooping), all multicast packets whose destination addresses are not registered on any port will be dropped.

#### Example

The following example shows how to enable the MLD snooping function:

```
switch_config# ipv6 mld-snooping
```

## 49.2 ipv6 mld-snooping solicitation

Syntax

**ipv6 mld-snooping solicitation**

**no ipv6 mld-snooping solicitation**

To enable or disable the hardware forwarding of the multicast group, run `ip mld-snooping solicitation`. To resume the default value, run `no ip mld-snooping solicitation`.

Parameters

None

Default Value

This function is shut down.

Usage Guidelines

None

Example

The following example shows how to enable the hardware forward of the multicast group.

```
switch_config#ipv6 mld-snooping solicitation
```

## 49.3 ipv6 mld-snooping vlan *vlan\_id* static *X:X:X:X::X* interface *intf\_name*

Syntax

**ipv6 mld-snooping vlan *vlan\_id* static *X:X:X:X::X* interface *intf\_name***

**no ipv6 mld-snooping vlan *vlan\_id* static *X:X:X:X::X* interface *intf\_name***

Parameters

Parameters	Description
<i>vlan id</i>	<b>Stands for the ID of a VLAN. Value range: 1-4094</b>
<i>X:X:X:X::X</i>	<b>IP address of the multicast</b>
<i>Intf_name</i>	<b>An interface</b>

Default Value

None

Usage Guidelines

This command is used to configure the static multicast address of VLAN. Its negative form is used to cancel the static multicast address.

Example

The following example shows how to add the static multicast address ff12::5 to port G0/1.

```
switch_config# ipv6 mld-snooping vlan 1 static ff12::5 interface g0/1
```

```
switch_config#
```

#### 49.4 *ipv6 mld-snooping timer router-age timer\_value*

Syntax

```
ipv6 mld-snooping timer router-age timer_value
```

```
no ipv6 mld-snooping timer router-age
```

Parameters

Parameters	Description
<i>time value</i>	Queries the time of the timer. Value range: 10-2147483647

Default Value

260 seconds

Usage Guidelines

This command is used to query the time of the timer of MLD-Snooping. The negative form of this command is used to resume the default value.

Example

The following example shows how to set the query time of the router to 300 seconds.

```
switch_config# ipv6 mld-snooping timer router-age 300
```

```
switch_config#
```

#### 49.5 *ipv6 mld-snooping timer response-time timer\_value*

Syntax

```
ipv6 mld-snooping timer response-time timer_value
```

```
no ipv6 mld-snooping timer response-time
```

To configure the maximum response time of IGMP snooping, run ip mld-snooping timer response-time *timer\_value*. To resume the default value of IGMP snooping, run no ip mld-snooping timer response-time *timer\_value*.

Parameters

Parameters	Description
<i>time value</i>	Queries the time of the timer. Value range: 10-2147483647

Default Value

10 seconds



## Usage Guidelines

None

## Example

The following example shows how to set the query response time of IGMP snooping to 20 seconds. `switch_config# ipv6 mld-snooping timer response-time 20`

### 49.6 *ipv6 mld-snooping querier*

#### Syntax

**ipv6 mld-snooping querier** [address <ip\_addr>]

**no ipv6 mld-snooping querier** [address]

To activate the mld-snooping querier mechanism, or set the source IP address of the automatic query packet, run `ip igmp-snooping querier [address <ip_addr>]`. To resume the default value, run `no ip igmp-snooping querier [address]`.

#### Parameters

Parameters	Description
<i>ip_addr</i>	IPv6 address of a normal unicast

#### Default Value

By default, the querier function is not enabled and the source IP address is FE80::3FF:FEFE:FD00:1.

## Usage Guidelines

None

## Example

The following example shows how to activate IGMP Querier to serve as a multicast router if no multicast router is working.

```
switch_config# ipv6 mld-snooping querier
```

```
switch_config#
```

### 49.7 *ipv6 mld-snooping vlan vlan\_id mrouter interface inft\_name*

#### Syntax

**ipv6 mld-snooping vlan** *vlan\_id* **mrouter** interface *inft\_name*

**no ipv6 mld-snooping vlan** *vlan\_id* **mrouter** interface *inft\_name*

To configure the port of the static multicast router of MLD snooping, run `ipv6 mld-snooping vlan vlan_id mrouter interface inft_name`.

#### Parameters

Parameters	Description
<i>vlan id</i>	Stands for the ID of a VLAN. Value range: 1-4094
<i>inft_name</i>	Shows the port type, the slot and the port ID.

#### Default Value

None

#### Usage Guidelines

None

#### Example

The following example shows how to set port G0/4 to the port of the static multicast router of MLD Snooping.

```
switch_config# ipv6 mld-snooping vlan 1 mrouter interface g0/4
```

### 49.8 *ipv6 mld-snooping vlan vlan\_id immediate-leave*

#### Syntax

```
ipv6 mld-snooping vlan vlan_id immediate-leave
```

```
no ipv6 mld-snooping vlan vlan_id immediate-leave
```

#### Parameters

Parameters	Description
<i>vlan id</i>	Stands for the ID of a VLAN. Value range: 1-4094

#### Default Value

The immediate-leave function is disabled.

#### Usage Guidelines

This command is used to set the immediate-leave function.

#### Example

The following example shows how to enable the immediate-leave functionality on VLAN 1:

```
switch_config# ipv6 mld-snooping vlan 1 immediate-leave
```

```
switch_config#
```

### 49.9 *show ipv6 mld-snooping*

#### Syntax

```
show ipv6 mld-snooping
```

#### Parameters

None

### Default Value

None

### Usage Guidelines

This command is used to display the information about MLD-snooping configuration.

### Example

The following example shows how to display the information about MLD snooping.

```
switch#show ipv6 mld-snooping
```

```
Global MLD snooping configuration:
```

```
-----  
Globally enable      : Enabled  
Querier              : Enabled  
Querier address: FE80::3FF:FEFE:FD00:1  
Router age: 260 s  
Response time: 10 s  
Handle Solicitation: Enabled  
Vlan 1:  
-----  
Running  
Routers: SWITCH(querier);  
Vlan 2:  
Running  
Routers: SWITCH(querier);  
Switch_config#show ipv6 mld-s g  
Vlan Group  Type Port(s)
```

```
-----  
1 FF02::1:FF13:647D MLD  G0/2  
1 FF02::1:FF13:394 MLD  G0/2  
2 FF02::1:FF00:2    MLD  G0/1  
1 FF02::1:FF00:12 MLD   G0/1  
1 FF02::1:FF00:2    MLD  G0/1
```

```
2 FF02::1:FF61:9901 MLD G0/2
```

```
switch#
```

### **49.10 show ipv6 mld-snooping vlan vlan\_id**

Syntax

```
show ipv6 mld-snooping vlan vlan_id
```

Parameters

Parameters	Description
<i>vlan id</i>	VLAN id. The value ranges from 1 to 4094.

Default Value

None

Usage Guidelines

The command is used to display the detailed information of MLD Snooping of specific vlan.

Example

The following example shows how to display the information about MLD snooping of specific vlan.

```
switch#show ipv6 mld-snooping vlan 1
```

```
Vlan 1:
```

```
-----
```

Running

```
Ports: g0/11 g0/12 g0/1 g0/13 g0/2 g0/14 g0/3 g0/4 g0/5 g0/6 g0/8 g0/9 g0/10
g0/16 g0/17 g0/18 g0/19 g0/20 g0/21 g0/22 g0/23 g0/24
```

Routers:

No querier, MLD snooping doesn't work on this vlan

### **49.11 show ipv6 mld-snooping timer**

Syntax

```
show ipv6 mld-snooping timer
```

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about the MLD-snooping clock.

### Example

The following example shows how to display the information about the MLD-snooping clock.  
switch#show ipv6 mld-snooping timers

```
vlan 1 Querier on port 0 : 251
```

```
vlan 2 Querier on port 0 : 251
```

```
vlan 2 multicast address 3333.0000.0005 response time : 13
```

```
switch#
```

Querier on port 0: 251 means the timeout time of the ageing timer of the router.

vlan 2 multicast address 3333.0000.0005 response time : this shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

## 49.12 show ipv6 mld-snooping groups

### Syntax

```
show ipv6 mld-snooping groups
```

### Parameters

None

### Default Value

None

### Usage Guidelines

This command is used to display the information about the multicast group of MLD-snooping.

### Example

The following example shows how to display the information about the multicast group of MLD-snooping.

```
switch# show ipv6 mld-snooping timer
```

```
Vlan Group  Type Port(s)
-----
2 FF02::1:FF00:2    MLD  G0/2
2 FF02::1:FF61:9901 MLD  G0/2
1 FF02::1:FF13:394 MLD  G0/1
```

```
1 FF02::1:FF00:2    MLD  G0/1
1 FF02::1:FF00:12 MLD   G0/1
1 FF02::1:FF13:647D MLD  G0/2

switch#
```

### **49.13 show ipv6 mld-snooping statistics**

#### Syntax

```
show ipv6 mld-snooping statistics
```

#### Parameters

None

#### Default Value

None

#### Usage Guidelines

This command is used to display the information about MLD-snooping statistics.

#### Example

The following example shows how to display the information about MLD-snooping statistics.

```
switch#show ipv6 mld-snooping statistics
v1_packets:0 Quantity of MLD v1 packets
v2_packets:6 Quantity of MLD v2 packets
general_query_packets:5  Quantity of general query packets
special_query_packets:0  Quantity of special query packets
listener_packets:6       Quantity of Report packets
done_packets:0           Quantity of Leave packets
send_query_packets:0     Quantity of sending packets
err_packets:0            Quantity of error packets
```

### **49.14 show ipv6 mld-snooping mac**

#### Syntax

```
show ipv6 mld-snooping mac
```

#### Parameters

None

#### Default Value

None

## Usage Guidelines

This command is used to display the multicast MAC of MLD snooping.

## Example

The following example shows how to display the information about MLD snooping.  
switch#show ipv6 mld-snooping mac

```
Vlan Mac      Ref Flags
-----
1 3333:0000:0001  1    2
2 3333:ff61:9901  1    0
      FF02::1:FF61:9901
1 3333:0000:0002  1    2
1 3333:ff00:0002  1    0
      FF02::1:FF00:2
1 3333:ff00:0012  1    0
      FF02::1:FF00:12
1 3333:ff13:647d  1    0
      FF02::1:FF13:647D
2 3333:ff00:0002  1    0
      FF02::1:FF00:2
1 3333:ff13:0394  1    0
      FF02::1:FF13:394
1 3333:ff00:0001  1    2
1 3333:ff8e:7000  1    2
switch#
```

Ref means the quantity of referred IPv6 addresses of MAC.

Flags means the debug output information, and 2 means the information need be sent to CPU.

## Chapter 50 Neighbor Detection Configuration Commands

Neighbor Detection Configuration Commands include:

- `debug ipv6 nd`
- `show ipv6 neighbors`
- `clear ipv6 neighbors`
- `ipv6 neighbor`

### 50.1.1 *debug ipv6 nd*

#### Syntax

To enable the switch of printing ND debugging information, run the following command:

```
debug ipv6 nd [entry | timer | X:X:X:X::X | adj-table]
```

#### Parameters

Parameters	Description
<i>entry</i>	<b>Stands for the switch of neighbor cache entry changes.</b>
<i>timer</i>	<b>Stands for the switch of neighbor cache timer changes.</b>
<i>X:X:X:X::X</i>	<b>Stands for the IPv6 address of neighbor cache.</b>
<i>adj-table</i>	<b>neighbor adjacent table switch</b>

#### Default Value

By default, the switch of printing ND debugging information is in disabled state.

#### Command Mode

EXEC

#### Usage Guidelines

If the command carries with no extension parameters, all debugging switches are enabled.

#### Example

None

#### Related Command

None

### 50.1.2 *show ipv6 neighbors*

#### Syntax

To display the current switch's neighbor cache, run the following command: **show ipv6 neighbors** [ *vlan vlanid* ]

#### Parameters



Parameters	Description
<i>vlanid</i>	vlan号。

#### Default Value

None

#### Command Mode

EXEC

#### Usage Guidelines

None

#### Related Command

None

### 50.1.3 *clear ipv6 neighbors*

#### Syntax

To cancel on a switch all neighbor caches that are not configured manually, run the following command:

```
clear ipv6 neighbors
```

#### Parameters

None

#### Default Value

None

#### Command Mode

EXEC

#### Usage Guidelines

This command can only cancel all those neighbor caches automatically obtained by a switch itself, not those manually configured by the ipv6 neighbor command.

#### Related Command

ipv6 neighbor

### 50.1.4 *ipv6 neighbor*

#### Syntax

To set neighbor caches of a switch in the global configuration mode, run the following command globally:

```
ipv6 neighbor address6 vlan vlanid mac
```

## Parameters

Parameters	Description
<i>address6</i>	IP address of the neighbor
<i>vlanid</i>	Stands for the ID of the VLAN port.
<i>mac</i>	Means the link-layer address of a neighbor.

## Default Value

None

## Command Mode

Global configuration mode

## Usage Guidelines

This command can be used to set neighbor caches of a switch. These neighbor caches never times out and are always reachable until no ipv6 neighbor is run.

## Example

The following example shows how to set on port interface vlan1 a neighbor whose IPv6 address is 1::1 and whose link-layer address is 00:e0:4c:5a:78:eb.

```
IPv6_config#ipv6 neighbor 1::1 vlan 1 00:e0::4c:5a:78:eb
```

## Related Command

```
show ipv6 neighbors
```

## Chapter 51 NTP Configuration Commands

### 51.1 ntp master

## Syntax

To set the device as the original NTP server (stratum=1), run the following command.

```
ntp master primary
```

To set the device as the secondary NTP server, run the following command.

```
ntp master secondary
```

To disable NTP server, run the following command.

```
no ntp master
```

## Parameters

None

## Default Value

None

## Command Mode

Global configuration mode

## Usage Guidelines

If the device is not configured with NTP server (`ntp server` command is not configured), `ntp master primary` command must be configured. Or the switch cannot provide time synchronization service. `ntp master secondary` command must be run when the switch configures NTP server. Moreover, the switch can provide time synchronization service to the NTP client in condition its own time synchronization is realized.

## Example

```
Switch_config#ntp master primary
```

```
Switch_config#ntp master secondary
```

```
Switch_config#no ntp master
```

## Related Command

**ntp server**

**ntp peer**

### **51.2 ntp authentication enable**

#### Syntax

To enable NTP identity authentication, run the following command.

**ntp authentication enable**

To return to the default setting, use the `no` form of this command.

**no ntp authentication enable**

#### Parameters

None

#### Default Value

Disabled

## Command Mode

Global configuration mode

## Usage Guidelines

For a secure network, NTP identity authentication must be enabled when operating NTP protocol. The identity authentication ensures that the client only realize time synchronization with the server which passes the identity authentication. Thus, the client will not obtain error time information from the illegal server.

## Example

```
Switch_config#ntp authentication enable
```

## Related Command

**ntp authentication key**

**ntp authentication trusted-key**

### **51.3 ntp authentication key**

To set NTP identity authentication key, run the first one of the following commands.

**ntp authentication key** *keyid md5 password*

To return to the default setting, use the no form of this command.

**no ntp authentication key** *keyid*

## Parameters

Parameters	Description
<i>keyid</i>	The serial number of the authentication key. The value ranges from 1 to 4294967295.
<i>password</i>	The key of keyed. The length ranges from 1 to 50.

## Default Value

None

## Command Mode

Global configuration mode

## Usage Guidelines

The command is used to set identity authentication key. The client and the server must set the same key serial number and key value, or they cannot realize time synchronization.

After set NTP authentication key, Set the key as the trusted key by command `ntp authentication trusted-key`. The trusted key will automatically disappear from the trusted key list when it is deleted. There is no need to run command “no ntp authentication trusted-key”.

The command can set multiple ntp authentication key commands.

## Example

```
Switch_config#ntp authentication key 5 md5 abc123
```

```
Switch_config#no ntp authentication key 5
```

## Related Command

**ntp authentication enable**

**ntp authentication trusted-key**

### **51.4 ntp authentication trusted-key**

To set the created key as the trusted key, run the first one of the following commands.

**ntp authentication trusted-key** *keyid*

To return to the default setting, use the no form of this command.

**no ntp authentication trusted-key** *keyid*

## Parameters

Parameters	Description
<i>keyid</i>	The serial number of the authentication key. The value ranges from 1 to 4294967295.

## Default Value

None

## Command Mode

Global configuration mode

## Usage Guidelines

Enable the identity authentication function, the client can only time synchronize with the server providing the trusted key. If the key provided by the server is not trusted, the client cannot synchronize to the NTP server.

The command must be configured after the key is set. The trusted key will automatically disappear from the trusted key list when it is deleted. There is no need to run command “no ntp authentication trusted-key”.

## Example

```
Switch_config#ntp authentication trusted-key 5
```

```
Switch_config#no ntp authentication trusted-key 5
```

## Related Command

**ntp authentication enable**

**ntp authentication key**

**51.5 ntp server**

## Parameters

To set NTP server, run the following command.

**ntp server** *ip-address* [**version number** | **key** *keyid*]\*

To return to the default setting, use the no form of this command.

**no ntp server** *ip-address*

## Parameters

Parameters	Description
<i>ip-address</i>	NTP Server IP address

<i>number</i>	NTP version number, the value ranges from: <1-4>, the default value is 4.
<i>keyid</i>	When sending NTP packets to the NTP server, calculate the packet information abstract with the key corresponds to the keyid. The value ranges from 1 to 4294967295. If the parameter is not set, the device will not authenticate the identity of the server, or vice verse.

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

After a NTP server is set, the device can time synchronize with the server, but the server time will not synchronize to the device.

Multiple ntp server commands can be configured. If using the NTP server on the public network, you have to configured at least 4 different NTP servers, so that the error clock source can be expelled.

### Example

```
Switch_config#ntp server 1.1.1.1 version 4 key 5
```

### Related Command

**ntp authentication enable**

**ntp authentication key**

**ntp authentication trusted-key**

## 51.6 ntp peer

To set a NTP peer for the device, run the following command.

```
ntp peer ip-address [version number | key keyid]*
```

To return to the default setting, use the no form of this command.

```
no ntp peer ip-address
```

### Parameters

Parameters	Description
<i>ip-address</i>	NTP peer IP address
<i>number</i>	NTP version number, the value ranges from: <1-4>, the default value is 4.
<i>keyid</i>	When sending NTP packets to the NTP peer, calculate the packet information abstract with the key corresponds to the keyid. The value ranges from 1 to 4294967295. If the parameter is not set, the device will not authenticate the identity of the peer, or vice verse.

### Default Value

None

### Command Mode

Global configuration mode

### Usage Guidelines

The command is used to set the NTP peer and synchronize the time of the peer to the device provided that the peer time is synchronized. The command is often used as backup between the NTP servers. The device as the client is usually not configure the command. The command `ntp server` is used to set the NTP server.

### Example

```
Switch_config#ntp peer 1.1.1.2 version 3 key 5
```

### Related Command

**ntp authentication enable**

**ntp authentication key**

**ntp authentication trusted-key**

### **51.7 show ntp**

To show NTP current status, run the following command.

**show ntp [status]**

To show NTP association status, run the following command.

**show ntp associations [detail]**

To show NTP timer status, run the following command.

**show ntp timers**

### Parameters

None

### Default Value

None

### Command Mode

EXEC

### Usage Guidelines

Show NTP relevant information

### Example

```
Switch#show ntp
```

```
Time-zone: GMT+8:00, Shanghai
Current time: 2014-05-21 10:45:26
```

```
Clock Status: synchronized
Clock Stratum: 3
Leap Indicator: 0
Reference ID: 211.233.84.186
Clock Jitter: 0.004149
Clock Precision: -18
Clock Offset: 6.561 ms
Root Delay: 172.153 ms
Root Dispersion: 587.873 ms
Packets Sent: 30788
Packets Received: 27969 (bad version: 0)
Reference Time: 2014-05-21 10:41:37
Last Update Time: 2014-05-21 10:37:08
```

```
Switch#show ntp associations
```

ip address	reference clock	st	poll	reach	delay	offset	dispersion
61.110.197.50	204.123.2.5	2	64	377	59.99	0.96	2.7
27.114.150.12	193.190.230.65	2	64	377	489.97-34.56		3.1
*211.233.84.186	204.123.2.5	2	64	377	19.99	9.15	3.0
198.55.111.50	216.229.0.50	3	64	377	229.98-40.09		3.4
199.241.31.224	132.163.4.103	2	64	377	198.042.51		3.6
204.2.134.163	241.199.164.101	2	64	360	169.97-17.16		942.8

Note: \* system peer(master), poll(s), delay(ms), offset(ms), dispersion(ms)

```
Total Associations: 6
```

**Related Command**



None

### **51.8 debug ntp**

To enable NTP packet debug switch, run the following command.

**debug ntp packet**

To enable NTP event debug switch, run the following command.

**debug ntp event**

To enable NTP error debug switch, run the following command.

**debug ntp error**

To enable NTP all debug switches, run the following command.

**debug ntp all**

To disable all debug switches, run the following command.

**no debug ntp**

#### Parameters

None

#### Default Value

None

#### Command Mode

EXEC

#### Usage Guidelines

Check NTP running process by debug information.

#### Example

None

#### Related Command

None

### **51.9 time-zone**

To enable time zone function, run the following command.

**time-zone** *name offset-hour [offset-minute]*

To return to the default setting, use the no form of this command.

**no time-zone**

#### Parameters

Parameters	Description
------------	-------------

<i>name</i>	Stands for the name of a time zone.
<i>offset-hour</i>	Hour off-set of local time to UTC time (-12~12)
<i>offset-minute</i>	Minute offset of local time to UTC time (0~59); the default value is 0.

**Default Value**

None

**Command Mode**

Global configuration mode

**Usage Guidelines**

The command is used to transfer UTC to the local time.

**Example**

```
Switch_config#time-zone Beijing 8
```

**Related Command**

None

## Chapter 52 Power Over Ethernet Configuration Commands

### Affects only for Pixietech POE-switches

#### 52.1 POE Configuration Commands

##### 52.1.1 show poe system

**Parameters**

To display the information about POE-related systems, run the following command. show poe system

**Parameters**

None

**Default Value**

None

**Command Mode**

Monitoring Mode

**Usage Guidelines**

POE DRIVER: means the drive of the chip.

POE CHIP: means the detailed chip type.

POE Port Num: means the maximum POE ports.

PSE Power Management: means the power supply management mode (automatic, preempt, non-preempt).

PSE Total Power: Total power of the power supply equipment

PSE Usage Threshold: power alarm (it is set according to the percentage)

PSE Alarm Power: means the power alarm threshold.

PSE Lower-Port-Disable Power: The threshold of the power supply for the relatively high priority preempt, which is effective only in non-automatic mode

PSE Lower-Port-NoConnect Power: The threshold of the power supply to forbid the lower or same-level priority preempt, which is effective only in non-automatic mode

PSE Consumed Power: the used power consumption

PSE Peak Power: peak power of the power supply equipment, which is effective when the power statistics is enabled

PSE Mib Notification: MIB notification occurs when the power supply for a port changes or the power changes.

PSE Temperature PSE: temperature of the chip

### Example

```
Switch_config# show poe system
POE DRIVER:PETH PD69000 DRV
POE CHIP:PD69100
POE Port Num:16
PSE PowerManagement:Non-Preemptive
PSE Total Power:6300000 mW
PSE Usage Threshold:90%
PSE Alarm Power:5670000 mW
PSE Lower-Port-Disable Power:6299900 mW
PSE Lower-Port-NoConnect Power:6299800 mW
PSE Consumed Power:0 mW
PSE Peak Power:0 mW
PSE Mib Notification:Disable
PSE Temperature:41 degree
```

### Related Command

None

### *52.1.2 show poe all*

To display the information description table of the POE port, run the following command.

---

```
show poe all
```

### Parameters

None

### Default Value

None

### Command Mode

Monitoring Mode

### Usage Guidelines

Port enabled/disabled: To enable or disable power supply for a port

Port detection: the power supply state of a port, which may be disabled, searching, delivering-power or fault.

delivering-power: means the power supply is normal.

Port pairs: the ordering of the power line of a port, of which signal means the power supply by way of the signal line and spare that by way of the spare line

Port priority: means the priority for port's power supply and it from high to low is critical, high and low.

### Example

```
Switch#show poe all
```

Port	EnableStatus	Pair	Priority
g0/1	enabled	disabled	signal low
g0/2	enabled	disabled	signal low
g0/3	enabled	disabled	signal low
g0/4	enabled	disabled	signal low
g0/5	enabled	disabled	signal low
g0/6	enabled	disabled	signal low
g0/7	enabled	disabled	signal low
g0/8	enabled	disabled	signal low
g0/9	enabled	searching	signal high
g0/10	enabled	searching	signal high
g0/11	enabled	searching	signal high
g0/12	enabled	searching	signal high
g0/13	enabled	delivering-power	signal high
g0/14	enabled	searching	signal high

```
g0/15 enabled    delivering-power    signal high
```

```
g0/16 enabled    searching    signal high
```

### Related Command

None

### 52.1.3 show poe power

To display the information about the power supply of all ports, run the following command.

```
show poe power
```

### Parameters

None

### Default Value

None

### Command Mode

Monitoring Mode

### Usage Guidelines

Max: means the maximum power limitation of a port. Current: means the current power of a port.

Average: means the average power of a port, which is effective only when the power statistics table is enabled.

Peak: means the peak power of a port, which is effective when the power statistics is enabled.

Bottom: means the bottom power of a port, which is effective only when the power statistics table is enabled.

### Example

```
Switch#show poe power
```

Port	Current	Max	Average	Peak	Bottom
g0/1	0 mW	30000 mW	0 mW	0 mW	0 mW
g0/2	0 mW	30000 mW	0 mW	0 mW	0 mW
g0/3	0 mW	30000 mW	0 mW	0 mW	0 mW
g0/4	0 mW	30000 mW	0 mW	0 mW	0 mW
g0/5	0 mW	30000 mW	0 mW	0 mW	0 mW
g0/6	0 mW	30000 mW	0 mW	0 mW	0 mW
g0/7	0 mW	30000 mW	0 mW	0 mW	0 mW
g0/8	0 mW	30000 mW	0 mW	0 mW	0 mW

```

g0/9  0 mW 30000 mW  0 mW 0 mW 0 mW
g0/10 0 mW 30000 mW  0 mW 0 mW 0 mW
g0/11 0 mW 30000 mW  0 mW 0 mW 0 mW
g0/12 0 mW 30000 mW  0 mW 0 mW 0 mW
g0/13 7600 mW  30000 mW  7620 mW  7800 mW  7600 mW
g0/14 0 mW 30000 mW  0 mW 0 mW 0 mW
g0/15 7600 mW  30000 mW  7600 mW  7800 mW  7600 mW
g0/16 0 mW 30000 mW  0 mW 0 mW 0 mW

```

### Related Command

None

#### 52.1.4 show poe interface

To display the detailed POE information of a designated port, run the following command.

```
show poe interface type slot/port
```

### Parameters

Parameters	Description
<i>type</i>	<b>Interface type</b>
<i>slot</i>	<b>Slot ID</b>
<i>Port</i>	<b>Port ID</b>

### Default Value

None

### Command Mode

Monitoring Mode

### Usage Guidelines

PSE Port Number: means the ID of an internal port.

Port Power Enabled: means to enable the power supply for a port.

Port Force Power: means to enable the forced power supply or the power supply for a low-priority port.

Port detection: the power supply state of a port, which may be disabled, searching, delivering-power or fault.

Port Fault Status: means the error information about a port.

Port Last Disconnection Reason: means the reason of the latest power cutoff on a port.

Port pairs: the ordering of the power line of a port, of which signal means the power supply by way of the signal line and spare that by way of the spare line

Port IEEE Class: means the class of a port.

Port priority: means the priority for port's power supply and it from high to low is critical, high and low.

Port Current : stands for the present current on a interface.

Port Voltage: means the current voltage of a port, which cannot be shown by some chips.

Port Current Power: stands for the current power on an interface.

Port Average Power: means the average power of a port, which is effective only when the power statistics table is enabled.

Port Peak Power : means the peak power of a port, which is effective when the power statistics is enabled.

Port Bottom Power: means the bottom power of a port, which is effective only when the power statistics table is enabled.

Port Max Powe: means the maximum power limitation of a port.

Port PD Description: stands for the description of a port.

### Example

```
Switch_config#show poe interface g0/1
```

```
PSE Port Number : 0
```

```
Port Power Enabled : disable
```

```
Port Force Power : enable
```

```
Port Detection Status : disabled
```

```
Port Fault Status :
```

```
Port Pairs : signal
```

```
Port IEEE Class : 0
```

```
Port Priority : low
```

```
Port Current : 0 mA
```

```
Port Voltage : 0 mV
```

```
Port Current Power : 0 mW
```

```
Port Average Power : 0 mW
```

```
Port Peak Power : 0 mW
```

```
Port Bottom Power : 0 mW
```

```
Port Max Power : 100 mW
```

```
Port PD Description : link_ssss
```

Switch\_config#

**Related Command**

None

**52.1.5 poe power-management**

To set the power supply management mode for a switch, run the following command.

```
poe power-management {auto | preemptive | non-preemptive | lowDisable | lowNoConnect} value
```

**Parameters**

Parameters	Description
<i>auto</i>	<b>Sets the power-supply management mode of a switch to automatic.</b>
<i>preemptive</i>	<b>Sets the power-supply management mode of a switch to preemptive.</b>
<i>non-preemptive</i>	<b>Sets the power-supply management mode of a switch to non-preemptive.</b>
<i>lowDisable</i>	<b>When the total power exceeds lowDisable, the port cannot be powered; when the total power is less than lowDisable, the power supply can go again. lowDisable = total power - value</b>
<i>lowNoConnect</i>	<b>When the total power exceeds lowNoConnect, those ports whose priorities are lower than or equal to the priority of the currently powered port, which is lowest priority among the powered ports, will be cut off from the power supply. lowNoConnect = lowDisable – value</b>

**Default Value**

The power supply management mode is auto by default.

**Command Mode**

Global configuration mode

**Usage Guidelines**

The maximum power limitation of a port cannot be set and the port's power supported by the chip is considered by default as the maximum power.

The power-supply priority of a port cannot be set and the default priority of this port is low.

Preemptive: it is to enable the function of limiting the maximum power of a port.

It is also to enable the power supply priority of a port.

Non-preemptive: it is to enable the function of limiting the maximum power of a port.

It is also to enable the power supply priority of a port.



Preempt means that a new PD device will be normally powered by a high-priority power supply port if the new PD device is connected to this high-priority port in full load and at the same time the port with the lowest power-supply priority will be cut off from power supply.

Non-preempt means that the power supply port with high priority will be notified that a PD device has accessed when this port is connected to a PD device in full load.

### Example

The following example shows how to set the power supply management mode to preemptive.

```
Switch_config#poe power-management preemptive
```

```
Switch_config#poe power-management lowDisable 18000
```

```
Switch_config#poe power-management lowNoConnect 18000
```

### Related Command

poe max-power

poe priority

### 52.1.6 poe led-time

To set the lasting time of the LED in PoE mode, run the following command.

```
poe led-time time
```

```
no poe led-time
```

### Parameters

Parameters	Description
<i>time</i>	<b>Unit: second</b>

### Default Value

The lasting time of LED in POE mode is 30 seconds.

### Command Mode

Global configuration mode

### Usage Guidelines

The no poe led-time command can set the lasting time back to the default value.

### Example

The following example shows how to set the lasting time to 10 seconds.

```
Switch_config#poe led-time 10
```

### Related Command

None

### ***52.1.7 poe mib notification-stop***

To stop sending the trap notification to users when power supply changes or power alarm occurs, run the following command:

```
poe mib notification-stop
```

```
no poe mib notification-stop
```

#### **Parameters**

None

#### **Default Value**

In the default settings, the change of power supply or the occurrence of power alarm will lead the system to send the trap notification to users.

#### **Command Mode**

Global configuration mode

#### **Usage Guidelines**

The “no” form of this command can be used to resume the default settings.

#### **Example**

The following example shows how to stop sending the trap notification to users when power supply changes or power alarm occurs:

```
Switch_config#poe mib notification-stop
```

#### **Related Command**

None

### ***52.1.8 poe pse-unprotect***

To set power supply protection for a port, run the following command:

```
poe pse-unprotect
```

```
no poe pse-unprotect
```

#### **Parameters**

None

#### **Default Value**

The power supply protection for ports is enabled by default.

#### **Command Mode**

Global configuration mode

#### **Usage Guidelines**

The “no” form of this command can be used to resume the default settings.

### Example

The following example shows how to disable the power supply protection:

```
Switch_config# poe pse-unprotect
```

### Related Command

None

### 52.1.9 poe counter value

To enable the power statistics globally, run the following command:

```
poe counter value
```

```
no poe counter
```

### Parameters

Parameters	Description
<i>value</i>	Stands for the sampling interval, whose unit is second.

### Default Value

The power statistics is disabled by default.

### Command Mode

Global configuration mode

### Usage Guidelines

The “no” form of this command can be used to resume the default settings.

### Example

The following example shows how to set the sampling interval of the power statistics to 5 seconds.

```
Switch_config# poe counter 5
```

### Related Command

None

### 52.1.10 poe threshold

To set the percentage between alarm power and the total power, run the following command.

```
poe threshold value
```

```
no poe threshold
```

### Parameters

Parameters	Description
<i>value</i>	<b>Sets the percentage between alarm power and the total power.</b>

### Default Value

The default percentage between alarm power and the total power is 100%.

### Command Mode

Global configuration mode

### Usage Guidelines

The “no” form of this command can be used to resume the default settings.

### Example

The following example shows how to set the percentage between the alarm power and the total power to 50%:

```
Switch_config#poe threshold 50
```

### Related Command

poe power-management

### 52.1.11 poe standard

To set the standard of PSE power supply, run the following command: poe standard {AF | AT | MAX}

#### Parameters

Parameters	Description
<i>AF</i>	<b>If you select the AF standard, the power supply for a port can reach up to 15.4W.</b>
<i>AT</i>	<b>If you select the AT standard, the power supply for a port can reach up to 30W.</b>
<i>MAX</i>	<b>If you select MAX, it means that as to the switch with support of both AF and AT, the AT standard will be selected, and as to the switch only support AF, the AF standard will be selected.</b>

### Default Value

The switch support MAX by default.

### Command Mode

Global configuration mode

### Usage Guidelines

If you select the AF standard, the power supply for a port can reach up to 15.4W. If you select the AT standard, the power supply for a port can reach up to 30W.

If you select MAX, it means that as to the switch with support of both AF and AT, the AT standard will be selected, and as to the switch only support AF, the AF standard will be selected.

### Example

The following example shows how to set the PSE power supply standard to AF.

```
Switch_config#poe standard AF
```

### Related Command

None

#### 52.1.12 poe disable

To enable the power supply of a port, run the following command.

```
poe disable { time-range name | <cr>}
```

```
no poe disable {time-range | <cr>}
```

### Parameters

Parameters	Description
<i>time-range name</i>	The parameter name stands for the name of the power-off time range.
<cr>	Means to enter poe disable alone and disable the port.

### Default Value

Power supply on a port is enabled and there is no time limit to power supply.

### Command Mode

Interface configuration mode

### Usage Guidelines

poe disable: means to shut down power supply.

no poe disable: means to open power supply.

poe disable time-range name to shut down the control of time range in the period of adding name.

no poe disable time-range to remove the control of time range in the period of adding name.

### Example

The following example shows how to disable the power supply of port g/1.

```
Switch_config_g0/1#poe disable
```

The following example shows how to disable power supply in the period of Sunday\_free.

```
Switch_config_g0/1poe disable time-range Sunday_free
```

## Related Command

time-range

### 52.1.13 poe max-power

Setting the Maximum Power of a Port

poe max-power value

no poe max-power

## Parameters

Parameters	Description
<i>value</i>	Means the maximum power of a port, whose unit is mW.

## Default Value

The default maximum power of a port is 30000mW.

## Command Mode

Interface configuration mode

## Usage Guidelines

The "no" form of this command can be used to resume the default maximum power. The command runs in non-auto mode.

## Example

The following example shows how to set the maximum power of port g0/1 to 15000mW.

```
Switch_config_g0/1#poe max-power 15000
```

## Related Command

poe power-management

### 52.1.14 poe priority

Setting the Power Supply Priority for a Port

poe priority {critical | high | low }

## Parameters

Parameters	Description
<i>critical</i>	Stands for the highest priority.
<i>high</i>	Stands for the high priority.
<i>low</i>	Stands for the lowest priority.

## Default Value

The power supply priority of a port is low by default.

### Command Mode

Interface configuration mode

### Usage Guidelines

The command runs in non-auto mode.

### Example

The following example shows how to set the power supply priority of port g0/1 to critical.  
Switch\_config\_g0/1#poe priority critical

### Related Command

poe power-management

#### 52.1.15 poe PD-description

To set the port description (usually for PD), run the following command.

poe PD-discription *string*

no poe PD-discription

### Parameters

Parameters	Description
<i>string</i>	Stands for the character string of port's description.

### Default Value

The default value is null.

### Command Mode

Interface configuration mode

### Usage Guidelines

The “no” form of this command is used to delete the description character string.

### Example

The following example shows how to set POE port description of g0/1 to AP-1.  
Switch\_config\_g0/1#poe PD-discription AP-1

### Related Command

None

#### 52.1.16 poe force-power

To set the forced power supply, run the following command.

poe force-power

```
no poe force-power
```

### Parameters

None

### Default Value

The forced power supply is disabled by default.

### Command Mode

Interface configuration mode

### Usage Guidelines

The “no” form of this command is used to disable the forced power supply.

### Example

The following example shows how to set the forced power supply for the POE port of g0/1.

```
Switch_config_g0/1#poe force-power
```

### Related Command

```
poe power-management
```

### 52.1.17 poe extern-power

Setting the power value of the external power supply

```
poe extern-power value
```

```
no poe extern-power
```

### Parameters

Parameters	Description
<i>value</i>	The actual power value of the external power supply. Unit: W

### Default Value

The external power is 0W by default.

### Command Mode

Global configuration mode

### Usage Guidelines

Use the no form of this command to set the default value of the external power to 0W. The total power of the POE power supply = the power of the internal power supply + the power of the external power supply. The power of the external power supply is the actual power of the external power supply.

### Example



The following example shows how to set the external power to 400W when the external power supply is 400W.

```
Switch_config#poe extern-power 400
```

#### Related Command

None

## Chapter 53 RIP Configuration Commands

### 53.1 RIP Configuration Commands

RIP Configuration Commands Include:

- auto-summary
- default-information originate
- default-metric
- ip rip authentication
- ip rip message-digest-key
- ip rip passive
- ip rip password
- ip rip receive version
- ip rip send version
- ip rip split-horizon
- neighbor
- network
- offset
- router rip
- timers expire
- timers holddown
- timers update
- validate-update-source
- version
- distance
- filter
- maximum-count
- show ip rip

- show ip rip database
- show ip rip protocol
- debug ip rip database
- debug ip rip protocol

### **53.1.1 auto-summary**

To activate the automatic summarization function, use the auto-summary command. To turn off this function, use the no form of this command.

**auto-summary**

**no auto-summary**

**parameter**

This command has no parameter or keywords.

**default**

Enabled by default

**command mode**

router configuration

**instruction**

Routing summarization reduces the amount of routing information in the routing tables and switching information. Routing Information Protocol(RIP) do not support subnet mask, therefore, if it is forwarded to subnets, routing possibly cause ambiguity. RIP Version 1 always uses routing summarization. If using RIP Version 2, you can turn off routing summarization by using the no auto-summary command. When routing summarization is off,. Subnets are advertised..

**example**

To specify RIP version on Serial 1/0 as RIP Version 2 and turn off routing summarization function

```
router rip
```

```
version 2
```

```
no auto-summary
```

**related commands**

**version**

### **53.1.2 default-information originate**

To generate a default route, use the default-information originate command. To disable this function , use the no form of this command..

**default-information originate**

**no default-information originate****parameter**

none

**default**

disable this function by default

**command mode**

router configuration

**instruction**

After the default-information originate command is activated, the routing information(0.0.0.0/0) is accompanied when send routing updating.

**example**

When send routing updating information, the default routing(0.0.0.0/0) is accompanied.

router rip

version 2

network 172.68.16.0

default-information originate

ip route default f0/0

**53.1.3 default-metric**

To set default metric values for import routing, use the default-metric command. To return the default stata, use the no form of this command..

**default-metric number****no default-metric**

Parameters	Description
<i>number</i>	<b>Default metric value. It has a value from 1 to 16.</b>

**default**

Built-in, automatic metric translations, as appropriate for each routing protocol

**command mode**

router configuration

**instruction**

The default-metric command is used to set default routing metric used in importing routing of other routing protocols into Rip packets. When import routing of other protocols, use the specified default routing by default-metric if no specified routing metric.

**example**

The following example shows a routing switch in autonomous system 119 using both the RIP and the OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the OSPF-derived routes a RIP metric of 8.

```
router rip
default-metric 8
redistribute ospf 119
```

**related commands****redistribute****default-information originate****53.1.4 ip rip authentication**

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the `ip rip authentication mode` command in interface configuration mode. To restore plain text authentication, use the `no` form of this command.

**ip rip authentication {simple | message-digest}**

**no ip rip authentication**

**parameter**

Parameters	Description
<i>simple</i>	Plain text authentication.
<i>message-digest</i>	Keyed Message Digest 5 (MD5) authentication.

**default**

disabled

**command mode**

interface configuration mode

**instruction**

RIP Version 1 does not support authentication.

**example**

The following example configures the interface to use MD5 authentication:

```
ip rip authentication message-digest
```

**related commands**

**ip rip password**

**ip rip message-digest-key**

### 53.1.5 ip rip message-digest-key

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify Message Digest 5 (MD5) authentication used on the interface, use the `ip rip message-digest-key md5` command. To prevent the authentication, use the `no` form of this command

**ip rip message-digest-key** *key-id* **md5** **password**

**no ip rip message-digest-key** [*key-id*]

parameter

Parameters	Description
<i>key-id</i>	A key identifier
<i>password</i>	The specified password

default

MD5 authentication is invalid.

command mode

interface configuration mode

instruction

No authentications are carried out on interface if no passwords are configured using the `ip rip message-digest-key key-id md5 password` command.

example

The following example configures interface to receive and send MD5 authentication packets that belong to password 'mykey':

```
ip rip message-digest-key 4 md5 mykey
```

related commands

ip rip authentication

### 53.1.6 ip rip passive

To cancel the routing switch to send routing updating on interface, use the `ip rip passive` command. To reactivate the routing updating, use the `no` form of this command.

**ip rip passive**

**no ip rip passive**

parameter

none

default

send routing updates on the interface

**command mode**

interface configuration mode

**instruction**

If you cancel routing updating on a certain interface, a specified subnetwork will keep on announcing to other interfaces, and the routing updating that from other routing switches can be continually accepted and dealt with on this interface.

**example**

The following example sends RIP packets updating to all interfaces that belong to the network 172.16.0.0 ( except Ethernet interface 1/0):

```
interface ethernet 1/0
ip address 172.15.0.1 255.255.0.0
ip rip passive
router rip
network 172.16.0.0
```

**related commands**

none

**53.1.7 ip rip password**

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify the plain text authentication used on the interface, use the ip rip password command Use the no form of this command to prevent authentication.

**ip rip password** *password***no ip rip password** *password***parameter**

Parameters	Description
<i>password</i>	the specified password

**default**

no authentication

**command mode**

interface configuration mode

**instruction**

No authentications are carried out on interface without using the ip rip password command to configure any password.

**example**

The following example configures interface to receive and send any plain text authentication packet that belong to password 'mykey'

```
ip rip password mykey
```

related commands

**ip rip authentication**

### *53.1.8 ip rip receive version*

To specify a Routing Information Protocol (RIP) version to receive on specified interface, use the `ip rip receive version` command in interface configuration mode. To follow the global version rules, use the `no` form of this command.

**ip rip receive version [1] [2]**

**no ip rip receive version**

parameter

Parameters	Description
1	(Optional) Accepts only RIP Version 1 packets on the interface.
2	(Optional) Accepts only RIP Version 2 packets on the interface.

default

Accepts RIP Version 1 and RIP Version 2 packets

command mode

interface configuration mode

instruction

Use this command to override the default behavior of RIP as specified by the `version` command. This command applies only to the interface being configured. You can configure the interface to receive both RIP versions.

example

The following example configures the interface to receive both RIP Version 1 and Version 2 packets:

```
ip rip receive version 1 2
```

The following example configures the interface to receive only RIP Version 1 packets:

```
ip rip receive version 1
```

related commands

**ip rip send version**

**version**

### 53.1.9 ip rip send version

To specify a Routing Information Protocol (RIP) version to send on specified interface, use the `ip rip send version` command in interface configuration mode. To follow the global version rules, use the `no` form of this command.

**ip rip send version [ 1 | 2 | compatibility ]**

**no ip rip send version**

parameter

Parameters	Description
<i>1</i>	<b>(Optional) Sends only RIP Version 1 packets out the interface.</b>
<i>2</i>	<b>(Optional) Sends only RIP Version 2 packets out the interface.</b>
<i>compatibility</i>	<b>(Optional) Broadcasts only RIP Version 2 packets out the interface.</b>

default

Sends only RIP Version 1 packets

command mode

interface configuration mode

instruction

Use this command to override the default behavior of RIP as specified by the `version` command. This command applies only to the interface being configured. the interface can be configured to receive both RIP Version 1 and Version 2 packets

example

The following example configures the interface to send only RIP Version 1 packets out the interface:

```
ip rip send version 1
```

The following example configures the interface to send only RIP Version 2 packets out the interface:

```
ip rip send version 2
```

related commands

**ip rip receive version**

**version**

### 53.1.10 ip rip split-horizon

To enable the split horizon mechanism, use the `ip split-horizon` command in interface configuration mode. To disable the split horizon mechanism, use the `no` form of this command.



**ip rip split-horizon****no ip rip split-horizon****parameter**

none

**default**

Default behavior varies with media type.

**command mode**

interface configuration mode

**instruction**

For all interfaces except those for which either Frame Relay or Switched Multimegabit Data Service (SMDS) encapsulation is enabled, the default condition for this command is `ip split-horizon`; in other words, the split horizon feature is active. If the interface configuration includes either the `encapsulation frame-relay` or `encapsulation smds` command, then the default is for split horizon to be disabled.

Note: For networks that include links over X.25 packet switched networks (PSNs), the `neighbor routing switch` configuration command can be used to defeat the split horizon feature. You can as an alternative explicitly specify the `no ip split-horizon` command in your configuration. However, if you do so you must similarly disable split horizon for all routing switches in any relevant multicast groups on that network.

If split horizon has been disabled on an interface and you want to enable it, use the `ip split-horizon` command to restore the split horizon mechanism.

Note: In general, changing the state of the default for the `ip split-horizon` command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a PSN), you must disable split horizon for all routing switches and access servers in any relevant multicast groups on that network.

**example**

The following simple example disables split horizon on a serial link. The serial link is connected to an X.25 network.

```
interface serial 1/0
encapsulation x25
no ip rip split-horizon
```

**related commands****neighbor**

### 53.1.11 neighbor

To define a neighboring routing switch with which to exchange routing information, use the `neighbor` command in routing switch configuration mode. To remove an entry, use the `no` form of this command.

**neighbor** *ip-address*

**no neighbor** *ip-address*

parameter

Parameters	Description
<i>ip-address</i>	<b>IP address of a peer routing switch with which routing information will be exchanged.</b>

default

No neighboring routing switches are defined.

command mode

router configuration

instruction

This command permits the point-to-point (nonbroadcast) exchange of routing information in order to meet special requirements of the specified nonbroadcast network.

example

In the following example, the `neighbor` routing switch configuration command permits the sending of routing updating to specific neighbors.

```
router rip
```

```
neighbor 131.108.20.4
```

related commands

**network**

### 53.1.12 network

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the `network` command in routing switch configuration mode. To remove an entry, use the `no` form of this command.

**network** *network-number* <*network-mask*>

**no network** *network-number* <*network-mask*>

parameter

Parameters	Description
<i>Network-number</i>	<b>IP address of the network of directly connected networks.</b>

<i>Network-mask</i>	<b>(optional) IP mask of the network of directly connected networks</b>
---------------------	---

**default**

No networks are specified.

**command mode**

router configuration

**instruction**

The network number specified must not contain any subnet information. There is no limit to the number of network commands you can use on the routing switch. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP updates.

**example**

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 128.99.0.0 and 192.31.7.0:

```
router rip
network 128.99.0.0
network 192.31.7.0
```

**related commands****router rip****53.1.13 offset**

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the offset command in routing switch configuration mode. To remove an offset list, use the no form of this command.

**offset** *{type number | \*} {in | out} access-list-name offset*

**no offset** *{type number | \*} {in | out}*

**parameter**

Parameters	Description
<i>In</i>	<b>Applies the access list to incoming metrics.</b>
<i>Out</i>	<b>Applies the access list to outgoing metrics.</b>
<i>access-list-name</i>	<b>Standard access list number to be applied. Access list number 0 indicates all access lists. If offset is 0, no action is taken.</b>
<i>offset</i>	<b>Positive offset to be applied to metrics for networks matching the access list.</b>
<i>type</i>	<b>Interface type to which the offset list is applied.</b>

<i>number</i>	<b>(Optional) Interface number to which the offset list is applied.</b>
---------------	---

### default

This command is disabled by default.

### command mode

router configuration

### instruction

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

### example

In the following example, the routing switch applies an offset of 10 to routes learned from Ethernet interface 1/0:

```
offset ethernet 1/0 in 21 10
```

### 53.1.14 router rip

To configure the Routing Information Protocol (RIP) routing process, use the `router rip` command in global configuration mode. To turn off the RIP routing process, use the `no` form of this command.

### router rip

### no router rip

### parameter

none

### default

No RIP routing process is defined.

### command mode

global configuration mode

### instruction

User should first enable RIP to enter router configuration mode to configure all global parameters of RIP. However, it is regardless whether RIP is enabled if you configure parameters related to interface,

### example

The following example shows how to begin the RIP routing process:

```
router rip
```

related commands

**network (RIP)**

### 53.1.15 timers expire

To adjust RIP network timers, use the `timers expire` router configuration command. To restore the default timers, use the `no` form of this command.

**timers expire interval**

**no timers expire**

parameter

Parameters	Description
<i>expire</i>	Interval of time in seconds after which a route is declared invalid; it should be at least three times the value of update. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.

default

180 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note: The current and default timer values can be seen by the `show ip rip` command.

example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

**router rip**

**timers expire 30**

### 53.1.16 timers holddown

To adjust RIP network timers, use the `timers holddown` routing switch configuration command. To restore the default timers, use the `no` form of this command.

**timers holddown second**

**no timers holddown**

parameter

Parameters	Description
<i>second</i>	Interval in seconds during which routing information regarding better paths is suppressed. It should be at least three times the value of update. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 120 seconds.

default

120 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

**Note:**

The current and default timer values can be seen by the show ip rip command.

example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

**router rip**

**timers holddown 30**

### 53.1.17 timers update

To adjust RIP network timers, use the timers update routing switch configuration command. To restore the default timers, use the no form of this command.

**timers update update**

**no timers update**

parameter

Parameters	Description
<i>update</i>	Rate in seconds at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.

**default**

30 seconds

**command mode**

router configuration

**instruction**

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

**Note:**

The current and default timer values can be seen by the `show ip rip` command.

**example**

In the following example, updates are broadcast every 5 seconds.

```
router rip
```

```
timers update 5
```

Note that by setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a big concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routing switches to spend an excessive amount of time processing updates.

**53.1.18 validate-update-source**

To have the software validate the source IP address of incoming routing updates for RIP routing protocols, use the `validate-update-source` routing switch configuration command. To disable this function, use the `no` form of this command.

**validate-update-source****no validate-update-source****parameter**

This command has no parameters or keywords.

**default**

Enabled

**command mode**

router configuration

**instruction**

This command is only applicable to RIP and IGRP. The software ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface.

Disabling split horizon on the incoming interface will also cause the system to perform this validation check.

For unnumbered IP interfaces (interfaces configured as `ip unnumbered`), no checking is performed.

### example

In the following example, a routing switch is configured to not perform validation checks on the source IP address of incoming RIP updates:

```
router rip
network 128.105.0.0
no validate-update-source
```

### 53.1.19 version

To specify a RIP version used globally by the routing switch, use the `version` routing switch configuration command. Use the `no` form of this command to restore the default value.

#### version {1 | 2}

#### no version

#### parameter

Parameters	Description
1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

#### default

The software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets.

#### command mode

router configuration

#### instruction

To specify RIP versions used on an interface basis, use the `ip rip receive version` and `ip rip send version` commands; or it will send RIP packets in terms of the global configuration version.

### example

The following example enables the software to send and receive RIP Version 2 packets:

```
version 2
```

#### related commands

#### ip rip receive version



**ip rip send version****53.1.20 distance**

To define an administrative distance for RIP routes, use the distance command in routing switch configuration mode.

Distance weight <address mask <access-list-name>>

parameter

Parameters	Description
<i>weight</i>	<b>Administrative distance. An integer from 1 to 255. It is recommended to use 10 to 255. (The values 0 to 9 are reserved for internal use. ) Routes with a distance value of 255 are not installed in the routing table.)</b>
<i>address</i>	<b>(Optional) Source IP address (in four-part, dotted decimal notation)</b>
<i>mask</i>	<b>(Optional) IP address mask (in four-part, dotted decimal notation) If a certain digit is 0, software will omit the corresponding value in the address.</b>
<i>access-list-name</i>	<b>(Optional) Named access list to be applied to incoming routing updates.</b>

default

120

command mode

EXEC

instruction

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. When the optional access list name or number is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the routing switch that supplies the routing information.

example

The following example sets the administrative distance to 100 for the routing switch with the address 192.1.1.0/24.

```
router rip
distance 100 192.1.1.0 255.255.255.0
```

**53.1.21 filter**

To filter for RIP routes, use the filter command.

```
filter * in access-list {access-list-name}
```

```
filter * in gateway {access-list-name}
```

```
filter * in prefix {prefix-list-name}
```

**filter type number in access-list** {*access-list-name*}

**filter type number in gateway** {*access-list-name*}

**filter type number in prefix** {*prefix-list-name*}

**no filter \* in**

**filter \* out access-list** {*access-list-name*}

**filter \* out gateway** {*access-list-name*}

**filter \* out prefix** {*prefix-list-name*}

**filter type number out access-list** {*access-list-name*}

**filter type number out gateway** {*access-list-name*}

**filter type number out prefix** {*prefix-list-name*}

**no filter \* out**

**no filter type number out**

#### Parameter

Parameters	Description
<i>access-list-name</i>	<b>Standard IP access list name. This list defines networks of which are received or suppressed in routing update.</b>
<i>prefix-list-name</i>	<b>Standard IP prefix list name. This list defines networks of which are received or suppressed in routing update.</b>
<i>in/out</i>	<b>Applies access list for in/out routing update.</b>
<i>type</i>	<b>(Optional) Interface type</b>
<i>number</i>	<b>(Optional) Indicates number of interface on which applies the access list for in/out routing update. If no interface is defined, the access list is applicable to all in/out routing update.</b>

#### Default

disabled

#### Command mode

EXEC

#### Instruction

Filter the route that are to be sent and received. If you use the access-list command to configure access list for dynamic routing protocol, you should use the standard access list.

#### Example

The following example filter route 10.0.0.0/8 from interface s2/1:

```
router rip
```

```
filter s2/1 out access-list mylist
```

```
ip access-list standard mylist
deny 10.0.0.0 255.0.0.0
```

### 53.1.22 maximum-count

To configure the maximum route count in local RIP routing table, use the maximum-count command. Use the no form of this command to restore default setting.

**maximum-count** *number*

**no maximum-count**

Parameter

Parameters	Description
<i>number</i>	The maximum route count to be configured, in the range from 512 to 4096.

Default

1024

Command mode

router configuration

Instruction

Use this command to configure the maximum route count in local RIP routing table. When routes in local routing table exceed the maximum value, no routes will be added to routing table.

Example

The following example configures 2000 as the maximum route count in the local RIP routing table:

```
router rip
maximum-count 2000
```

Related commands

none

### 53.1.23 show ip rip

To display RIP main information, use the show ip rip command.

**show ip rip**

Parameter

None

Default

none

## Command mode

EXEC

## Instruction

User can see the current configuration status about RIP according to the output of this command.

## Example

The following example displays configuration parameter information about RIP:

```
router#show ip rip
```

```
RIP protocol: Enabled
```

```
Decided on the interface version control
```

```
AUTO-SUMMARY: Yes
```

```
Update: 30, Expire: 180, Holddown: 120
```

```
Distance: 120
```

```
default-metric: 1
```

The meaning of the above fields are as follows:

field	Description
<i>Enabled</i>	Indicates current state of the active routing protocol process.
<i>Distance</i>	Indicates current administrative distance.
<i>version</i>	Indicates current version of the protocol.
<i>AUTO-SUMMARY</i>	Indicates whether to allow auto-summary or not.
<i>Update</i>	Interval of time at which updates are sent.
<i>Holddown</i>	Interval (in seconds) during which routing information regarding better paths is suppressed.
<i>Expire</i>	Interval of time after which a route is expired.
<i>RIP default-metric</i>	Default metric value during redistribute

### 53.1.24 show ip rip database

To display summary address entries in the Routing Information Protocol (RIP), use the show ip rip database command

```
show ip rip database
```

## Parameter

none

## Default

none

**Command mode**

EXEC

**Instruction**

Summary address entries will appear in the database from output of this command.

**Example**

The following output shows a summary address entry:

```
router#show ip rip database
1.0.0.0/8 auto-summary
1.1.1.0/24 directly connected Loopback1
100.0.0.0/8 via 192.1.1.2 00:00:02
192.1.1.0/24 directly connected Serial2/1
192.1.1.0/24 auto-summary
```

The meanings of the following fields are as follows:

<b>field</b>	<b>Description</b>
<i>Network-number/network-mask</i>	<b>RIP routes</b>
<i>Summary/connected/via gateway</i>	<b>The corresponding RIP route types</b>
<i>interface</i>	<b>RIP directly connected and summary routes interface</b>
<i>time</i>	<b>refreshed time</b>

**53.1.25 show ip rip protocol**

To display RIP protocol configuration information, use the show ip rip protocol command.

**show ip rip protocol****Parameter**

none

**Default**

none

**Command mode**

EXEC

**Instruction**

User can see the current RIP protocol configuration information from output of this command.

**Example**

The following example displays RIP protocol configuration information:

```
router#show ip rip protocol
```

```
RIP is Active
```

```
Sending updates every 30 seconds, next due in 30 seconds
```

```
Invalid after 180 seconds, holddown 120
```

```
update filter list for all interfaces is:
```

```
update offset list for all interfaces is:
```

```
Redistributing:
```

```
redistribute connect
```

```
Default version control: send version 1, receive version 1 2
```

Interface	Send	Recv
Async0/0	1	1 2
FastEthernet0/0	1	1 2
Serial1/0	1	1 2
Ethernet1/1	1	1 2
Serial2/0	1	1 2
Serial2/1	1	1 2
Loopback1	1	1 2

```
Automatic network summarization is in effect
```

```
Routing for Networks:
```

```
174.168.0.0/16
```

```
Distance: 120 (default is 120)
```

### ***53.1.26 debug ip rip database***

To monitor RIP routed events, use the `debug ip rip database` command.

#### **debug ip rip database**

##### **Parameter**

none

##### **Default**

none

##### **Command mode**

EXEC

##### **Instruction**

User can see some events of the current RIP routes from output of this command.

### Example

The following example monitors some events of the RIP routes:

```
router# debug ip rip database
```

```
RIP-DB: Adding summary route 192.1.1.0/24 <metric 0> to RIP database
```

The meanings of the above fields are as follows:

field	Description
<i>summary</i>	Indicates the route type that added to the routing table
<i>192.1.1.0/24</i>	Indicates the route that added to the routing table
<i>&lt;metric 0&gt;</i>	Route metric value

### 53.1.27 debug ip rip protocol

To monitor RIP packets, use the debug ip rip protocol command.

#### debug ip rip protocol

##### Parameter

none

##### Default

none

##### Command mode

EXEC

##### Instruction

User can see the current content of RIP packets from the output of this command.

### Example

The following example monitors RIP packets:

```
router# debug ip rip protocol
```

```
RIP: send to 255.255.255.255 via Loopback1
```

```
vers 1, CMD_RESPONSE, length 24
```

```
192.1.1.0/0 via 0.0.0.0 metric 1.
```

The following output will be displayed when ran on the version 2:

```
RIP: send to 255.255.255.255 via Loopback1
```

```
vers 2, CMD_RESPONSE, length 24
```

```
192.1.1.0/24 via 0.0.0.0 metric 1
```

The meaning of the above fields are as follows:

field	Description
<i>Send/Recv</i>	Indicates packets that are sent or received packets
<i>to 255.255.255.255</i>	Indicates the destination address of IP packets
<i>via Loopback1</i>	Indicates the interface on which RIP packets that are sent and received.
<i>vers 2</i>	Indicates version of RIP packets that are sent and received.
<i>CMD_RESPONSE/ CMD_REQUEST</i>	Indicates type of the packet
<i>length 24</i>	Indicates length of packet.
<i>192.1.1.0/24</i>	Indicates destination network in routing information
<i>via 0.0.0.0</i>	Indicates next hop address.
<i>metric</i>	Route metric value

## Chapter 54 BEIGRP Configuration Commands affects ONLY PXT-S2790G/2795G or higher

### 54.1 BEIGRP Configuration Commands

BEIGRP Configuration Commands Include:

- auto-summary
- clear ip beigrp neighbors
- debug ip beigrp
- debug ip beigrp fsm
- debug ip beigrp neighbours
- debug ip beigrp packet
- debug ip beigrp transmit
- default-metric
- distance
- filter
- beigrp log-neighbor-changes
- beigrp router-id
- ip beigrp bandwidth-percent
- ip beigrp hello-interval
- ip beigrp hold-time



- ip beigrp passive
- ip beigrp split-horizon
- ip beigrp summary-address
- metric weights
- network
- offset
- redistribute
- router beigrp
- show ip beigrp interface
- show ip beigrp neighbors
- show ip beigrp protocol
- show ip beigrp topology
- show ip beigrp traffic

#### **54.1.1 auto-summary**

To allow automatic summarization of BEIGRP routes, use the auto-summary command in routing switch configuration mode. The automatic summarization function is enabled by default. To disable this function and send every specific routing information to its neighbours, use the no form of this command.

##### **auto-summary**

##### **no auto-summary**

##### **Parameter**

none

##### **Default**

Enabled

##### **Command mode**

router configuration

##### **Instruction**

In the current BEIGRP version, route summarization is closely related to network commands. It enforces the following summarization rules:

- When one BEIGRP process defines various networks, create route summarization of defined network as long as BEIGRP Topology Table includes one subnet in the current network.
- The summary routes point to Null0 interface, which have the minimum distance of all the concrete routes that summary routes contain. The summary routes insert to the

main IP routing table, and the administrative distance is 5(which cannot be configured)

- When send updates to neighbours of different main IP networks, cancel the subnets in automatic summarization of the first rule and the second rule, just send the summarization route.
- Summarize the subnets in networks that belong to BEIGRP process definition list.

## Related commands

### ip beigrp summary-address

### network

#### 54.1.2 clear ip beigrp neighbors

To delete entries from the neighbor table, use the clear ip beigrp neighbors command in privileged EXEC mode.

**clear ip beigrp** [*as-number*] **neighbors** [*ip-address* | *interface-type interface-number*]

## Parameter

field	Description
<i>ip-address</i>	(Optional) Address of BEIGRP's neighbor.
<i>interface</i>	(Optional) Interface name. After typing this parameter, all neighbors on this interface will perform adjacent reset.

## Default

none

## Command mode

EXEC

## Instruction

All BEIGRP's neighbors will be reset without specifying any parameter.

The use of this command will lead adjacent reset of one or several neighbors, and then triggers routing operation. In the case when many routes are influenced, it may cause route fluctuation, and it needs some time to convergence again. So we recommend not to use this command unless the system is in the network debugging stage.

## Example

The following example removes all neighbors on ethernet1/1 and triggers recalculation of the related routes:

```
clear ip beigrp ethernet1/1
```

### 54.1.3 debug ip beigrp

To trace BEIGRP protocol information, you can press this command in the privileged EXEC mode.

#### **debug ip beigrp**

##### 1. **no debug ip beigrp**

#### Parameter

none

#### Default

none

#### Command mode

EXEC

#### Instruction

It helps to find network malfunction using this command.

#### Example

The following example removes all neighbors on Ethernet 1/1 and triggers recalculation of the related routes:

```
clear ip beigrp ethernet1/1
```

### 54.1.4 debug ip beigrp fsm

To trace the change of state machine of BEIGRP DUAL algorithm, use the debug ip beigrp fsm command in EXEC command.

#### **debug ip beigrp fsm [detail]**

#### Parameter

field	Description
<i>detail</i>	<b>(Optional) Displays detailed information.</b>

#### Default

none

#### Command mode

EXEC

#### Instruction

It helps to find network malfunction using this command

#### Related commands

**debug ip beigrp packet**

### 54.1.5 debug ip beigrp neighbors

To display the establishment and deletion of BEIGRP neighbors, use the debug ip beigrp neighbors command in EXEC mode.

#### debug ip beigrp neighbors

##### Parameter

none

##### Default

none

##### Command mode

EXEC

##### Instruction

It helps to find network malfunction using this command.

##### Example

```
TestC#debug ip beigrp neighbors
```

```
BEIGRP: Neighbor 192.168.20.141 went down on Ethernet1/1 for peer restarted.
```

```
BEIGRP: Neighbor(192.168.20.141) not yet found.
```

```
BEIGRP: Neighbor(192.168.20.141) not yet found. BEIGRP: New neighbor 192.168.20.141
```

```
BEIGRP: Neighbor 202.117.80.143 went down on Ethernet2/1 for manually cleared.
```

```
BEIGRP: Neighbor 192.168.20.141 went down on Ethernet1/1 for manually cleared.
```

```
BEIGRP: New neighbor 192.168.20.204
```

```
BEIGRP: New neighbor 202.117.80.143
```

```
BEIGRP: New neighbor 192.168.20.141
```

##### Related commands

#### debug ip beigrp fsm

### 54.1.6 debug ip beigrp packet

To display BEIGRP packets situations, use the debug ip beigrp packet command in EXEC mode.

**debug ip beigrp packets [ack | hello | query | reply | retry | terse | update]**

**no debug ip beigrp packets [ack | hello | query | reply | retry | terse | update]**

##### Parameter

field	Description
ack	(Optional) Traces ACK packets

<i>hello</i>	<b>(Optional) Traces hello packets.</b>
<i>query</i>	<b>(Optional) Traces query packets.</b>
<i>reply</i>	<b>(Optional) Traces reply packets</b>
<i>retry</i>	<b>(Optional) Traces retry packets.</b>
<i>terse</i>	<b>(Optional) Traces all packets except hello packets.</b>
<i>update</i>	<b>(Optional) Traces update packets.</b>

## Default

none

## Command mode

EXEC

## Instruction

It helps to find network malfunction using this command.

## Example

```
router#debug ip beigrp packet
```

```
BEIGRP: Send HELLO packet to 224.0.0.10 via Ethernet2/1 with Ack 0/0
```

```
BEIGRP: Receive ACK packet from 192.168.20.141 via Ethernet1/1 with Ack 0/54
```

```
BEIGRP: Receive HELLO packet from 202.117.80.143 via Ethernet2/1 with Ack 0/0
```

```
BEIGRP: Receive UPDATE packet from 192.168.20.204 via Ethernet1/1 with Ack 142/0
```

```
BEIGRP: Send HELLO packet to 192.168.20.204 via Ethernet1/1 with Ack 0/142
```

```
BEIGRP: Receive HELLO packet from 192.168.20.141 via Ethernet1/1 with Ack 0/0
```

```
BEIGRP: Receive HELLO packet from 192.168.20.204 via Ethernet1/1 with Ack 0/0
```

```
BEIGRP: Receive QUERY packet from 192.168.20.204 via Ethernet1/1 with Ack 143/0
```

```
BEIGRP: Send HELLO packet to 192.168.20.204 via Ethernet1/1 with Ack 0/143
```

```
BEIGRP: Send REPLY packet to 192.168.20.204 via Ethernet1/1 with Ack 55/143
```

```
BEIGRP: Send UPDATE packet to 224.0.0.10 via Ethernet2/1 with Ack 57/0
```

```
BEIGRP: Receive ACK packet from 192.168.20.204 via Ethernet1/1 with Ack 0/55
```

```
BEIGRP: resend UPDATE packet for neighbor 192.168.20.204 with retry num 1.
```

```
BEIGRP: Receive ACK packet from 202.117.80.143 via Ethernet2/1 with Ack 0/57
```

```
BEIGRP: Send UPDATE packet to 202.117.80.143 via Ethernet2/1 with Ack 57/77
```

```
BEIGRP: Send UPDATE packet to 224.0.0.10 via Ethernet1/1 with Ack 56/0
```

```
BEIGRP: Receive ACK packet from 192.168.20.204 via Ethernet1/1 with Ack 0/56
```

BEIGRP: Send UPDATE packet to 192.168.20.141 via Ethernet1/1 with Ack 56/88  
 BEIGRP: Send UPDATE packet to 192.168.20.204 via Ethernet1/1 with Ack 56/143  
 BEIGRP: Receive UPDATE packet from 202.117.80.143 via Ethernet2/1 with Ack 79/0  
 BEIGRP: Send HELLO packet to 202.117.80.143 via Ethernet2/1 with Ack 0/79  
 BEIGRP: Receive ACK packet from 192.168.20.204 via Ethernet1/1 with Ack 0/56  
 BEIGRP: Send QUERY packet to 224.0.0.10 via Ethernet1/1 with Ack 60/0  
 BEIGRP: Send UPDATE packet to 224.0.0.10 via Ethernet1/1 with Ack 61/0

field	Description
<i>Recv/Send/ Enqueueing</i>	<b>Receives, sends or enqueueings packet to send -queue</b>
<i>HELLO / UPDATE / QUERY / ACK</i>	<b>Packet types that are received or sent.</b>
<i>192.1.1.1</i>	<b>Neighbor IP address to send packet</b>
<i>Serial1/2</i>	<b>In or out interface of packet</b>
<i>Ack 56/88</i>	<b>Acknowledgement number of packet/ sequence number of neighbor packet</b>

## Related commands

**debug ip beigrp fsm**

### 54.1.7 debug ip beigrp transmit

To display transmit event of BEIGRP packet, use the debug ip beigrp transmit command in EXEC mode.

**debug ip beigrp transmit [ack | build | link | packetize | peerdnwn | startup]**

**no debug ip beigrp transmit [ack | build | link | packetize | peerdnwn | startup]**

## Parameter

field	Description
<i>ack</i>	<b>(Optional) Traces events</b>
<i>build</i>	<b>(Optional)Traces BUILD events.</b>
<i>link</i>	<b>(Optional)Traces LINK events</b>
<i>packetize</i>	<b>(Optional)Traces PACKETIZE events.</b>
<i>peerdnwn</i>	<b>(Optional)Traces PEERDOWN events</b>
<i>startup</i>	<b>(Optional)Traces STARTUP events.</b>

## Default

none

## Command mode

EXEC

### Instruction

It helps to find network malfunction using this command.

### Related commands

**debug ip beigrp fsm**

### 54.1.8 default-metric

To reset the default vector metric for the Enhanced Interior Gateway Routing Protocol (BEIGRP), use the default-metric command in routing switch configuration mode. To restore the default state, use the no form of this command.

**default-metric bandwidth delay reliability loading mtu**

**no default-metric**

### Parameter

parameter	Description
<i>bandwidth</i>	<b>Default bandwidth</b>
<i>delay</i>	<b>Default interface delay.</b>
<i>reliability</i>	<b>Default interface reliability</b>
<i>loading</i>	<b>Default interface load</b>
<i>mtu</i>	<b>The default value for the maximum transmission unit (MTU),</b>

### Default

bandwidth: 128kpbs

delay: 2000 (10ms)

reliability: 255 (255 indicates 100%)

loading: 255 (255 indicates 100%)

mtu: 1500

### Command mode

router configuration

### Instruction

it is generally used with redistribute command to specify default metrics of route of other routing protocols assigned into BEIGRP. This command will trigger the new algorithm of related route that are previously assigned into BEIGRP.

Forwarding static route, straight connected route and BEIGRP protocol route, you can not configure default-metric command, or you must configure this command

### Example

The following example shows how the redistributed Routing Information Protocol (RIP) metrics are translated into EIGRP metrics with values as follows: bandwidth = 200, delay = 100, reliability = 100, loading = 200, and MTU = 1500:

```
default-metric 200 1000 100 200 1500
```

## Related commands

### redistribute

#### 54.1.9 distance

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the distance beigrp command in routing switch configuration mode. To reset these values to their defaults, use the no form of this command.

**distance beigrp internal-distance external-distance no distance beigrp**

**distance weight ip-address ip-address-mask [ip-access-list]**

**no distance weight ip-address ip-address-mask [ip-access-list]**

## Parameter

parameter	Description
<i>internal-distance</i>	<b>Administrative distance for Enhanced Internal Gateway Routing Protocol (BEIGRP) internal routes. The distance can be a value from 1 to 255.</b>
<i>external-distance</i>	<b>Administrative distance for EIGRP external routes. The distance can be a value from 1 to 255.</b>
<i>ip-address</i>	<b>BEIGRP neighbor IP address</b>
<i>ip-address-mask</i>	<b>BEIGRP neighbor IP address mask</b>
<i>ip-access-list</i>	<b>BEIGRP neighbor access list</b>

## Default

internal-distance: 90

external-distance: 170

## Command mode

router configuration

## Instruction

An administrative distance is to compare the priority of routes of different protocols. Therefore, adjustment on the administrative distance value of BEIGRP will affect the choice of routing switch to meet different demands of users.

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list.

## Example

```
router beigrp 2
```



```
network 192.10.0.0 255.255.0.0
distance beigrp 100 200
distance 110 192.31.7.0 255.255.255.0
distance 220 128.88.1.0 255.255.255.0
```

In the above example, the routing switch beigrp global configuration command sets up BEIGRP internal administrative and external administrative to 100 and 200. The network routing switch configuration commands specify BEIGRP routing on networks 192.31.7.0/24 and 128.88.1.0/24 to 110 and 220.

## Related commands

### show ip protocol

#### 54.1.10 filter

To allows us to filter the routes that learned or sent on the specified interface, use the filter command. Use the no form of this command to disable filter.

```
filter {interface-type interface-number | *} {in | out} {access-list access-list-name |
gateway access-list-name | prefix-list prefix-list-name}
no filter {interface-type interface-number | *} {in | out} {access-list access-list-name |
gateway access-list-name | prefix-list prefix-list-name}
```

## Parameter

parameter	Description
<i>interface-type</i> <i>interface-number</i>	<b>Interface type and number</b>
*	<b>all interfaces</b>
<i>in</i>	<b>Applies access-list to the incoming routing update</b>
<i>out</i>	<b>Applies access-list to the ourcoming routing update</b>
<i>access-list</i>	<b>Applies standard access list to filter routes, to define which network is sent and which network is suppressed in routing update.</b>
<i>gateway</i>	<b>Filters gateway of route using standard access list.</b>
<i>access-list-name</i>	<b>Standard IP access list number or name</b>
<i>prefix-list</i>	<b>Filters route using the prefix-list</b>
<i>prefix-list-name:</i>	<b>Standard IP prefix- list-name. This list defines which networks are received and which are surpressed.</b>

## Default

none

## Command mode

router configuration

## Instruction

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list.

## Example

The following example permits only one network at 131.108.0.0 to be declared by BEIGRP routing process:

```
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255

router beigrp 64
network 131.108.0.0

filter * out 1
```

### 54.1.11 *beigrp log-neighbor-changes*

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (BEIGRP) neighbor adjacencies, use the `beigrp log-neighbor-changes` command in router configuration mode. To disable the logging of changes in BEIGRP neighbor adjacencies, use the `no` form of this command.

**beigrp log-neighbor-changes**

**no beigrp log-neighbor-changes**

#### Parameter

none0

#### Default

disabled

#### Command mode

router configuration

### 54.1.12 *beigrp router-id*

To set the routing switch ID used by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the `eigrp router-id` command in router configuration mode. To remove the configured routing switch ID, use the `no` form of this command.

**beigrp router-id *ip-address***

**no beigrp router-id**

#### Parameter

parameter	Description
<i>ip-address</i>	Router ID in dotted decimal notation.

## Default

EIGRP automatically selects an IP address to use as the routing switch ID. Set the largest loopback interface as the routing switch ID if there is a loopback interface or set the largest direct-connect interface address as the the routing switch ID.

## Command mode

router configuration

### 54.1.13 *ip beigrp bandwidth-percent*

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (BEIGRP) on an interface, use the `ip bandwidth-percent eigrp` command. To restore the default value, use the `no` form of this command.

**ip beigrp bandwidth-percent** *percent*

**no ip beigrp bandwidth-percent** *percent*

## Parameter

parameter	Description
<i>percent</i>	Percent of bandwidth that EIGRP may use.

## Default

50%

## Command mode

interface configuration mode

## Instruction

For low speed lines, you can adjust the configuration of this command to restrict the enabled bandwidth for BEIGRP to avoid that BEIGRP affect the normal data transmission. .

## Example

```
interface Ethernet1/1
```

```
ip beigrp bandwidth-percent 100
```

The above example allows BEIGRP to use all bandwidth of the interface

## Related commands

bandwidth

### 54.1.14 *ip beigrp hello-interval*

To configure the hello interval for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the `ip hello-interval eigrp` command in interface configuration mode. To restore the default value, use the `no` form of this command.

**ip beigrp hello-interval** *seconds*

**no ip beigrp hello-interval** *seconds*

Parameter

parameter	Description
<i>second</i>	Hello interval (in seconds).

Default

5 seconds-

Command mode

interface configuration mode

Instruction

Example

```
interface Ethernet1/1
```

```
ip beigrp hello-interval 20
```

The above example sets 20 seconds as the hello interval for ethernet1/1:

Related Commands

**ip beigrp hold-time**

*54.1.15 ip beigrp hold-time*

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the `ip hold-time eigrp` command in interface configuration mode. To restore the default value, use the `no` form of this command.

**ip beigrp hold-time** *seconds*

**no ip beigrp hold-time** *seconds*

Parameter

parameter	Description
<i>second</i>	Hold time is in seconds if do not receive any BEIGRP

Default

15 seconds

Command mode

interface configuration mode

Instruction

### Example

```
interface Ethernet1/1
ip beigrp hold-time 60
```

The above example sets 60 seconds the hold time for ethernet1/1:

### Related commands

#### **ip beigrp hello-interval**

#### *54.1.16 ip beigrp passive*

To enable interacting BEIGRP routing update on a certain interface, use the `ip beigrp passive` command. Use the `no` form of this command to restore the default value.

#### **ip beigrp passive**

#### **no ip beigrp passive**

#### Parameter

none

#### Default

the interface is not in passive mode

#### Command mode

interface configuration mode

#### Instruction

If the `ip beigrp passive` is configured on an interface, then no routing update is received on this interface, and also no neighborhood relation is established between this interface and any accessible neighbors. But a direct route generate on this interface will be broadcast by other interface that runs the BEIGRP.

### Example

The following command set ethernet1/1 as the passive interface:

```
interface ethernet1/1
ip beigrp passive
```

#### *54.1.17 ip beigrp split-horizon*

To enable Enhanced Interior Gateway Routing Protocol (BEIGRP) split horizon, use the `ip beigrp split-horizon` command in interface configuration mode. To disable split horizon, use the `no` form of this command.

#### **ip beigrp split-horizon**

#### **no ip beigrp split-horizon**

#### Parameter

none

### Default

The behavior of this command is enabled by default.

### Command mode

interface configuration mode

### Instruction

Using this command is to prevent route cycle, so you must confirm that it will not cause any bad effects before turn off the split horizon.

### Example

```
interface Ethernet1/1
```

```
no ip beigrp split-horizon
```

The above example disables split horizon on ethernet 1/1:

#### **54.1.18 ip beigrp summary-address**

To configure a summary aggregate address for a specified interface, use the `ip beigrp summary-address` command in interface configuration mode. To disable a configuration, use the `no` form of this command.

**ip beigrp summary-address** *as\_number address mask*

**no ip beigrp summary-address** *as\_number address mask*

### Parameter

parameter	Description
<i>as_number</i>	<b>Autonomous system number.</b>
<i>address</i>	<b>Summary IP address to apply to an interface.</b>
<i>mask</i>	<b>Subnet mask.</b>

### Default

none

### Command mode

interface configuration mode

### Instruction

The following is default behavior if an incomplete configuration is entered:

When the `ip beigrp summary-address` command is configured on an interface, the summary routes of the defined network are generated as if there is a subnet in BEIGRP topology table.

The summary routes point to Null0 interface, which have the minimum distance of all the concrete routes that summary routes contain. The summary routes insert to the main IP routing table, and the administrative distance is 5(which cannot be configured).

Configuring the sending of routing updates on an interface in the rummary routes range cancels concrete routes that belong to the summary network. The update sent to the other interfaces is not affected.

### Example

an administrative distance of 95 on interface Ethernet 0/0 for the 192.168.0.0/16

summary address:

```
interface Ethernet1/1
```

```
ip beigrp summary-address 100 12.1.0.0 255.255.0.0
```

The above example configures all the concrete routes that belong to the network 12.1.0.0/16(which belong to router beigrp 100) not to be broadcast on ethernet1/1

### Related commands

#### **auto-summary**

#### *54.1.19 metric weights*

To tune Enhanced Interior Gateway Routing Protocol (BEIGRP) metric calculations, use the metric weights command in routing switch configuration mode. To reset the values to their defaults, use the no form of this command

```
metric weights k1 k2 k3 k4 k5
```

```
no metric weights
```

#### Parameter

parameter	Description
<i>k1,k2,k3,k4,k4</i>	<b>Constants that convert an EIGRP metric vector into a scalar quantity.</b>

#### Default

k1: 1

k2: 0

k3: 1

k4: 0

k5: 0

#### Command mode

router configuration

#### Instruction

Use this command to alter the default behavior of EIGRP routing and metric computation and allow the tuning of the EIGRP metric calculation for a particular type of service (ToS).

The tuning of the EIGRP metric calculation for a composite metric adopts two steps:

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

$$\text{metric} = [k1 * \text{bandwidth} + (k2 * \text{bandwidth}) / (256 - \text{load}) + k3 * \text{delay}]$$

If k5 does not equal zero, an additional operation is performed:

$$\text{Composite metric} = \text{Composite metric} * [k5 / (\text{reliability} + k4)]$$

K2, K4 and K5 are the left objects of IGRP, compatible with Eigrp protocol of Cisco. In general, Load and Reliability are not used in composite metric algorithm. Therefore, do not change the default value of K2, K4 and K5, unless you confirm that will not cause bad effect, to prevent unexpected result on route decision

### Example

```
router beigrp 2
network 131.108.0.0 255.255.0.0
metric weights 2 0 2 0 0
```

### Related commands

#### bandwidth

#### delay

#### 54.1.20 network

To specify the network for an Enhanced Interior Gateway Routing Protocol (BEIGRP) routing process, use the network command in routing switch configuration mode. To remove an entry, use the no form of this command.

**network** *network-number* [*netmask*]

**no network** *network-number* [*netmask*]

### Parameter

parameter	Description
<i>network-number</i>	<b>Network address.</b>
<i>netmask</i>	<b>Network mask.</b>

### Default

none

### Command mode

router configuration

### Instruction



Various network statements (network commands) can be configured on a routing switch, to enable BEIGRP dynamic routing protocol to run on many networks; use the default mask if there is no configured mask.

### Example

```
router beigrp 2
network 131.108.0.0 255.255.0.0
network 122.11.2.0
```

### Related commands

#### router beigrp

#### 54.1.21 offset

To add an offset to incoming and outgoing metrics to routes learned via Enhanced Interior Gateway Routing Protocol (BEIGRP), use the offset command in router configuration mode. To remove an offset list, use the no form of this command.

**offset** {*type number* | \*} {*in* | *out*} *access-list-name* **offset**

**no offset** {*type number* | \*} {*in* | *out*}

### Parameter

parameter	Description
<i>In</i>	<b>Applies the access list to incoming metrics.</b>
<i>Out</i>	<b>Applies the access list to outgoing metrics.</b>
<i>access-list-name</i>	<b>Standard access list name to be applied</b>
<i>Offset</i>	<b>Positive offset to be applied to metrics for networks matching the access list.</b>
<i>Type</i>	<b>(Optional) Interface type to which the offset list is applied.</b>
<i>Number</i>	<b>(Optional) Interface number to which the offset list is applied.</b>

### Default

none

### Command mode

router configuration

### Instruction

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

BEIGRP is a vector metric, so the offset is added to delay

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list

### Example

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 21:

```
offset * out 21 10
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

```
offset e0/0 in 21 10
```

### Related commands

ip access-list

#### 54.1.22 redistribute

To redistribute routes from other routing protocols into the local BEIGRP routing process routing table, use the redistribute command.

**redistribute protocol [process] route-map name**

**redistribute protocol [process]**

### Parameter

parameter	Description
<i>protocol</i>	Source protocol from which routes are being redistributed. It must be one of following keywords: <b>bgp, ospf, static, connected, and rip.</b>
<i>process</i>	(Optional) For <b>bgp</b> or <b>bigp</b> , this parameter indicates the 16-digit autonomous number. For <b>OSPF</b> , this parameter indicates the relevant OSPF process ID of the routes need to be redistributed. This marks the routing process. It is a non-zero decimal number. For <b>rip</b> , there is no need to mark the process.
<i>route-map</i>	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to IS-IS. If not specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported.
<i>name</i>	Name character string of route-map

### Default

none

### Command mode

BEIGRProuter configuration

### Instruction

To redistribute direct routes, static routes and routes from other BEIGRP process, the default-metric command is not necessarily to be configured; otherwise, the default-metric must be configured.

### Example

```
default-metric 64 250 255 255 1500
```

```
redistribute ospf 1
```

### 54.1.23 router beigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the router beigrp command in global configuration mode. To delete the BEIGRP routing process, use the no form of this command.

```
router beigrp autonomous-system-number
```

```
no router beigrp autonomous-system-number
```

### Parameter

parameter	Description
<i>autonomous-system-number</i>	<b>Autonomous system number that identifies the routes to the other BEIGRP routers.</b>

### Default

none

### Command mode

global configuration mode

### Instruction

This command can be used to operate multiple BEIGRP processes.

### Example

The following example configures EIGRP process 30:

```
router beigrp 30
```

### Related commands

network

### 54.1.24 show ip beigrp interface

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the show ip beigrp interfaces command in privileged EXEC mode.

```
show ip beigrp interfaces [interface-type interface-number] [as-number]
```

### Parameter

parameter	Description
-----------	-------------

<i>as-number</i>	<b>Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process</b>
<i>interface</i>	<b>Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface</b>

### Default

none

### Command mode

EXEC or global configuration mode

### Instruction

Use the show ip eigrp interfaces command to learn information about BEIGRP dynamic routing relating to those interfaces.

### Related commands

**show ip beigrp topology**

#### *54.1.25 show ip beigrp neighbors*

To display neighbors discovered by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the show ip eigrp neighbors command in EXEC mode.

**show ip beigrp neighbors** [*interface-type interface-number*] [*as-number*] [*detail*]

### Parameter

parameter	Description
<i>as-number</i>	<b>Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process</b>
<i>interface</i>	<b>Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface</b>
<i>detail</i>	<b>Displays detailed neighbor information.</b>

### Default

none

### Command mode

EXEC or global configuration mode

### Instruction

Use the show ip beigrp neighbors command to determine what neighbours they are and when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

### Example

```
Router# show ip beigrp neighbors
```

```
Information of BEIGRP neighbors with AS 1024 Address      interface      hold uptime
Q_cnt Seq
192.168.20.204    Ethernet1/1  15    00:08:06    0    159
202.117.80.143   Ethernet2/1  10    00:08:05    0    100
192.168.20.141   Ethernet1/1  12    00:07:38    0    254
```

field	explanation
<i>AS 64</i>	<b>Autonomous system number</b>
<i>Address</i>	<b>IP address of the BEIGRP peer.</b>
<i>Interface</i>	<b>Interface on which the router is receiving hello packets from the peer.</b>
<i>Hold</i>	<b>Length of time that the software will wait to hear from the peer before declaring it down.</b>
<i>Uptime</i>	<b>Elapsed time since the local router first heard from this neighbor.</b>
<i>Q Count</i>	<b>Number of EIGRP packets that the software is waiting to send.</b>
<i>Seq</i>	<b>Sequence number of the last update that was received from this neighbor.</b>

## Related commands

**show ip beigrp topology**

### 54.1.26 show ip beigrp protocol

To display the Enhanced Interior Gateway Routing Protocol (BEIGRP) routing protocol process parameter and statistics, use the `show ip beigrp protocols` command.

**show ip beigrp protocols** [*as-number*]

## Parameter

field	explanation
<i>as-number</i>	<b>(Optional) Autonomous system number. If the parameter is specified, it will display only the parameters and statistics of this BEIGRP process</b>

## Command mode

EXEC or global configuration mode

## Instruction

This command can be used to check BEIGRP topology table at any time.

## Example

```
R142#show ip bei pro
```

Protocol Information of BEIGRP with AS 1024:

Metric Weight: K1=1, K2=0, K3=1, K4=0, K5=0.

Filter \* in access-list in12

Filter \* out access-list ou12

Offset \* in in23 12

Offset \* out ou23 12

Redistributing: connect, ospf 1, ospf 2

Automatic network summarization is enable.

Active-time: 3(minutes)

Routing for Networks: 192.168.20.0/24

10.0.0.0/8

167.20.0.0/16

202.117.80.0/24

Distance: internal 90, external 170

Active Route:

## Related commands

### show ip beigrp topology

#### 54.1.27 show ip beigrp topology

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the show ip beigrp topology command in privileged EXEC mode.

**show ip beigrp topology** [*as-number*] [*network-number subnet-mask*] [*active*] [*all-links*] [*pending*] [*summary*] [*zero-successors*]

#### Parameter

parameter	description
<i>as-number</i>	<b>(Optional) Autonomous system number. If the parameter is specified, it will display only the topology table of BEIGRP process</b>
<i>network-number</i>	<b>Displays detailed information about the specified network.</b>
<i>subnet-mask</i>	<b>(Optional) Subnet mask.</b>
<i>active</i>	<b>(Optional) Displays only active entries in the BEIGRP topology table.</b>
<i>all-link</i>	<b>(Optional) Displays all entries in the BEIGRP topology table.</b>
<i>pending</i>	<b>(Optional) Displays all entries in the BEIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.</b>
<i>summary</i>	<b>(Optional) Displays a summary of the BEIGRP topology table.</b>

<i>zero-successors</i>	<b>(Optional) Displays available routes in the EIGRP topology table.</b>
------------------------	--

**Default**

none

**Command mode**

EXEC or global configuration mode

**Instruction**

This command can be used to check BEIGRP topology table at any time.

**Example**

```
Router# show ip beigrp topology
P 10.10.10.0/24 successors: 1 FD: 13056
via connect(Loopback1) Metric: 13056/0
P 167.20.0.0/16 successors: 1 FD: 261132
via 202.117.80.143(Ethernet2/1) Metric: 261132/258560
P 192.166.100.0/24 successors: 1 FD: 281856
via redistribute Metric: 281856/0
P 192.168.20.0/24 successors: 1 FD: 258560
via connect(Ethernet1/1) Metric: 258560/0
P 202.1.1.0/24 successors: 1 FD: 297246988
via 192.168.20.204(Ethernet1/1) Metric: 297246988/297244416
P 202.117.80.0/24 successors: 1 FD: 258560
via connect(Ethernet2/1) Metric: 258560/0
A 202.117.93.0/24 successors: 1 FD: unreachable, R serno: 32
via 192.168.20.141(Ethernet1/1) Metric: 271372/13056
SIA-Info: (active: 00:02:20 query-origin: Local origin)
Unreplied Neighbors:
via 202.117.80.143, Ethernet2/1
P 202.192.168.0/24 successors: 1 FD: 284172
via 192.168.20.204(Ethernet1/1) Metric: 284172/281600
```

field	description
<i>160.89.90.0 and so on</i>	<b>Destination network number</b>
<i>255.255.255.0</i>	<b>Destination network mask</b>
<i>successors</i>	<b>Number of successors.</b>
<i>FD</i>	<b>Feasible distance.</b>
<i>Via</i>	<b>Gateway address</b>
<i>Ethernet1/1</i>	<b>Interface from which this information was learned.</b>
<i>SIA-Info</i>	<b>active routing information</b>
<i>active</i>	<b>Lasting time when entering Active status.</b>
<i>query-origin</i>	<b>Origin of entering query state</b>
<i>Unreplied Neighbors</i>	<b>Neighbor lists that are not received reply.</b>

### Related commands

**show ip beigrp neighbor**

#### *54.1.28 show ip beigrp traffic*

To display the flow information of Enhanced Interior Gateway Routing Protocol (BEIGRP) packets sent and received, use the show ip beigrp traffic command in EXEC mode.

**show ip beigrp traffic** [*as-number*]

### Parameter

field	description
<i>as-number</i>	<b>(Optional) Autonomous system number. If the parameter is specified ,then display the flow statistics information</b>

### Default

none

### Command mode

EXEC or global configuration mode

### Instruction

Use this command to check the flow statistics information of BEIGRP packets sent and received at any time.

### Example

```
R142#show ip bei tra
```

```
Traffic Statistics of BEIGRP 1024
```



Packet Type	Hello	Update	Query Reply	ACK		
Send/Receive	770/1021	133/44	29/7	7/9	60/147	

Related commands

`show ip beigrp topology`

## Chapter 55 OSPF Configuration Commands

### 55.1 OSPF Configuration Commands

OSPF Configuration Commands Include:

- `area authentication`
- `area default-cost`
- `area range`
- `area stub`
- `area virtual-link`
- `debug ip ospf adj`
- `debug ip ospf events`
- `debug ip ospf flood`
- `debug ip ospf lsa-generation`
- `debug ip ospf packet`
- `debug ip ospf retransmission`
- `debug ip ospf spf`
- `debug ip ospf tree`
- `default-information originate`
- `default-metric`
- `distance ospf`
- `filter`
- `ip ospf cost`
- `ip ospf dead-interval`
- `ip ospf hello-interval`
- `ip ospf message-digest-key`
- `ip ospf network`
- `ip ospf passive`
- `ip ospf password`

- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- neighbor
- network area
- redistribute
- router ospf
- show ip ospf
- show ip ospf border-routers
- show ip ospf database
- show ip ospf interface
- show ip ospf neighbor
- show ip ospf virtual-link
- summary-address
- timers delay
- timers hold

### 55.1.1 area authentication

To enable authentication for an Open Shortest Path First (OSPF) area, use the area authentication command in routing switch configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command.

**area** *area-id* **authentication** [**simple** | **message-digest**]

**no area** *area-id* **authentication**

**no area** *area-id*

Parameter

parameter	description
<i>area-id</i>	Identifier of the area for which authentication is to be enabled.
<i>simple</i>	(Optional) authentication information, Plain text authentication
<i>message-digest</i>	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument.

Default

no authentication of interface receiving OSPF packet by default

## Command mode

router configuration

## Instruction

The authentication value will be added into OSPF packet. The authentication type of all routing switches in the same area must be the same. The authentication password for all OSPF routing switches on a network must be the same if they are to communicate with each other via OSPF..

## Example

The following example mandates authentication simple for areas 0 and 36.0.0.0.

```
interface ethernet 1/0
ip address 131.119.251.201 255.255.255.0
ip ospf password adcdefgh
!
interface ethernet 1/0
ip address 36.56.0.201 255.255.0.0
ip ospf password ijklmnop
!
router ospf 1
network 36.0.0.0 255.0.0.0 area 36.0.0.0
network 131.119.0.0 255.255.0.0 area 0
area 36.0.0.0 authentication simple
area 0 authentication simple
```

## Related commands

**ip ospf password**

**ip ospf message-digest-key**

### *55.1.2 area default-cost*

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the `area default-cost` command in router address family topology or routing switch configuration mode. To remove the assigned default route cost, use the no form of this command.

**area *area-id* default-cost *cost***

**no area *area-id* default-cost**

**no area *area-id***

## Parameter

parameter	description
<i>area-id</i>	Identifier for the stub area.
<i>cost</i>	Cost for the default summary route used for a stub

## Default

cost.1

## Command mode

router configuration

## Instruction

This command is used only on an routing switch attached to a stub area or NSSA.

After configured the area stub default-information-originate command, the routing switch will send LSA(SUM-NER-LSA) including default router information to correspondent field, the cost configured I this command is the correspondent cost used in LSA.

## Note:

To remove the specified area from the software configuration, use the no area area-id command (without other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

## Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet 1/0
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 255.0.0.0 area 36.0.0.0
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20
```

## Related commands

**area nssa**

**area stub**

### 55.1.3 area range

To consolidate and summarize routes at an area boundary, use the area range command. To disable this function, use the no form of this command.

**area area-id range address mask[ not-advertise ]**

**no area** *area-id range address mask not-advertise*

**no area** *area-id range address mask*

**no area** *area-id*

#### Parameter

parameter	description
<i>area-id</i>	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix.
<i>address</i>	IP address
<i>mask</i>	IP address mask
<i>advertise</i>	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
<i>not-advertise</i>	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

#### Default

This command is disabled by default.

#### Command mode

router configuration

#### Instruction

The area range command is used only with Area Border Routing switches. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization.

Multiple area range routing switch configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note: To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, such as `area default-cost`, `area nssa`, `area range`, `area stub`, and `area virtual-link`.

#### Example

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
interface ethernet 0
ip address 192.42.110.201 255.255.255.0
!
```

```

interface ethernet 1
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 255.0.0.0 area 36.0.0.0
network 192.42.110.0 255.0.0.0 area 0
area 36.0.0.0 range 36.0.0.0 255.0.0.0
area 0 range 192.42.110.0 255.255.255.0

```

#### 55.1.4 area stub

To define an area as a stub area, use the `area stub` command. To disable this function, use the `no` form of this command.

**area** *area-id* **stub** [**no-summary**]

**no area** *area-id* **stub**

**no area** *area-id*

#### Parameter

parameter	description
<i>area-id</i>	Identifier for the stub area; either a decimal value or an IP address.
<i>no-summary</i>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

#### Default

No stub area is defined.

#### Command mode

router configuration

#### Instruction

You must configure the `area stub` command on all routers and access servers in the stub area. Use the `area router configuration` command with the `default-cost` keyword to specify the cost of a default internal route sent into a stub area by an ABR switch.

There are two stub area router configuration commands: the `stub` and `default-cost` options of the `area routing switch configuration` command. In all routing switches attached to the stub area, the area should be configured as a stub area using the `stub` keyword of the `area` command. Use the `default-cost` keyword only on an ABR attached to the stub area. The `default-cost` keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the `no-summary` keyword on the ABR switch to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Note: To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, such as `area authentication`, `area default-cost`, `area nssa`, `area range`, `area stub`, and `area virtual-link`.

### Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet 0
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 255.0.0.0 area 36.0.0.0
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20
```

### Related commands

**area authentication**

**area default-cost**

#### 55.1.5 area virtual-link

To define a virtual link, use the `area virtual-link` command

```
area area-id virtual-link neighbor-ID [authentication simple | message-digest] [dead-interval dead-value][ hello-interval hello-value][ retransmit-interval retrans-value][ transdly dly-value][ password pass-string] [ message-digest-key key-id MD5 md5-string]
```

```
no area area-id virtual-link neighbor-ID
```

### Parameter

parameter	description
<i>area-id</i>	Area ID assigned to the transit area for the virtual link.
<i>neighbor-id</i>	Router ID associated with the virtual link neighbor.
<i>simple</i>	Plain text authentication. The value must be the same for all routing switches and access servers attached to a common network.
<i>message-digest</i>	Enables Message Digest 5 (MD5) on virtual-link. The value must be the same for all routing switches and access servers attached to a common network.
<i>dead-value</i>	Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The value must be the same for all routing switches and access servers attached to a common network.

<i>hello-value</i>	<b>Time (in seconds) between the hello packets that the software sends on an interface. The value must be the same for all routing switches and access servers attached to a common network.</b>
<i>retrans-value</i>	<b>Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be the same for all routing switches and access servers attached to a common network.</b>
<i>dly-value</i>	<b>Delay value in seconds to inform LSA on virtual-link for a routing switch. The configured value on both sides of the virtual-link should be the same.</b>
<i>pass-string</i>	<b>If virtual-link uses plain text authentication, the the maximum character of the configured password should be 8. The configured value on both sides of the virtual-link should be the same.</b>
<i>key-id</i>	<b>If virtual-link uses MD5 authentication, the valid range of the used MD5 key should from 1 to 255. The configured value on both sides of the virtual-link should be the same.</b>
<i>MD5-String</i>	<b>Configures MD5 password, which is 16-character at most. The configured value on both sides of the virtual-link should be the same.</b>

## Default

No virtual-link is configured.

Default value of other parameters are as follows:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s, no authentication

## Command mode

OSPFrouter configuration

## Instruction

To establish a virtual link, user should configure both sides of the virtual link. The virtual link will fail if this command is only configured on one side.

The parameter-id must be a non-zero character, for the virtual link and the transit area must be a non-backbone area. The configured area-id of the virtual link must be the same.

The neighbor-ID must be the same as the ospf router-id on the remote side during configuration, or the virtual link will not be established. Even if the configured neighbor-ID is another IP address of the other side.

You must make sure that all parameters on both sides must be the same.

The authentication parameters that configured on virtual-link become effective only when configured authentication types of virtual-link or configured the relevant authentication methods in backbone are (via the command area authentication) Only one kind of authentication parameter can be configured on virtual-link, that is, the MD5 and the plain text authentication are mutually exclusive.



Use the command `no area area-id virtual-link neighbor-ID` to cancel the formerly-configured virtual link.

Use the command `show ip ospf virtual-link` to check state of the virtual link.

### Example

The following example configured a virtual link between router A and router B: The configuration on router A (router-id: 200.200.200.1)

```
!  
router ospf 100  
network 192.168.20.0 255.255.255.0 area 1  
area 1 virtual-link 200.200.200.2
```

```
!
```

The configuration on router B :

```
!
```

```
router ospf 100  
network 192.168.30.0 255.255.255.0 area 1  
area 1 virtual-link 200.200.200.1
```

```
!
```

### Related commands

**show ip ospf virtual-link**

#### *55.1.6 debug ip ospf adj*

To monitor Open Shortest Path First (OSPF)-related establishment process , use the `debug ospf adj` command

**debug ip ospf adj**

#### Parameter

none

#### Default

none

#### Command mode

EXEC

#### Instruction

User can check the process of OSPF-related establishment process from the output of this command.

### Example

```
Router# debug ip ospf adj
OSPF: Interface 192.168.40.0 on Serial1/0 going down
OSPF NBR: 192.168.40.2 address 192.168.40.2 on Serial1/0 is dead, state DOWN
OSPF NBR: 192.168.40.3 address 192.168.40.3 on Serial1/0 is dead, state DOWN
Line on Interface Serial1/0, changed state to up
Line protocol on Interface Serial1/0 changed state to up
OSPF: Interface 192.168.40.0 on Serial1/0 going Up
OSPF: 2 Way Communication to 192.168.40.2 on Serial1/0, state 2WAY
OSPF: NBR 192.168.40.2 on Serial1/0 Adjacency OK, state NEXSTART.
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.2 on Serial1/0 Negotiation Done. We area the SLAVE
OSPF: Exchange Done with 192.168.40.2 on Serial1/0
OSPF: Loading Done with 192.168.40.2 on Serial1/0, database Synchronized (FULL)
OSPF: 2 Way Communication to 192.168.40.3 on Serial1/0, state 2WAY
OSPF: NBR 192.168.40.3 on Serial1/0 Adjacency OK, state NEXSTART.
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.3 on Serial1/0 Negotiation Done. We area the SLAVE
OSPF: Bad Sequence with 192.168.40.3 on Serial1/0, state NEXSTART
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.3 on Serial1/0 Negotiation Done. We area the SLAVE
OSPF: Exchange Done with 192.168.40.3 on Serial1/0
OSPF: Loading Done with 192.168.40.3 on Serial1/0, database Synchronized (FULL)
.....
```

### *55.1.7 debug ip ospf events*

To monitor OSPF interface and OSPF-related events, , use the `debug ip ospf events` command.

#### **debug ip ospf events**

##### **Parameter**

none

##### **Default**

none

##### **Command mode**

EXEC

### Instruction

To display OSPF interface and OSPF-related adjacency events from the output of this command.

### Example

```
Router# debug ip ospf events OSPF: Interface Serial1/0 going Up
```

```
OSPF: INTF(192.168.40.0) event INTF_UP
```

```
OSPF: NBR(192.168.40.2) event HELLO_RX
```

```
OSPF: NBR(192.168.40.2) event TWOWAY
```

```
OSPF: NBR(192.168.40.2) event ADJ_OK
```

```
OSPF: NBR(192.168.40.2) event NEGO_DONE
```

```
OSPF: NBR(192.168.40.2) event EXCH_DONE
```

```
OSPF: NBR(192.168.40.2) event LOAD_DONE
```

```
OSPF: NBR(192.168.40.3) event HELLO_RX
```

```
OSPF: NBR(192.168.40.3) event TWOWAY
```

```
OSPF: NBR(192.168.40.3) event ADJ_OK
```

```
OSPF: NBR(192.168.40.3) event NEGO_DONE
```

```
OSPF: NBR(192.168.40.3) event SEQ_MISMATCH
```

```
OSPF: NBR(192.168.40.3) event NEGO_DONE
```

```
OSPF: NBR(192.168.40.3) event EXCH_DONE
```

```
OSPF: NBR(192.168.40.3) event LOAD_DONE
```

```
.....
```

### *55.1.8 debug ip ospf flood*

To display OSPF-related database pervasion process, use the debug ip ospf flood command.

### **debug ip ospf flood**

#### Parameter

none

#### Default

none

#### Command mode

EXEC

#### Instruction

To display OSPF-related database pervasion process from the output of this command.

### Example

```
Router# debug ip ospf flood
```

```
OSPF: rcv UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022B
```

```
OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ  
0x80000234
```

```
OSPF: Send ACK, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022B
```

```
OSPF: rcv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ  
0x80000234
```

```
OSPF: rcv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 18 SEQ  
0x80000233
```

```
OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 10 SEQ  
0x8000022B
```

```
OSPF: rcv UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021C
```

```
OSPF: Send UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ  
0x8000021C
```

```
OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ  
0x80000235
```

```
OSPF: rcv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 4 SEQ 0x8000021C
```

```
.....
```

### *55.1.9 debug ip ospf lsa-generation*

To display OSPF-related LSA generation process, use the debug ip ospf lsa generation command.

#### **debug ip ospf lsa-generation**

##### Parameter

none

##### Default

none

##### Command mode

EXEC

##### Instruction

To display OSPF interface and adjacency events from the output of this command.

### Example

```
router# debug ip ospf lsa-generation
```

.....

```
OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 10 SEQ
0x8000022D
OSPF: rcv UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021E
OSPF: Send UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021E
OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ
0x80000239
OSPF: rcv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 4 SEQ 0x8000021E
OSPF: Send ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021E
OSPF: rcv UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 1 SEQ 0x8000022E
OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022E
OSPF: rcv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ
0x80000239
OSPF: rcv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021E
OSPF: rcv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ
0x80000239
```

.....

### ***55.1.10 debug ip ospf packet***

To display OSPF packets, use the `debug ip ospf packet` command.

#### **debug ip ospf packet**

##### **Parameter**

none

##### **Default**

none

##### **Command mode**

EXEC

##### **Instruction**

To display OSPF interface and adjacency events from the output of this command.

##### **Example**

```
router# debug ip ospf packet
```

.....

```
OSPF: Recv HELLO packet from 192.168.40.3 (addr: 192.168.40.3) area 0 from Serial1/0
OSPF: End of hello processing
```

```
OSPF: Send HELLO to 224.0.0.5 on Loopback0
      HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
OSPF: Send HELLO to 224.0.0.5 on Loopback0
      HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
OSPF: Send HELLO to 224.0.0.5 on Loopback0
      HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
OSPF: Recv HELLO packet from 192.168.40.2 (addr: 192.168.40.2) area 0 from Serial1/0
OSPF: End of hello processing
OSPF: Send HELLO to 224.0.0.5 on Serial1/0
      HelloInt 30 Dead 120 Opt 0x2 Pri 1 len 52
OSPF: Recv HELLO packet from 192.168.40.3 (addr: 192.168.40.3) area 0 from Serial1/0
OSPF: End of hello processing
OSPF: Send HELLO to 224.0.0.5 on Loopback0
      HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
.....
```

#### ***55.1.11 debug ip ospf retransmission***

To display retransmission of OSPF pakeket, uset the debug ip ospf retransmission command;

#### **debug ip ospf retransmission**

##### **Parameter**

none

##### **Default**

none

##### **Command mode**

EXEC

##### **Instruction**

To display transmission processo OSPF packets.

##### **Example**

```
router# debug ip ospf retransmission
OSPF: retransmit UPDATE to 192.168.40.3 (RID 192.168.40.3), state FULL
.....
```

#### ***55.1.12 debug ip ospf spf***

To display information of SPF algorithm, use the debug ip ospf spf statistic command

---

```
debug ip ospf spf statistic
```

```
debug ip ospf spf
```

```
debug ip ospf spf intra
```

```
debug ip ospf spf inter
```

```
debug ip ospf spf external
```

#### Parameter

none

#### Default

none

#### Command mode

EXEC

#### Instruction

The `debug ip ospf spf statistic` command displays the OSPF routes calculation process.

#### Example

```
router# debug ip ospf spf
```

```
OSPF: run ospf_spf_run
```

```
OSPF: start doing SPF for AREA 0.0.0.0
```

```
OSPF: RTAB_REV(ospf) 1390.
```

```
OSPF : Initializing to do SPF
```

```
OSPF: addroute LSID 192.168.20.240
```

```
OSPF: ospf_nh_find: 192.168.40.2
```

```
.....
```

```
OSPF: addroute LSID 192.168.40.3
```

```
OSPF: build a OSPF_ROUTE, dest: 192.168.40.3
```

```
OSPF: addroute LSID 192.168.40.2
```

```
.....
```

```
OSPF: SPF Area A running Network Summary
```

```
OSPF: Processing LS_SUM_NET 192.168.40.24, mask 255.255.255.248, adv 192.168.40.3,  
age 599
```

```
OSPF: addroute LSID 192.168.40.24
```

```
OSPF: ospf_build_route RT 192.168.40.24
```

```
OSPF: build route 192.168.40.24(255.255.255.248).
```

.....

OSPF: Processing LS\_SUM\_NET 1.1.1.1, mask 255.255.255.255, adv 192.168.20.240, age 228

OSPF: addroute LSID 192.168.20.236

OSPF: build a OSPF\_ROUTE, dest: 192.168.20.236

OSPF: start Building AS External Routes

OSPF: processing LS\_ASE 192.168.42.0, mask 255.255.255.248, adv 192.168.20.236, age 258

OSPF: addroute LSID 192.168.42.0

OSPF: ospf\_build\_route RT 192.168.42.0

OSPF: build route 192.168.42.0(255.255.255.248).

OSPF: processing LS\_ASE 192.168.43.0, mask 255.255.255.0, adv 192.168.20.236, age 258

OSPF: addroute LSID 192.168.43.0

OSPF: ospf\_build\_route RT 192.168.43.0

OSPF: build route 192.168.43.0(255.255.255.0).

OSPF: processing LS\_ASE 192.168.44.0, mask 255.255.255.0, adv 192.168.20.236, age 258

OSPF: addroute LSID 192.168.44.0

OSPF: ospf\_build\_route RT 192.168.44.0

OSPF: build route 192.168.44.0(255.255.255.0).

.....

OSPF: end doing SPF for AREA 0.0.0.0

## 2. Description of the displaying fields:

Field	description
<i>LSA(192.168.20.23 6, LS_SUM_ASB)</i>	<b>ID and type of LSA</b>

### 55.1.13 debug ip ospf tree

To display establishment of SPF tree of OSPF, use the debug ip ospf tree.

#### debug ip ospf tree

##### Parameter

none

##### Default

none

##### Command mode

EXEC



## Instruction

To display establishment of SPF tree of OSPF from the output of this command.

## Example

```

router# debug ip ospf tree B3710_221#
OSPF: add LSA(192.168.40.0, LS_STUB) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.2, LS_RTR) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.3, LS_RTR) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.1, LS_STUB) 0 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.3, LS_STUB) 1600 under LSA(192.168.40.3, LS_RTR)
OSPF: add LSA(192.169.1.5, LS_RTR) 3200 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.18, LS_STUB) 1600 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.2, LS_STUB) 1600 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.17, LS_STUB) 3200 under LSA(192.169.1.5, LS_RTR)
OSPF: add LSA(192.168.40.24, LS_SUM_NET) 1601 under LSA(192.168.40.3, LS_RTR)
OSPF: add LSA(192.168.40.32, LS_SUM_NET) 3200 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.40, LS_SUM_NET) 14577 under LSA(192.169.1.5, LS_RTR)
OSPF: add LSA(192.168.20.236, LS_SUM_ASB) 3200 under LSA(192.168.40.2, LS_RTR)

```

Description of the displaying fields:

Field	description
<i>LSA(192.168.20.236, LS_SUM_ASB)</i>	<b>ID and type of LSA</b>
<i>add</i>	<b>Sub-LSA</b>
<i>under</i>	<b>parent LSA</b>

### 55.1.14 default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the default-information originate command

**default-information originate** [**always**] [**route-map** *map-name*]

**no default-information originate** [**always**] [**route-map** *map-name*]

## Parameter

parameter	description
<i>originate</i>	<b>Generate a default external route into an Open Shortest Path First (OSPF) routing domain</b>
<i>Always</i>	<b>(Optional) Always advertises the default route regardless of whether the software has a default route.</b>

<i>route-map</i> <i>map-name</i>	<b>(Optional) Routing process will generate the default route if the route map is satisfied.</b>
-------------------------------------	--

## Default

This command is disabled by default. No default external route is generated into the OSPF routing domain.

## Command mode

router configuration

## Instruction

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPF routing domain, the software automatically becomes an Autonomous System Boundary Router Switch. However, an ASBR Switch does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the always keyword.

When you use this command for the OSPF process, you must satisfy the route-map argument. Use the default-information originate always route-map command when you do not want the dependency on the default network in the routing table.

## Example

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
router ospf 109
redistribute rip
default-information originate
```

## Related commands

### Redistribute

#### 55.1.15 default-metric

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the default-metric command. To return to the default state, use the no form of this command.

**default-metric** *value*

**no default-metric**

## Parameter

parameter	description
<i>value</i>	<b>Default metric value appropriate for the specified routing protocol, in the range 1~4294967295.</b>

## Default

Default metric value is 10.

## Command mode

router configuration

## Instruction

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

## Example

The example assigns 10 as the default metric routes.

```
router_config_ospf_100#default-metric 3
```

## Related commands

### redistribute

#### 55.1.16 distance ospf

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the distance ospf command To restore the default value, use the no form of this command.

```
distance ospf {[intra-area dist1] [inter-area dist2] [external dist3]}
```

```
no distance ospf [intra-area] [inter-area] [external]
```

## Parameter

parameter	description
<i>intra-area dist1</i>	<b>(Optional) Sets the distance for routes in an area, learned by redistribution. The default value is 110.</b>
<i>inter-area dist2</i>	<b>(Optional) Sets the distance for all routes from one area to another area. The default value is 110.</b>
<i>external dist3</i>	<b>(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 110.</b>

## Default

intra-area: 110

inter-area: 110

external: 150

## Command mode

router configuration

## Instruction

This command performs the same function as the distance command used with an access list. However, the distance ospf command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

## Example

The following example changes the external distance to 200:

Router A

```
router ospf 1
redistribute ospf 2
distance ospf external 200
!
```

```
router ospf 2
redistribute ospf 1
distance ospf external 200
```

Router B

```
router ospf 1
redistribute ospf 2
distance ospf external 200
!
```

```
router ospf 2
redistribute ospf 1
distance ospf external 200
```

## Related commands

### distance

#### *55.1.17 filter*

To configure routing filter list, use the filter command. Use the no filter command to restore the default.

```
filter {interface-type interface-number | *} {in | out } {access-list access-list-name |
gateway access-list-name | prefix-list prefix-list-name}
no filter {interface-type interface-number | *} {in | out} {access-list access-list-name |
gateway access-list-name | prefix-list prefix-list-name}
```

## Parameter

parameter	description
<i>interface-type</i>	Interface type
<i>interface-number</i>	Interface number
*	All interfaces
<i>In</i>	Filters incoming ospf routes
<i>out</i>	Filters outgoing routes
<i>access-list-name</i>	Name of access list
<i>access-list-name</i>	Name of access list
<i>prefix-list-name</i>	Name of prefix list

### Default

none

### Command mode

router configuration

### Instruction

none

### Example

```
filter * in access-list mylist
```

### 55.1.18 ip ospf cost

To specify the cost of OSPF protocol on an interface, use the `ip ospf cost` command in interface configuration mode. To restore to the default value, use the `no` form of this command.

**ip ospf cost** cost

**no ip ospf cost**

### Parameter

parameter	description
<i>cost</i>	the cost of OSPF protocol. It can be a value in the range from 1 to 65535.

### Default

Default value of the OSPF protocol cost depends on rate of the interface.

### Command mode

interface configuration mode

### Example

The following example sets the interface cost value to 2:

```
ip ospf cost 2
```

specify the the interface cost of OSPF protocol, to restore the default value,use the no ip ospf command

### 55.1.19 ip ospf dead-interval

To set the dead-interval of specified routing switch in neighbourhood, use the ip ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command.

```
ip ospf dead-interval seconds
```

```
ip ospf dead-interval
```

Parameter

parameter	description
<i>Seconds</i>	<b>Interval (in seconds) of specified routing switch in neighbourhood. The range is 1 to 65535.</b>

Default

40 seconds

Command mode

interface configuration

Instruction

The dead interval is advertised in OSPF hello packets and sent with OSPF hello packets. This value must be the same for all networking devices on a specific network and four times the interval set by the ip ospf hello-interval command.

Example

The following example sets the OSPF dead interval to 60 seconds:

```
router_config_S1/0#ip ospf dead-interval 60
```

Related commands

```
ip ospf hello-interval
```

### 55.1.20 ip ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the ip ospf hello-interval command. To return to the default value, use the no form of this command.

```
ip ospf hello-interval seconds
```

```
no ip ospf hello-interval
```

Parameter

parameter	description
<i>Seconds</i>	<b>Specifies the interval (in seconds)of sending hello packets. The range is from 1 to 255.</b>

### Default

10 seconds

### Command mode

interface configuration mode

### Instruction

This value is advertised in the hello packets and sent with the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

### Example

The following example sets the interval between hello packets to 20 seconds:

```
router_config_S1/0#ip ospf hello-interval 20
```

### Related commands

**ip ospf dead-interval**

#### 55.1.21 ip ospf message-digest-key

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the `ip ospf message-digest-key md5` command. To remove an old MD5 key, use the `no` form of this command.

**ip ospf message-digest-key** *keyid* **md5** **key**

**no ip ospf message-digest-key** *keyid*

### Parameter

parameter	description
<i>keyid</i>	<b>An identifier in the range from 1 to 255.</b>
<i>key</i>	<b>Alphanumeric password of up to 16 bytes.</b>

### Default

OSPF MD5 authentication is disabled.

### Command mode

interface configuration mode

### Instruction

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

```
interface ethernet 1
ip ospf message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface ethernet 1
ip ospf message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
no ip ospf message-digest-key 100
```

Then, only key 101 is used for authentication on Ethernet interface 1.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

### Example

The following example sets a new key 19 with the password 8ry4222:

```
interface ethernet 1
ip ospf message-digest-key 10 md5 xv560qle
ip ospf message-digest-key 19 md5 8ry4222
```

### Related commands

#### **area authentication**

#### ***55.1.22 ip ospf network***

To configure the Open Shortest Path First (OSPF) network type, use the `ip ospf network` command. To return to the default value, use the `no` form of this command.



```
ip ospf network { broadcast | nonbroadcast | point_to_multipoint | point-to-point}
```

```
no ip ospf network { broadcast | nonbroadcast | point_to_multipoint | point-to-point}
```

#### Parameter

parameter	description
<i>broadcast</i>	<b>Sets the network type to broadcast.</b>
<i>nonbroadcast</i>	<b>Sets the network type to nonbroadcast multiaccess</b>
<i>point-to-point</i>	<b>Sets the network type to point-to-point.</b>
<i>point-to-multipoint</i>	<b>Sets the network type to point-to-multipoint.</b>

#### Command mode

interface configuration mode

#### Instruction

Using this feature, you can configure broadcast networks as NBMA networks. Configuring NBMA networks as point-to-multipoint network if there is no assurance to direct connection between any two routing switches..

#### Example

The following example sets serial1/0 as a nonbroadcast network type:

```
router_config_S1/0#ip ospf network nonbroadcast
```

#### 55.1.23 ip ospf passive

To cancel sending a HELLO packets on an interface, use the ip ospf passive command. Use the no form of this command to reactivate the sending of HELLO packet.

```
ip ospf passive
```

```
no ip ospf passive
```

#### Parameter

This command has no keywords or parameters.

#### Default

disabled

#### Command mode

all configuration mode

#### Instruction

If you cancel sending a HELLO packet on an interface, a specified subnetwork will keep on declaring to other interfaces, and the routing update from other routing switch to this interface can still be received and dealt with. This is usually applicable to the STUB network, for in this kind of network there is usually no other OSPF routing switches.

## Example

The following example sends a HELLO packet to all interfaces(except for Ethernet 1/0) overridden by network 172.16.0.0:

```
interface ethernet 1/0
ip address 172.16.0.1 255.255.0.0
ip ospf passive
router ospf 110
network 172.16.0.0 255.255.0.0 area 1
```

## Related commands

none

### 55.1.24 ip ospf password

To configure password for a neighbor route, use the ip ospf password command. Use the no form of this command to cancel the configuration.

**ip ospf password** *password*

**no ip ospf password**

## Parameter

parameter	description
<i>password</i>	<b>Any consecutive 8-digit character string</b>

## Default

No password is predefined by default.

## Command mode

Interface configuration mode

## Instruction

The password generated by this command directly inserts OSPF information packet. This command can configure one password for each network of each interface. All neighbor routers must have the same password to exchange OSPD routing information.

**Note:** This command is only valid when configured with the area authentication command.

## Example

```
ip ospf password yourpass
```

## Related commands

**area authentication**

### 55.1.28 *ip ospf priority*

To set the router priority, use the `ip ospf priority` command. To return to the default value, use the `no` form of this command.

**ip ospf priority** *priority*

**no ip ospf priority**

Parameter

parameter	description
<i>priority</i>	specifies the priority. The range is from 0 to 255.

Default

Priority of 1

Command mode

interface configuration mode

Instruction

When two routing switches attached to a network both attempt to become the designated routing switch, the one with the higher routing switch priority takes precedence. If there is a tie, the routing switch with the higher routing switch ID takes precedence. A routing switch with a routing switch priority set to zero is ineligible to become the designated routing switch or backup designated routing switch. routing switch priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First (OSPF) for nonbroadcast networks using the `neighbor` routing switch configuration command for OSPF.

Example

The following example sets the routing switch priority value to 8:

```
router_config_S1/0#ip ospf priority 8
```

Related commands

**neighbor**

### 55.1.29 *ip ospf retransmit-interval*

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the `ip ospf retransmit-interval` command. To return to the default value, use the `no` form of this command.

**ip ospf retransmit** *seconds*

**no ip ospf retransmit**

Parameter

parameter	description
-----------	-------------

<i>seconds</i>	<b>Time (in seconds) between retransmissions. The range is from 1 to 65535 seconds.</b>
----------------	---

### Default

The default is 5 seconds.

### Command mode

interface configuration mode

### Instruction

When a routing switch sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the routing switch receives no acknowledgment, it will resend the LSA. The setting of the seconds argument should be greater than the expected round-trip delay between any two routing switches on the attached network..

### Example

The following example sets the retransmit interval value to 8 seconds:

```
router_config_S1/0#ip ospf retransmit 8
```

### 55.1.30 neighbor

To configure Open Shortest Path First (OSPF) routing switch interconnecting to nonbroadcast networks, use the neighbor command. To remove a configuration, use the no form of this command.

**neighbor** *ip-address* [*priority number*] [**poll-interval** *seconds*] [**cost** *number*]

**no neighbor** *ip-address* [*priority number*] [**poll-interval** *seconds*] [*cost number*]

### Parameter

parameter	description
<i>ip-address</i>	<b>Interface IP address of the neighbor.</b>
<i>priority number</i>	<b>(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.</b>
<i>poll-interval seconds</i>	<b>(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.</b>
<i>cost number</i>	<b>(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the number argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.</b>

## Default

no default value

## Command mode

router configuration

## Instruction

In X.25 and Frame Relay networks you can configure OSPF to run as a broadcast network. Detailed information is as follow:

In X.25 and frame relay map

One nonbroadcast network neighbor must be configured in the routing switch. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive, it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called Poll Interval.

When the routing switch first starts up, it sends only hello packets to those routing switches with nonzero priority, that is, routing switches that are eligible to become designated routeing switch (DRs) and backup designated routing switches (BDRs). After the DRs and BDRs are selected, DRs and BDRs will then start sending hello packets to all neighbors in order to form adjacencies.

## Example

The following example declares a routing switch at address 131.108.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
router ospf
neighbor 131.108.3.4 priority 1 poll-interval 180
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204 no shut
!
router ospf 1
network 10.0.1.0 255.255.255.0 area 0
```

```
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

#### Related commands

#### ip ospf priority

#### 55.1.31 network area

To define the interfaces on which Open Shortest Path First (OSPF) runs and to define the area ID for those interfaces, use the network area command. To disable the feature, use the no form of this command.

```
network network mask area area_id [ advertise | not-advertise ]
[ no ] network network mask area area_id [ advertise | not-advertise ]
```

#### Parameter

parameter	description
<i>network</i>	<b>Network Ip address, in dotted decimal format.</b>
<i>mask</i>	<b>Mask, in dotted decimal format.</b>
<i>area_id</i>	<b>Id of area.</b>
<i>Advertise notadvertise</i>	<b>Specifies whether to advertise the abstract information or not</b>

#### Default

This command is disabled by default.

#### Command mode

router configuration

#### Instruction

Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the network command list and ignore the subsequent overlapping portions. Importing network range and specifying the range can reduce the switch state of routing information among areas

#### Example

The following example defines network range 10.0.0.0 255.0.0.0 and adds to area 2:

```
router_config_ospf_10#network 10.0.0.0 255.0.0.0 area 2
```

#### 55.1.32 redistribute

To configure OSPF to redistribute routes of other routing protocols, use the redistribute command. Use the no form of this command to restore the default.

```
redistribute protocol [as-number] [route-map map-tag]
```

**no redistribute protocol** [*as-number*] [*route-map map-tag*]

#### Parameter

parameter	description
<i>protocol</i>	Redistributes former protocols that learned, it should be one of the following: beigrp, bgp, connect, ospf, rip, static
<i>as_number</i>	(Optional) Autonomous system number. There is no parameter for connect, rip and static.
<i>map-tag</i>	(Optional) Name of the route map

#### Default

disabled

#### Command mode

router configuration

#### Instruction

none

#### Example

The following example redistributes OSPF protocol from the autonomous system 0:  
Redistribute ospf 0

#### 55.1.33 router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the `router ospf` command. To terminate an OSPF routing process, use the `no` form of this command.

**router ospf** *process-id*

**no router ospf** *process-id*

#### Parameter

parameter	description
<i>process-id</i>	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

#### Default

No OSPF routing process is defined.

#### Command mode

global configuration mode

#### Instruction

You can specify multiple OSPF routing processes in each router.

### Example

The following example configures an OSPF routing process and assign a process number of 109:

```
router ospf 109
```

### Related commands

#### network area

#### 55.1.34 show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the show ip ospf command.

```
show ip ospf [process-id]
```

### Parameter

parameter	description
<i>process-id</i>	(Optional) Process ID. If

### Default

none

### Command mode

EXEC

### Instruction

Troubleshoot OSPF problems according to the output of this command. To display only the global configuration information of the corresponding OSPF process if configured with the process-id parameter.

### Example

The following display the configuration information of OSPF process:

```
router#show ip ospf
```

```
OSPF process: 1, Router ID is 192.168.99.81
```

```
Distance: intra-area 110 inter-area 130 external 150
```

```
Source Distance Access-list
```

```
240.240.1.1/24 1 what
```

```
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
```

```
Number of areas is 3
```

```
AREA: 1
```



Number of interface in this area is 1(UP: 1)

Area authentication type: None

AREA: 36.0.0.1

This is a stub area.

Number of interface in this area is 0(UP: 0)

Area authentication type: None

AREA: 192.168.20.0

Number of interface in this area is 0(UP: 0)

Area authentication type: None Net Range list:

10.0.0.0/255.0.0.0 Not-Advertise

140.140.0.0/255.255.0.0 Advertise

filter list on receiving UPDATE is Gateway: weewe

filter list on sending UPDATE is Prefix: trtwd

Summary-address list:

150.150.0.0/16 advertise

router#

description of the displaying fields

field	description
<i>OSPF process: 1</i>	<b>OSPF process ID</b>
<i>Router ID is 192.168.99.81</i>	<b>Routing switch ID</b>
<i>Distance: intra-area 110 inter-area 130 external 150</i>	<b>The default administrative distance that the current routing switch adopts</b>
<i>Source Distance Access- list</i>	<b>Administrative distance based on concrete routing configuration</b>
<i>SPF schedule delay 5 secs, Hold time between two SPFs 10 secs</i>	<b>Value of two timer related to OSPF</b>
<i>Number of areas is 3</i>	<b>The number of the field that currently configured and the parameter configured in each field</b>
<i>filter list on receiving</i>	<b>The configured filter list on receiving routes</b>
<i>filter list on sending</i>	<b>The configured filter list on sending routes</b>
<i>Summary-address list</i>	<b>The configured routing summary address</b>

### 55.1.35 show ip ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the show ip ospf border-routers command.

**show ip ospf border-routers****Parameter**

none

**Default**

none

**Command mode**

EXEC

**Example**

router#

router#sh ip os bor

OSPF process: 1

Codes: i - Intra-area route, I - Inter-area route

Destination Adv-Rtr Cost Type Area

i 192.168.20.77 192.168.20.77 11 ABR 0

router#

field description:

field	description
<i>Destination</i>	<b>Routing switch ID of the destination.</b>
<i>Adv-Rtr</i>	<b>Next hop toward the destination.</b>
<i>Cost</i>	<b>Cost of using this route.</b>
<i>Type</i>	<b>The routing switch type of the destination; it is either an ABR or ASBR or both.</b>
<i>Area</i>	<b>The area ID of the area from which this route is learned.</b>

**55.1.36 show ip ospf database**

To display lists of information related to the Open Shortest Path First (OSPF) database, use the show ip ospf database command.

**show ip ospf database****Parameter**

none

**Default**

none

**Command mode**

EXEC

**Instruction**

Display lists of information related to the Open Shortest Path First (OSPF) database in accordance with debugging information of the command, and it is helpful for users in troubleshooting

**Example**

```
router#
router#show ip ospf database
OSPF process: 1
(Router ID 192.168.99.81)
AREA: 0
Router Link States
Link ID ADV Router Age Seq # Checksum Link count
192.168.20.77 192.168.20.77 77 0x8000008a 0x90ed 1
192.168.99.81 192.168.99.81 66 0x80000003 0xd978 1
Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.20.77 192.168.20.77 80 0x80000001 0x9625
Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.99.0 192.168.99.81 87 0x80000003 0xd78c
AREA: 1
Router Link States
Link ID ADV Router Age Seq # Checksum Link count
192.168.99.81 192.168.99.81 70 0x80000002 0x0817 1
Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.20.0 192.168.99.81 66 0x80000006 0xd1c1
router#
```

field description:

field	description
AREA: 1	OSPF area.

<i>Router Link States/Net Link States/Summary Net Link States</i>	<b>LSA type</b>
<i>Link ID</i>	<b>LSA ID.</b>
<i>ADV Router</i>	<b>Advertising routing switch's ID.</b>
<i>Age</i>	<b>Link state age.</b>
<i>Seq #</i>	<b>Link state sequence number</b>
<i>Checksum</i>	<b>Fletcher checksum of the complete contents of the link state advertisement.</b>

### 55.1.37 show ip ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the show ip ospf interface command.

#### show ip ospf interface

##### Parameter

none

##### Default

none

##### Command mode

EXEC

##### Instruction

To display configuration and operation situation of OSPF on an interface according to the debugging information of this command. Users can confirm whether the configuration is right or not and it is helpful in troubleshooting

##### Example

```
router#sh ip os int
```

```
Ethernet 1/0 is up, line protocol is up
```

```
Internet Address: 192.168.20.81/24, Nettype: BROADCAST
```

```
OSPF process is 1, AREA 0, Router ID 202.96.135.201
```

```
Cost 10, Transmit Delay is 1 sec, Priority 1
```

```
Hello interval 10, Dead timer 40, Retransmit 5
```

```
OSPF INTF State is DrOther
```

```
Designated Router id 131.119.254.10, Interface address 131.119.254.10
```

```
Backup Designated router id 131.119.254.28, Interface addr 131.119.254.28
```

```
Neighbor Count is 8, Adjacent neighbor count is 2
```

Adjacent with neighbor 131.119.254.28 (Backup Designated Router)

Adjacent with neighbor 131.119.254.10 (Designated Router)

router#

displaying field description:

field	description
<i>Internet Address:</i>	<b>Interface IP address</b>
<i>Nettype</i>	<b>Net type of OSPF interface</b>
<i>OSPF process is</i>	<b>OSPF process number</b>
<i>AREA</i>	<b>OSPF area.</b>
<i>Router ID</i>	<b>Routing switch ID</b>
<i>Cost</i>	<b>Cost of routing switch OSPF interface</b>
<i>Transmit Delay is</i>	<b>Transmit delay</b>
<i>Priority</i>	<b>Priority of routing switch interface</b>
<i>Hello interval</i>	<b>Number of seconds until next hello packet is sent out this interface.</b>
<i>Dead timer</i>	<b>Dead timer</b>
<i>Retransmit</i>	<b>Retransmit interval</b>
<i>OSPF INTF State is</i>	<b>OSPF nterface state</b>
<i>Designated Router id</i>	<b>Designated router id and interface ip address</b>
<i>Backup Designated router id</i>	<b>Backup Designated routing switch id and interface ip address</b>
<i>Neighbor Count is</i>	<b>Number of the neighbor routing switch</b>
<i>Adjacent neighbor count is</i>	<b>Number of the adjacent neighbor that has established</b>
<i>Adjacent with neighbor</i>	<b>List of the adjacent neighbor</b>

### 55.1.38 show ip ospf neighbor

To display Open Shortest Path First (OSPF)-neighbor information, use the show ip ospf neighbor command.

#### show ip ospf neighbor

##### Parameter

none

##### Default

none

##### Command mode

EXEC

## Instruction

To display neighbor situation of OSPF from the output of this command to help user troubleshoot OSPF.

## Example

```
router#show ip ospf neighbor
```

```
OSPF process: 1
```

```
AREA 1
```

```
Neighbor Pri State DeadTime Address Interface
```

```
21.0.0.32 1 FULL /DR 31 192.168.99.32 Ethernet1/0
```

```
AREA 36.0.0.1
```

```
Neighbor Pri State DeadTime Address Interface
```

```
199.199.199.137 1 EXSTART/DR 31 202.19.19.137 Ethernet2/1
```

```
AREA 192.168.20.0
```

```
Neighbor Pri State DeadTime Address Interface
```

```
140.140.0.46 1 FULL /DR 108 140.140.0.46 Serial 1/0
```

```
133.133.2.11 1 FULL /DR 110 133.133.2.11 Serial1/0
```

```
192.31.48.200 1 FULL / DROTHER 31 192.31.48.200 Ethernet1/0
```

Displaying field description:

field	description
<i>OSPF process</i>	<b>OSPF process number</b>
<i>AREA</i>	<b>OSPF area</b>
<i>Neighbor</i>	<b>Neighbor routing switch ID.</b>
<i>Pri</i>	<b>Routing switch priority of the neighbor, neighbor state.</b>
<i>State</i>	<b>OSPF state.</b>
<i>DeadTime</i>	<b>Expected time before software will declare the neighbor dead.</b>
<i>Address</i>	<b>Neighbor ip address</b>
<i>Interface</i>	<b>Interface to which connects the neighbor</b>

### 55.1.39 show ip ospf virtual-link

To display information of Open Shortest Path First (OSPF) virtual links, use the show ip ospf virtual-links command.

```
show ip ospf virtual-link
```

Parameter

none

## Default

none

## Command mode

EXEC

## Instruction

The information displayed by the `show ip ospf virtual-links` command is useful in debugging OSPF routing operations. To display the detailed information of adjacency relation of the OSPF neighbour, use the `show ip ospf neighbour` command

## Example

```
router#show ip ospf vir
```

```
Virtual Link Neighbor ID 200.200.200.2 (UP)
```

```
Run as Demand-Circuit
```

```
TransArea: 1, Cost is 185
```

```
Hello interval is 10, Dead timer is 40 Retransmit is 5
```

```
INTF Adjacency state is IPOINT_TO_POINT
```

Description of the displaying fields:

field	description
<i>neighbor ID</i>	The configured neighbor ID of the remote side
<i>neighbour state</i>	Adjacency relation of the OSPF neighbor
<i>Demand-Circuit</i>	Indicates working under DC mode
<i>TransArea</i>	The transit area through which the virtual link is formed.
<i>cost</i>	The cost of reaching the OSPF neighbor through the virtual link.
<i>Hello Interval</i>	The current Hello interval
<i>DeadTime</i>	Expected time before software will declare the neighbor dead.
<i>Retrans</i>	Retransmit interval
<i>INTF Adjacency State</i>	The state of virtual link.

## Related commands

`area virtual-link`

`show ip ospf neighbor`

### 55.1.40 summary-address

To create aggregate addresses for Open Shortest Path First (OSPF), use the summary-address command. To restore the default, use the no form of this command.

**summary-address** *address mask* [**not-advertise**]

**no summary-address** *address mask*

#### Parameter

parameter	description
<i>address</i>	<b>Summary address designated for a range of addresses.</b>
<i>Mask</i>	<b>IP subnet mask used for the summary route.</b>
<i>not-advertise</i>	<b>(Optional) Suppress match routes that creat LSA</b>

#### Default

none

#### Command mode

router configuration

#### Instruction

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Routing switch (ASBRs) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the area range command for route summarization.

#### Example

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
summary-address 10.1.0.0 255.255.0.0
```

#### Related commands

**area range**

**ip ospf password**

**ip ospf message-digest-key**



### 55.1.41 timers delay

To specify the delay interval between OSPF receiving a topology structure variety and initializing a minimum route priority computation, use the timer delay command. Use the no form of this command to restore default value.

**timers delay** *spf-delay*

**no timers delay**

Parameter

parameter	description
<i>spf-delay</i>	<b>Delay between topology variety and computation commencement in seconds, from 0 to 65535. Default value is 5 seconds. If the value is 0, that indicates there is no delay, namely, once there is a variety, the commencement of computation immediately starts.</b>

Default

spf-delay: 5 seconds

Command mode

router configuration

Instruction

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

Example

```
timers spf 10
```

### 55.1.42 timers hold

To configure the interval between two continuous SPF computation, use the timers hold command. Use the no form of this command to restore the default value.

**timers hold** *spf-holdtime*

**no timers hold**

Parameter

parameter	description
<i>spf-holdtime</i>	<b>The minimum value between two continuous computation, in the range from 0 to 65535.</b>

Default

spf-holdtime: 10 seconds

Command mode

router configuration

## Instruction

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

## Example

3. `timers spf 20`

## Chapter 56 BGP Configuration Commands affects ONLY PXT-S2790G/2795G or Higher

BGP Configuration Commands include:

- `aggregate-address`
- `bgp always-compare-med`
- `bgp bestpath med`
- `bgp client-to-client reflection`
- `bgp cluster-id`
- `bgp confederation identifier`
- `bgp confederation peers`
- `bgp dampening`
- `bgp default`
- `bgp deterministic-med`
- `bgp redistribute-internal`
- `clear ip bgp`
- `debug chat`
- `debug dialer`
- `debug ip bgp`
- `distance`
- `filter`
- `neighbor default-originate`
- `neighbor description`
- `neighbor distribute-list`
- `neighbor ebgp-multihop`
- `neighbor filter-list`
- `neighbor maximum-prefix`

- neighbor next-hop-self
- neighbor password
- neighbor prefix-list
- neighbor remote-as
- neighbor route-map
- neighbor route-reflector-client
- neighbor route-refresh
- neighbor send-community
- neighbor shutdown
- neighbor soft-reconfiguration
- neighbor timers
- neighbor update-source
- neighbor weight
- network (BGP)
- redistribute(BGP)
- router bgp
- show ip bgp
- show ip bgp community
- show ip bgp neighbors
- show ip bgp paths
- show ip bgp prefix-list
- show ip bgp regexp
- show ip bgp summary
- synchronization
- table-map
- timers

#### ***56.1.43 aggregate-address***

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the `aggregate-address` command in address family or routing switch configuration mode. To disable this function, use the `no` form of this command.

```
aggregate-address A.B.C.D/n [summary-only] [route-map map-name]
```

```
no aggregate-address A.B.C.D/n [summary-only] [route-map map-name]
```

## Parameter

parameter	description
<i>A.B.C.D/n</i>	<b>Aggregate network</b>
<i>summary-only</i>	<b>Filters all more-specific routes from updates.</b>
<i>route-map</i>	<b>Name of the route map used to set the attribute of the aggregate route.</b>
<i>map-name</i>	<b>Name of the route map</b>

## Default

none

## Command mode

BGP configuration mode

## Instruction

You can implement aggregate routing in BGP in three methods: first, dynamic implement routing by forwarding redistribute; second, static implement routing by network command; third, static implement routing by aggregate. The routing created in this way are local routing, which can be announced to other equivalent, but not implement local IP address table.

Using the aggregate-address command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix which matches the aggregate must exist in the RIB.) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the as-set keyword.)

Using the as-set keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS\_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the aggregate-address command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the summary-only keyword not only creates the aggregate route (for example, 19.\*.\*.\*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the neighbor distribute-list command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the suppress-map keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the match clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the `advertise-map` keyword selects specific routes that will be used to build different components of the aggregate route, such as `AS_SET` or `community`. This form of the `aggregate-address` command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with `AS_SET`, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the `AS_SET` to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists match clauses are supported.

Using the `attribute-map` keyword allows attributes of the aggregate route to be changed. This form of the `aggregate-address` command is useful when one of the routes forming the `AS_SET` is configured with an attribute such as the `community no-export` attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

### Example

In the following example, an aggregate BGP address is created :

```
router bgp 5
aggregate-address 193.0.0.0/8
```

### Related commands

#### **route-map**

#### ***56.1.44 bgp always-compare-med***

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the `bgp always-compare-med` command. To disallow the comparison, use the `no` form of this command.

#### **bgp always-compare-med**

#### **no bgp always-compare-med**

### Parameter

none

### Default

Default does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the `no` form of this command is entered..

### Command mode

BGP configuration mode

### Instruction

Default does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the `no` form of this command is entered. The MED is compared only if the autonomous system path for the compared routes is identical.

### Example

The following example enables the function

```
router bgp 5
```

```
bgp always-compare-med
```

Related commands

**bgp bestpath med**

**bgp deterministic-med**

### 56.1.45 bgp bestpath med

To modify the process way of Border Gateway Protocol (BGP) on Multi Exit Discriminator (MED) attribute, use the `bgp bestpath med` command. To disable the feature, use the `no` form of this command.

Parameter

parameter	description
<i>confed</i>	<b>Autonomous system confederation MED comparison attribute</b>
<i>missing-as-worst</i>	<b>(Optional) Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable.</b>

Default

none

Command mode

BGP configuration mode

Instruction

If the MED attribute of BGP route is not configured, the value of MED is always considered to be 0, that is the least value, which has the most priority. When configured with the `missing-as-worst` option, if the MED attribute of BGP route is not configured, the value of MED is always considered to be the most maximum value, which has the least priority.

Example

By default, the MED comparison between (100) and (200) doesn't occur for they are not the routes from the same sub-autonomous system. But the MED comparison occurs when configured with the `bgp bestpath med confed` command, for they come from the sub-autonomous system 100 and 200 respectively in the autonomous system alliance.

Related commands

**bgp always-compare-med**

**bgp deterministic-med**

### 56.1.46 *bgp client-to-client reflection*

To enable or restore route reflection from a BGP route reflector to clients, use the `bgp client-to-client reflection` command. To disable client-to-client route reflection, use the `no` form of this command.

**bgp client-to-client reflection**

**no bgp client-to-client reflection**

#### Parameter

none

#### Default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

#### Command mode

BGP configuration mode

#### Instruction

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the `no bgp client-to-client reflection` command to disable client-to-client reflection.

#### Example

In the following example, the local routing switch is a route reflector, and the three neighbors are fully meshed, turn off client-to-client reflection

```
router bgp 5
neighbor 192..168.20.190 router-reflector-client
neighbor 192..168.20.191 router-reflector-client
neighbor 192..168.20.192 router-reflector-client
no bgp client-to-client reflection
```

#### Related commands

**neighbor route-reflector-client**

**bgp cluster-id**

### 56.1.47 *bgp cluster-id*

To set the cluster ID on a route reflector in a route reflector cluster, use the `bgp cluster-id` command in router configuration mode. To remove the cluster ID, use the `no` form of this command.

**bgp cluster-id** *cluster-id*

**no bgp cluster-id** *cluster-id*

## Parameter

parameter	description
<i>cluster-id</i>	<b>Cluster ID of this router acting as a route reflector; maximum of 4 bytes.</b>

## Default

The local routing switch ID of the route reflector is used as the cluster ID when no ID is specified or when the no form of this command is entered.

## Command mode

BGP configuration mode

## Instruction

Together, a route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the routing switch ID of the route reflector. The `bgp cluster-id` command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.

## Example

In the following example, the local routing switch is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
bgp cluster-id 50000
```

## Related commands

**neighbor route-reflector-client**

**show ip bgp summary**

### 56.1.48 bgp confederation identifier

To specify a BGP confederation identifier, use the `bgp confederation identifier` command. To remove the confederation identifier, use the no form of this command.

**bgp confederation identifier autonomous-system**

**no bgp confederation identifier autonomous-system**

## Parameter

parameter	description
<i>autonomous-system</i>	<b>Autonomous system number to be configured to internally include multiple autonomous systems.</b>



## Default

none

## Command mode

BGP configuration mode

## Instruction

The `bgp confederation identifier` command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation.

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it is a single autonomous system.

Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you enables to you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

## Example

In the following example, the routing domain is divided into autonomous systems AS4001, 4002, 4003, 4004, 4005, 4006 and 4007 and identified by the confederation identifier 50000. Neighbor 1.2.3.4 is a peer inside of the routing domain confederation. Neighbor 3.4.5.6 is a peer outside of the routing domain confederation.

```
router bgp 4001
  bgp confederation identifier 5
  bgp confederation peers 4002 4003 4004 4005 4006 4007
  neighbor 1.2.3.4 remote-as 4002
  neighbor 3.4.5.6 remote-as 510
```

## Related commands

### **bgp confederation peers**

**show ip bgp summary**      **30**

### *56.1.49 bgp confederation peers*

To configure subautonomous systems to belong to a single confederation, use the `bgp confederation peers` command in router configuration mode. To remove an autonomous system from the confederation, use the `no` form of this command.

**bgp confederation peers autonomous-system [autonomous-system]**

**no bgp confederation peers autonomous-system [autonomous-system]**

## Parameter

parameter	description
<i>autonomous-system</i>	<b>Autonomous system numbers for BGP peers that will belong to the confederation.</b>

## Default

none

## Command mode

BGP configuration mode

## Instruction

The `bgp confederation peers` command is used to configure multiple autonomous systems as a single confederation. The ellipsis (...) in the command syntax indicates that your command input can include multiple values for the `as-number` argument.

The autonomous systems specified in this command are visible internally to the confederation. Each autonomous system is fully meshed within itself. The `bgp confederation identifier` command specifies the confederation to which the autonomous systems belong.

## Example

In the following example, autonomous systems 1091, 1092 and 1093 are configured to belong to a single confederation under the identifier 1090:

```
router bgp 1090
bgp confederation identifier 23
bgp confederation peers 1091 1092 1093
```

## Related commands

**bgp confederation identifier**

**show ip bgp summary**

### 56.1.50 bgp dampening

To enable BGP route dampening or change BGP route dampening parameters, use the `bgp dampening` command in address family or router configuration mode. To disable BGP dampening, use the `no` form of this command.

**bgp dampening** [*route-map name*] | [*half-time resuse-value suppress-value hold-time*]

**no bgp dampening** [*route-map name*] | [*half-time resuse-value suppress-value hold-time*]

## Parameter

parameter	description
<i>route-map</i>	<b>Name of route map that controls where BGP route dampening is enabled.</b>
<i>name</i>	<b>Name of route map that controls parameters</b>

<i>half-time</i>	<b>Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period</b>
<i>reuse-value</i>	<b>Reuse values based on accumulated penalties.</b>
<i>suppress-value</i>	<b>A route is suppressed when its penalty exceeds this limit.</b>
<i>hold-time</i>	<b>Maximum time (in minutes) a route can be suppressed.</b>

## Default

half-time: 15 minutes

reuse-value: 750

suppress-value: 2000

hold-time: 60 minutes

## Command mode

BGP configuration mode

## Instruction

The `bgp dampening` command is used to enable BGP route dampening. This command can be entered without any arguments or keywords. The half-life, reuse, suppress, and hold-time arguments are position-dependent; meaning that if any of these arguments are entered, then all optional arguments must be entered.

When BGP dampening is configured and a prefix is withdrawn, BGP considers the withdrawn prefix as a flap and increases the penalty by a 1000. If BGP receives an attribute change, BGP increases the penalty by 500. If then the prefix has been withdrawn, BGP keeps the prefix in the BGP table as a history entry. If the prefix has not been withdrawn by the neighbor and BGP is not using this prefix, the prefix is marked as dampened. Dampened prefixes are not used in the BGP decision process and not installed to the routing table.

## Example

In the following example, the `bgp dampening` command can be used to enable BGP route dampening function and use default parameter configuration. Use the following commands to configure different dampening parameters for different routing configurations:

```
Router bgp 100
bgp dampening route-map DMAP
!
route-map DMAP 10 permit
match as-path ASLIST-1
set dampening 15 750 2000 60
!
route-map DMAP 20 permit
```

```

match as-path ASLIST-2
set dampening 2 750 2000 8
!
ip as-path access-list ASLIST-1 permit ^3_
ip as-path access-list ASLIST-2 permit ^5_

```

### Related commands

#### set dampening

#### 56.1.51 bgp default

To configure default parameter of BGP process, use the `bgp default` command. Use the `no` form of this command to restore the default value.

**bgp default local-preference** <0-4294967295>

**no bgp default local-preference** <0-4294967295>

#### Parameter

parameter	description
<i>local-preference</i>	<b>Configures default parameter of the local preference.</b>
<0-4294967295>	<b>Default value of the local preference</b>

#### Default

100

#### Command mode

BGP configuration mode

#### Instruction

The route received from IBGP will be set as the local preference by BGP. The default value is 100, which can be modified via this command.

#### Example

The following example configures 200 as the local preference for the route from IBGP neighbor:

```

router bgp 100
bgp default local-preference 200

```

#### Related commands

none

### 56.1.52 *bgp deterministic-med*

To enforce the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system, use the `bgp deterministic-med` command in router configuration mode. To disable the required MED comparison, use the `no` form of this command.

**bgp deterministic-med**

**no bgp deterministic-med**

#### Parameter

none

#### Default

none

#### Command mode

BGP configuration mode

#### Instruction

The `bgp always-compare-med` command is used to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. After the `bgp always-compare-med` command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted). The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

#### Example

none

#### Related commands

**bgp bestpath med**

**bgp always-compare-med**

### 56.1.53 *bgp redistribute-internal*

To configure iBGP redistribution into an interior gateway protocol (IGP), such as RIP or OSPF, use the `bgp redistribute-internal` command in address family or router configuration mode. To return the router to default behavior and stop iBGP redistribution into IGPs, use the `no` form of this command.

**bgp redistribute-internal**

**no bgp redistribute-internal**

#### Parameter

none

### Default

IBGP routes are not redistributed into IGP.

### Command mode

BGP configuration mode

### Instruction

The `bgp redistribute-internal` command is used to configure iBGP redistribution into an IGP. The `clear ip bgp` command must be entered to reset BGP connections after this command is configured. When redistributing BGP into any IGP, be sure to use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed.

### Example

In the following example, BGP to OSPF3 route redistribution is enabled:

```
router ospf 3
redistribute bgp 2
!
router bgp 2
bgp redistribute-internal
!
```

### Related commands

none

#### 56.1.54 *clear ip bgp*

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the `clear ip bgp` command in privileged EXEC mode.

```
clear ip bgp { * | ip-address | as-number | peer-group name | aggregates | networks | redistribute } [soft [in | out]]
```

### Parameter

parameter	description
*	<b>Specifies that all current BGP sessions will be reset.</b>
<i>ip-address</i>	<b>Specifies that only the identified BGP neighbor will be reset.</b>
<i>AS</i>	<b>Specifies that sessions with BGP peers in the specified autonomous system will be reset.</b>
<i>peer-group-name</i>	<b>Specifies that the identified BGP peer group will be reset.</b>
<i>aggregates</i>	<b>Specifies that all aggregate routes will be reset</b>
<i>networks</i>	<b>Specifies that all static network routes will be reset</b>

<i>redistribute</i>	<b>Specifies that all redistributed routes will be reset</b>
<i>soft</i>	<b>Initiates a soft reset</b>
<i>in   out</i>	<b>Initiates inbound or outbound reconfiguration.</b>

## Command mode

EXEC

## Instruction

The `clear ip bgp` command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the `neighbor soft-reconfiguration inbound` command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

If all BGP routers support the route refresh capability, use the `clear ip bgp` command with the `in` keyword. You need not use the `soft` keyword, because soft reset is automatically assumed when the route refresh capability is supported.

## Example

The following example clear all the current BGP sessions:

```
clear ip bgp *
```

## Related commands

**`neighbor soft-reconfiguration`**

**`show ip bgp`**

### *56.1.55 debug chat*

To display script events, like to startup a script, to stop a script, to display the enforcement process of a script, use the `debug chat` command. Use the `no` form of this command to stop displaying information.

**`debug chat`**

**`no debug chat`**

## Parameter

This command has no parameters or keywords.

## Command mode

EXEC

## Example

```
Router#debug chat
Router#SCRIPT: start script default_dialer_script...
SCRIPT:Sending string: ATZ
SCRIPT:Expecting string: OK
SCRIPT: Receive string:
41 54 0D 0D 0A 4F 4B 0D 0A AT...OK..
SCRIPT:Completed match for expect:OK
SCRIPT:Sending string: ATDT 2
SCRIPT:Expecting string: CONNECT
SCRIPT: Receive string:
43 4F 4E 4E 45 43 54 CONNECT
SCRIPT: Completed match for expect:CONNECT
SCRIPT:Chat script finished
```

The first message indicates the script named default\_dialer\_script is started up.

The second message indicates the ATZ character string is sent.

The third message indicates the character string OK is expected to be received.

The fourth message indicates the character string OK is received.

The fifth message indicates ATDT 2 character string is sent, that is asking for modem dial-up.

The sixth message indicates the character string CONNECT is expected to be received.

The seventh message indicates the expected character string CONNECT is received.

The eighth message indicates the success of script enforcement.

## Related commands

### **chat-script**

### **56.1.56 debug dialer**

To display debugging information about the packets received on a dialer interface, use the debug dialer events command in privileged EXEC mode. To disable debugging output, use the no form of this command.

### **debug dialer**

### **no debug dialer**



## Parameter

This command has no parameters or keywords.

## Command mode

EXEC

## Example

```
Router#debug dialer
```

```
DIALER Serial 1/0: Dialing cause ip(PERMIT).
```

```
DIALER Serial 1/0: Dialing using Modem script: default_dialer_script & System script: none
```

```
DIALER Serial 1/0: Attempting to dial 2
```

```
DIALER Serial 1/0: process started
```

```
DIALER Serial 1/0: Chat script default_dialer_script (dialer) started.....
```

```
DIALER Serial 1/0: Connection established
```

```
DIALER Serial 1/0: Modem script finished successfully
```

The first message indicates that dialer checks whether the packet is permitted to cause dialing, and the result is the ip packet allows cause dialing.

The second message indicates that dialing uses default dialer script as the modem script rather than the system script.

The third message indicates that the dialer number is 2.

The fourth message indicates that the dialer process is started.

The fifth message indicates thath the dialer script is started.

The sixth and seventh message indicate that the connection is established successfully.

### 56.1.57 debug ip bgp

To display information related to processing of the Border Gateway Protocol (BGP), use the debug ip bgp command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ip bgp {all | fsm | keepalive | open | update}
```

```
no debug ip bgp {all | fsm | keepalive | open | update}
```

## Parameter

parameter	description
<i>all</i>	<b>Displays all BGP debugging functions.</b>
<i>dampening</i>	<b>Displays BGP dampening.</b>
<i>event</i>	<b>Displays BGP events.</b>
<i>fsm</i>	<b>Displays BGP fsm</b>

<i>keepalive</i>	<b>Displays BGP keepalives.</b>
<i>notify</i>	<b>Displays BGP notifies</b>
<i>open</i>	<b>Displays BGP opens</b>
<i>update</i>	<b>Displays BGP updates.</b>

## Default

No default behavior or values

## Command mode

EXEC

## Instruction

It is valid globally when configured with the `debug ip bgp` command to display debugging information and other VTY. If configured with the `terminal monitor` command, the debugging information will also be displayed. Use the `no terminal monitor` to close this function to disable displaying any debugging information on the VTY.

The command `debug ip bgp all` can enable all BGP debugging function, including dampening, fsm,keepalives,open and update. Use the `no debug ip bgp all` command to disable all BGP debugging functions.

## Example

The following example is the process to establish a BGP. The debugging information shows that a router establishes a connection with BGP neighbor 10.1.1.3.

```
BGP: 10.1.1.3 start connecting to peer
BGP: 10.1.1.3 went from Idle to Connect
BGP: 10.1.1.3 went from Connect to OpenSent
BGP: 10.1.1.3 send OPEN, length 41
BGP: 10.1.1.3 rcv OPEN, length 41
BGP: 10.1.1.3 went from OpenSent to OpenConfirm
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 rcv KEEPALIVE, length 19
BGP: 10.1.1.3 went from OpenConfirm to Established
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 rcv KEEPALIVE, length 19
BGP: 10.1.1.3 rcv KEEPALIVE, length 19
```

### 56.1.58 distance

To configure the administrative distance for BGP routes, use the distance command in router configuration mode. To return to the administrative distance to the default value, use the no form of this command.

**distance** **bgp** *external-distance internal-distance local-distance*

**no distance** **bgp**

Parameter

parameter	description
<i>external-distance</i>	<b>Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The default value is 20.</b>
<i>internal-distance</i>	<b>Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The default value is 200.</b>
<i>local-distance</i>	<b>Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The default value is 200.</b>

#### Default

external-distance: 20

internal-distance: 200

local-distance: 200

#### Command mode

BGP configuration

#### Instruction

The distance bgp command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

#### Example

In the following example, the administrative distance for BGP routes is set:

```
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
```

distance 20 20 200

#### Related commands

**set metric**

**set tag**

#### 56.1.59 filter

To filter routes based on an interface in order to realize the administrative strategy. Use the no form of this command to delete the configuration.

**filter interface <in | out> access-list *access-list-name* gateway *access-list-name* prefix-list *prefix-list-name***

**no filter interface <in | out> access-list *access-list-name* gateway *access-list-name* prefix-list *prefix-list-name***

#### Parameter

parameter	description
<i>interface</i>	<b>Interface name. Asterisk signifies all interfaces.</b>
<i>in   out</i>	<b>Filter the incoming of outgoing routes</b>
<i>access-list</i>	<b>Specifies the access-list to filter routes</b>
<i>access-list-name</i>	<b>Name of the access list</b>
<i>gateway</i>	<b>Specifies the access list to filter gateway</b>
<i>access-list-name</i>	<b>Name of the access list</b>
<i>prefix-list</i>	<b>Specifies the prefix list to filter routes</b>
<i>prefix-list-name</i>	<b>Name of the prefix list</b>

#### Default

none

#### Command mode

BGP configuration mode

#### Instruction

The access-list option specifies the access list to filter network prefix of routes; the gateway option specifies the access list to filter nexthop attribute of routes; the prefix list option specifies the prefix list filter network prefix of routes.

The access list and the prefix list options are mutually exclusive simultaneously. But then can be used with the gateway option together.

The asterisk signifies all interfaces.

If a none-existent prefix list or access list is configured on an interface, then all routes will pass.

## Example

The following example configures prefix and gateway to filter routes received on all interface:

```
router bgp 109
filter * in prefix-list prefix-guize gateway gateway-guize
```

## Related commands

**neighbor distribute-list**

**neighbor filter-list**

**neighbor route-map**

### 56.1.60 neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the neighbor default-originate command in address family or router configuration mode. To send no route as a default, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **default-originate**

**no neighbor** {*ip-address* | *peer-group-name*} **default-originate**

## Parameter

parameter	description
<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

## Default

No default route is sent to the neighbor.

## Command mode

BGP configuration mode

## Instruction

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a match ip address clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also. You can use standard or extended access lists with the neighbor default-originate command.

## Example

In the following example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 rather than to 160.89.2.1:

```
router bgp 109
```

```
network 160.89.0.0
neighbor 160.89.2.1 remote-as 100
neighbor 160.89.2.3 remote-as 200
neighbor 160.89.2.3 default-originate
```

### Related commands

#### **neighbor ebgp-multihop**

#### *56.1.61 neighbor description*

To associate a description with a neighbor, use the neighbor description command in router configuration mode. To remove the description, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **description** **LINE**

**no neighbor** {*ip-address* | *peer-group-name*} **description** **LINE**

### Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>
<i>line</i>	<b>Text that describes the neighbor.</b>

### Default

There is no description of the neighbor.

### Command mode

BGP configuration mode

### Instruction

It is easier for user to understand the configuration to associate a description with a neighbor.

### Example

In the following example, the description of the neighbor is "peer with abc.com":

```
router bgp 109
network 160.89.0.0
neighbor 160.89.2.3 description peer with abc.com
```

#### *56.1.62 neighbor distribute-list*

To distribute BGP neighbor information as specified in an access list, use the neighbor distribute-list command in address family or router configuration mode. To remove an entry, use the no form of this command.

```
neighbor {ip-address | peer-group-name} distribute-list {access-list name} {in | out}
```

```
no neighbor {ip-address | peer-group-name} distribute-list {access-list name} {in | out}
```

#### Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>
<i>access-list name</i>	<b>Name of a standard or extended access list.</b>
<i>In</i>	<b>Access list is applied to incoming advertisements to that neighbor.</b>
<i>Out</i>	<b>Access list is applied to outgoing advertisements to that neighbor.</b>

#### Default

none

#### Command mode

BGP configuration mode

#### Instruction

Use access-list filters network prefix of BGP routes; use aspath-list filters AS\_PATH attribute of BGP routes; use prefix list to filter network prefix of BGP routes.

The access-list option specifies the access list to filter network prefix of routes; the gateway option specifies the access list to filter nexthop attribute of routes; the prefix list option specifies the prefix list filter network prefix of routes.

If you specify a non-existent access list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

#### Example

The following router configuration mode example applies list beijing to incoming advertisements from neighbor120.23.4.1.

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 distribute-list beijing in
```

#### Related commands

ip aspath-list

neighbor filter-list

ip prefix-list 1

neighbor prefix-list

### 56.1.63 neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

**no neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**

Parameter

parameter	description
<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>ttl</i>	Time-to-live in the range from 1 to 255 hops.

#### Default

For EBGP-speaking neighbor, only directly connected neighbors are allowed, ttl default value is 1; for IBGP-speaking neighbor, ttl default is 255.

#### Command mode

BGP configuration mode

#### Instruction

Under default, BGP connection can not be established unless EBGP neighbors are directly connected ones. The allowable maximum number of hops for EBGP neighbors can be set with the neighbor ebgp-multihop command. Ttl is configured to 255 if not specified. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

#### Example

The following example allows connections to neighbor 131.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109:
```

```
neighbor 131.108.1.1 ebgp-multihop
```

#### Related commands

**neighbor default-originate**

### 56.1.64 neighbor filter-list

To set up a BGP filter, use the neighbor filter-list command in address family or router configuration mode. To disable this function, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **filter-list** *as-path-list name* {**in** | **out**}



```
no neighbor {ip-address | peer-group-name} filter-list as-path-list name {in | out}
```

### Parameter

parameter	description
<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>as-path-list name</i>	AS-PATH list name. The <code>ip as-path-list</code> command can be used to define this list.
<i>In</i>	Access list applied to incoming routes.
<i>Out</i>	Access list applied to outgoing routes.

### Default

none

### Command mode

BGP configuration mode

### Instruction

Use access-list filters network prefix of BGP routes; use aspath-list filters AS\_PATH attribute of BGP routes; use prefix list to filter network prefix of BGP routes.

If you specify a non-existent access list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

### Example

In the following router configuration mode example, the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system AS123:

```
ip as-path-list shanghai deny _123_
ip as-path-list shanghai deny ^123$
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
neighbor 128.125.1.1 filter-list shanghai out
```

### Related commands

**ip aspath-list**

**neighbor distribute-list**

**ip prefix-list 1****neighbor prefix-list****56.1.65 neighbor maximum-prefix**

To control how many prefixes can be received from a neighbor, use the neighbor maximum-prefix command in router configuration mode. To disable this function, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum*

**no neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix**

## Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>
<i>Maximum</i>	<b>Maximum number of prefixes allowed from this neighbor.</b>

## Default

This command is disabled by default. There is no limit on the number of prefixes.

## Command mode

BGP configuration mode

## Instruction

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer. When the number of received prefixes exceeds the maximum number configured, the router terminates the peering (by default). However, if the warning-only keyword is configured, the router instead only sends a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the clear ip bgp command is issued.

## Example

The following example sets the maximum number of prefixes allowed from the neighbor at 129.140.6.6 to 1000:

```
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 maximum-prefix 1000
```

## Related commands

**clear ip bgp**

### 56.1.66 neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor or peer group, use the `neighbor next-hop-self` command in router configuration mode. To disable this feature, use the `no` form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**

**no neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**

#### Parameter

parameter	description
<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

#### Default

This command is disabled by default.

#### Command mode

BGP configuration mode

#### Instruction

The disposal of nexthop attribute in BGP is more complicated than IGP . It usually follows three rules:

4. For EBGP session, configure the local ip address of BGP connection as the nexthop attribute when sending routes;
5. For IBGP session, configure the local ip address of BGP connection as the nexthop attribute if the routes are locally generated; if the routes are learned from EBGP, the nexthop attribute is to be filled in intactly the packet when sending routes;
6. If the nexthop parameter of the ip address of the routes belong to the network of BGP session, then the nexthop attribute always adopts the former nexthop;

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet. If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

#### Example

The following example forces all updates destined for 131.108.1.1 to advertise this router as the next hop:

```
router bgp 109
neighbor 131.108.1.1 next-hop-self
```

#### Related commands

**set ip next-hop 18****56.1.67 neighbor password**

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the `neighbor password` command in router configuration mode. To disable this function, use the `no` form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **password** *LINE*

**no neighbor** {*ip-address* | *peer-group-name*} **password**

## Parameter

parameter	description
<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>password</i>	Enables MD5 authentication
<i>LINE</i>	Plainr text password

## Default

none

## Command mode

BGP configuration mode

## Instruction

Use the `neighbor remote-as` command to specify the neighbor before using this command.

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The length of password should be between 1 and 20 characters.

If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command.

## Example

The following example configures 'abcd' as the authentication password of neighbor 120.23.4.1:

```
router bgp 109
neighbor 120.23.4.1 remote-as 108
neighbor 120.23.4.1 password abcd
```

## Related commands

**neighbor remote-as**

### 56.1.68 neighbor prefix-list

To prevent distribution of Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, a Connectionless Network Service (CLNS) filter expression, or a CLNS filter set, use the neighbor prefix-list command in address family or router configuration mode. To remove a filter list, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **prefix-list** *prefix-listname* {**in** | **out**}

**no neighbor** {*ip-address* | *peer-group-name*} **prefix-list** *prefix-listname* {**in** | **out**}

#### Parameter

parameter	description
<i>ip-address</i>	<b>IP address of neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>
<i>prefix-list</i>	<b>Prefix list is applied to advertisements of that neighbor</b>
<i>prefix-listname</i>	<b>Prefix list名 Name of a prefix list.</b>
<i>In</i>	<b>Filter list is applied to incoming advertisements from that neighbor.</b>
<i>Out</i>	<b>Filter list is applied to outgoing advertisements to that neighbor.</b>

#### Default

none

#### Command mode

BGP configuration mode

#### Instruction

Using prefix lists is one of three ways to filter BGP advertisements. You can also use AS-path filters, defined with the ip as-path access-list global configuration command and used in the neighbor filter-list command to filter BGP advertisements. The third way to filter BGP advertisements uses access or prefix lists with the neighbor distribute-list command. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group. Use the neighbor prefix-list command in address family configuration mode to filter NSAP BGP advertisements.

#### Example

The following router configuration mode example applies the prefix list named abc to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list abc in
```

The following router configuration mode example applies the prefix list named CustomerA to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list CustomerA in
```

#### Related commands

**ip prefix-list**

**ip prefix-list description**

**ip prefix-list sequence-number**

**show ip prefix-list**

**clear ip prefix-list**

**neighbor filter-list**

#### 56.1.69 neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the neighbor remote-as command in router configuration mode. To remove an entry from the table, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*

**no neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*

#### Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>
<i>Number</i>	<b>Number of autonomous system to which the neighbor belongs.</b>

#### Default

none

#### Command mode

BGP configuration mode

#### Instruction

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the router bgp global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

## Example

The following example assigns a BGP router to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighbor routers.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

## Related commands

### neighbor peer-group (creating)

#### 56.1.70 neighbor route-map

To apply a route map to incoming or outgoing routes, use the neighbor route-map command in address family or router configuration mode. To remove a route map, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}

**no neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}

## Parameter

parameter	description
<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP or multiprotocol BGP peer group.
<i>map-name</i>	Name of a route map.
<i>in</i>	Applies route map to incoming routes.
<i>Out</i>	Applies route map to outgoing routes.

## Default

none

## Command mode

BGP configuration mode

## Instruction

It is only based on neighbor to filter routes using distribute-list, prefix-list and as-path-list, while it is not only based on neighbor to filter routes but also based on neighbor to modify the attribute of routes to realize a more flexible routing strategy.

Different routes have different attributes. The route-map can modify attributes of different kinds of routes. If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map. The rules which is valid to BGP route are as follows: match aspath-list、match community-list、match ip address 、match ip nexthop 、match ip prefix-list 、match metric 、match tag 、set aggregator、set as-path、set atomic-aggregate、set community、set community-additive、set ip nexthop、set local-preference、set metric、set origin、set tag、set weight.

If configured with a non-existent route-map, then all routes is allowed to receive as a result without any modification.

If you specify a BGP or multiprotocol BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

### Example

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 198.92.70.24:

```
router bgp 5
neighbor 198.92.70.24 route-map internal-map in
route-map internal-map
match as-path abc
set local-preference 100
```

### Related commands

#### **neighbor peer-group (creating)**

#### **route-map 1**

#### **56.1.71 neighbor route-reflector-client**

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command in address family or router configuration mode. To indicate that the neighbor is not a client, use the no form of this command.

**neighbor ip-address route-reflector-client**

**no neighbor ip-address route-reflector-client**

### Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the BGP neighbor being identified as a client.</b>



## Default

There is no route reflector in the autonomous system.

## Command mode

BGP configuration mode

## Instruction

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the `neighbor route-reflector-client` command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The `bgp client-to-client reflection` command controls client-to-client reflection.

## Example

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 198.92.70.24.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
```

## Related commands

**bgp cluster-id**

**show ip bgp**

### *56.1.72 neighbor route-refresh*

To allow neighbor to use route refresh function, use the `neighbor route-refresh` command. Use the `no` form of this command to disable route refresh function.

**neighbor ip-address route-refresh**

**no neighbor ip-address route-refresh**

## Parameter

parameter	description
<i>ip-address</i>	<b>BGP neighbor and ip address</b>

## Default

disabled

## Command mode

BGP configuration mode

## Instruction

By default, BGP route exchange for only once when the connection is established, then only exchanging changed routes afterwards. If the routing strategy configuration is modified, it will not become effective immediately. Generally, there are two methods:

- Reset BGP connection
- Use soft-reconfiguration function

The first method is relatively slow, and the routes vary greatly. The second method needs too much storage space and occupies more CPU time. These two methods are not good method, and therefore a new method arises, that is, the route refresh.

The route refresh is a negotiation option based on BGP connection, aiming to send the route refresh request packet to ask neighbor to re-send all update packets to oneself, which do not need to reset BGP connection and also do not need to store a great amount of routes. This a a more ideal solution at the moment.

## Example

The following example allows neighbor at address 198.92.70.24 to use route refresh function:

```
router bgp 5
neighbor 198.92.70.24 route-refresh
```

## Related commands

**show ip bgp neighbors**

### *56.1.73 neighbor send-community*

To specify that a communities attribute should be sent to a BGP neighbor, use the neighbor send-community command in address family or router configuration mode. To remove the entry, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **send-community**

**no neighbor** {*ip-address* | *peer-group-name*} **send-community**

## Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>

## Default

The communities attribute can be sent to the neighbor.

## Command mode

BGP configuration mode

## Instruction

The route's group attribute of routes can be configured via the set community command of route-map or via neighbor's routing inform.

Use the show ip bgp neighbors command to see whether allows to send group attribute to neigh or not.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

## Example

In the following router configuration mode example, the router belongs to autonomous system 109 and is not permitted to send the communities attribute to its neighbor at IP address 198.92.70.23:

```
router bgp 109
no neighbor 198.92.70.23 send-community
```

## Related commands

**match community-list** 4

**neighbor peer-group (creating)**

**set community** 15

**set community-additive** 17

### 56.1.74 neighbor shutdown

To disable a neighbor or peer group, use the neighbor shutdown command in router configuration mode. To reenble the neighbor or peer group, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **shutdown**

**no neighbor** {*ip-address* | *peer-group-name*} **shutdown**

## Parameter

parameter	description
<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

## Default

none

## Command mode

BGP configuration mode

## Instruction

The neighbor shutdown command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly. To display a summary of BGP neighbors and peer group connections, use the show ip bgp summary command. Those neighbors with an Idle status and the Admin entry have been disabled by the neighbor shutdown command.

## Related commands

**show ip bgp summary**

**show ip bgp neighbors**

### 56.1.75 neighbor soft-reconfiguration

To configure the software to start storing updates, use the neighbor soft-reconfiguration command in router configuration mode. To not store received updates, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]

**no neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]

## Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the BGP-speaking neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>
<i>inbound</i>	<b>Indicates that the update to be stored is an incoming update.</b>

## Default

The incoming update is not stored and the outgoing update is stored.

## Command mode

BGP configuration mode

## Instruction

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Clearing the BGP session using the neighbor soft-reconfiguration command has a negative effect on network operations and should only be

used as a last resort. Routers can use the `clear ip bgp {* | address | peer-group name}` in command to clear the BGP session.

To determine whether a BGP router supports this capability, use the `show ip bgp neighbors` command. If a router supports the route refresh capability, the following message is displayed:

If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command.

### Example

The following example enables inbound soft reconfiguration for the neighbor 131.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy.

```
router bgp 100
neighbor 131.108.1.1 remote-as 200
neighbor 131.108.1.1 soft-reconfiguration inbound
```

### Related commands

**clear ip bgp**

**neighbor peer-group (creating)**

#### 56.1.76 neighbor timers

To set the timers for a specific BGP peer or peer group, use the `neighbor timers` command in router configuration mode. To clear the timers for a specific BGP peer or peer group, use the `no` form of this command.

**neighbor** *{ip-address | peer-group-name}* **timers** **keepalive** *holdtime*

**no neighbor** *{ip-address | peer-group-name}* **timers** **keepalive** *holdtime*

### Parameter

parameter	description
<i>ip-address</i>	A BGP peer or peer group IP address.
<i>peer-group-name</i>	Name of the BGP peer group.
<i>Keepalive</i>	Frequency (in seconds) with which the software sends keepalive messages to its peer.
<i>Holdtime</i>	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead.

### Default

keepalive: 60 s

holdtime: 180 s

### Command mode

BGP configuration mode

## Instruction

Generally, the value of holdtime is three times larger than keepalive. If you configure 0 as the value of keepalive and holdtime, then the sending of keepalive packets is disabled, which needs tcp connection manager to inform BGP module for state change.

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the timers bgp command.

## Example

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.98.47.10:

```
router bgp 109
neighbor 192.98.47.10 timers 70 210
```

### 56.1.77 neighbor update-source

To have the software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the neighbor update-source command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the no form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **update-source interface**

**no neighbor** {*ip-address* | *peer-group-name*} **update-source interface**

## Parameter

parameter	description
<i>ip-address</i>	<b>IP address of the BGP-speaking neighbor.</b>
<i>peer-group-name</i>	<b>Name of a BGP peer group.</b>
<i>Interface</i>	<b>Interface name</b>

## Default

Best local address

## Command mode

BGP configuration mode

## Instruction

By default, the ip module decides the local ip address of TCP connection when BGP establishes the connection. IP module decides interface depending on routes, and then binds the main ip address of this interface as the local address of TCP. Use the update-source command can bind the main ip address of the local specified interface during the establishment of TCP connection.

It is generally specified to use loopback interface, for the loopback interface 's protocol state is always up. And so this keeps the stability of BGP session and avoids route fluctuation.

If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command.

### Example

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface:

```
router bgp 110
network 160.89.0.0
neighbor 160.89.2.3 remote-as 110
neighbor 160.89.2.3 update-source Loopback0
```

### Related commands

#### **neighbor peer-group (creating)**

#### *56.1.78 neighbor weight*

To assign a weight to a neighbor connection, use the `neighbor weight` command in address family or router configuration mode. To remove a weight assignment, use the `no` form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **weight** *weight*

**no neighbor** {*ip-address* | *peer-group-name*} **weight** *weight*

### Parameter

parameter	description
<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>Weight</i>	Weight to assign. Acceptable values are from 0 to 65535.

### Default

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

### Command mode

BGP configuration mode

### Instruction

BGP routing metric is the important standard to choose routes. The default metric of all routes that learned from neighbors is 0. Use this command to set metric for routes that learned from neighbor.

If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command.

### Example

The following router configuration mode example sets the weight of all routes learned via 151.23.12.1 to 50:

```
router bgp 109 neighbor 151.23.12.1 weight 50
```

Related commands

**neighbor peer-group (creating)**

**set weight 23**

### 56.1.79 network (BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP), use the network command. To remove an entry from the routing table, use the no form of this command.

**network A.B.C.D/n route-map map-name backdoor**

**no network A.B.C.D/n route-map map-name backdoor**

Parameter

parameter	description
<i>A.B.C.D/n</i>	<b>Network prefix that BGP will advertise</b>
<i>route-map</i>	<b>The specified route map</b>
<i>map-name</i>	<b>Name of the route map</b>
<i>backdoor</i>	<b>Backdoor network</b>

Default

No networks are specified.

Command mode

BGP configuration mode

Instruction

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

A totally same route in the main routing table of IP is the basis for the network configured with the network command to become effective.

A more precise or totally same route in the local BTP routing table is the basis for the network to become effective that configured with the aggretegate-address command.



The length of mask code is generated in term of standard network type if not specified Use the route-map to configure route's attribute.

The backdoor network is used to modify route distance rather than to generate routes. It changes route's default distance that learned from the neighbor to the local route's distance. The default value is 200.

The maximum number of network commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

### Example

The following example sets up network 131.108.0.0/8 to be included in the BGP updates:

```
router bgp 120
network 131.108.0.0/8
```

### Related commands

**redistribute (BGP)**

**aggregate-address**

#### 56.1.80 redistribute(BGP)

To redistribute a route process to Border Gateway Protocol (BGP), use the redistribute command. To remove the redistribute command from the configuration file, use the no form of this command.

**redistribute protocol** [*process-id*] [route-map *map-name*]

**no redistribute protocol** [*process-id*] [route-map *map-name*]

### Parameter

parameter	description
<i>protocol</i>	Type of routing protocol
<i>process-id</i>	Process id of routing protocol, such as process id of ospf
<i>route-map</i>	Applies route map to configure route attribute
<i>map-name</i>	Name of route map

### Default

disabled

### Command mode

BGP configuration mode

### Instruction

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

Use redistribute command to include routes dynamically to BGP. The change of route source will be reflected to BGP automatically. The automatically-included routes will be informed to other neighbors. The configuration of the redistribute command will re-check the specified type of routes in the routing table. The outer routes in OSPF will not be included to BGP.

Use the route-map to configure route's attribute.

### Example

The following example configures routes from OSPF process 23 to be redistributed into BGP:

```
router bgp 109
redistribute ospf 23
```

### Related commands

**route-map 1**

#### 56.1.81 router bgp

To configure the BGP routing process, use the router bgp command in global configuration mode. To remove a routing process, use the no form of this command.

**router bgp** *as-number*

**no router bgp** *as-number*

### Parameter

parameter	description
<i>as-number</i>	Number of autonomous system

### Default

No BGP routing process is enabled by default.

### Command mode

global configuration mode

### Instruction

The system allows to configure one BGP process at most. The BGP task is established in the process of system initialization, and it is activated when the BGP process is started up. The BGP task only receives information from command module without configuring the BGP

process. It is not related to routing module or any other module and will not response other information. The related show and clear command are all invalid.

Use no router bgp command to delete BGP process, and at the same time other configuration related to BGP will also be deleted, such as neighbors and so on. The BGP route in routing table is also be deleted.

To configure BGP process using the show running and show ip bgp summary command to check.

### Example

The following example configures a BGP process for autonomous system 200:

```
router bgp 200
```

### Related commands

**neighbor remote-as**

#### 56.1.82 show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the show ip bgp command in user EXEC or privileged EXEC mode.

**show ip bgp [network]**

### Parameter

parameter	description
<i>network</i>	<b>Displays the specified routing information</b>

### Command mode

EXEC

### Instruction

The show ip bgp command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

### Example

The following is a group of BGP displaying information. The former two lines display some marked information.

Status code indicates the status of the table entry. The status is displayed at the beginning of each line in the table. S indicates the table entry is suppressed, which is the invalid route and will not be chosen. D indicates the table entry is dampened, which is the invalid route. H indicates the table entry history, which is not a ture route and is the invalid route. "\*" indicates the table entry is valid, which can be chosen as the best route." > "indiates the table entry is the best entry to use for that network. "I" indicates the table entry was learned via an internal BGP (iBGP) session.

Origin codes indicates the origin of the entry. I is the entry originated from an Interior Gateway Protocol (IGP). E is the entry originated from an Exterior Gateway Protocol (EGP). ? is the origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.

IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network. Local preference value as set with the set local-preference route-map configuration command. The default value is 100. Weight of the route as set via autonomous system filters. Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The last line displays number of routes, including all valid and invalid routes.

```
B3710_118#show ip bgp
```

Status codes: s suppressed, d damped, h history, \* valid, > best, i internal Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.168.10.0/24	192.168.69.5	0	10	400	i
*>i192.168.10.0/24	192.168.69.14	100	0	(65030)	400 i
*>i192.168.11.0/24	192.168.69.14	100	0	(65030)	400 i
* 192.168.65.0/30	192.168.69.1	100	0	(65020)	10 ?
*> 192.168.65.0/30	192.168.69.5		0	10	?
* 192.168.65.4/30	192.168.69.1	100	0	(65020)	10 ?
*> 192.168.65.4/30	192.168.69.5		0	10	?
* 192.168.65.8/30	192.168.69.1	100	0	(65020)	10 ?
*> 192.168.65.8/30	192.168.69.5		0	10	?
* 192.168.66.0/30	192.168.66.2	100	0	(65020)	?
*> 192.168.66.0/30	0.0.0.0		32768		?
* i192.168.66.4/30	192.168.66.6	100	0		?
*> 192.168.66.4/30	0.0.0.0		32768		?
*>i192.168.66.8/30	192.168.66.6	100	0		?
*>i192.168.67.0/30	192.168.69.18	200	100	0	500 ?

Number of displayed routes: 15

#### Related commands

```
show ip bgp community
```

```
show ip bgp neighbors
```

```
show ip bgp paths
```

```
show ip bgp prefix-list
```

```
show ip bgp regexp
```

```
show ip bgp summary
```

### 56.1.83 show ip bgp community

To display routes that belong to specified BGP communities, use the `show ip bgp community` command in EXEC mode.

```
show ip bgp community
```

#### Parameter

none

#### Command mode

exec

#### Instruction

This command is used to display statistics information of BGP communities attribute structure in the system.

#### Related commands

```
show ip bgp
```

```
show ip bgp neighbors
```

```
show ip bgp paths
```

```
show ip bgp prefix-list
```

```
show ip bgp regexp
```

```
show ip bgp summary
```

### 56.1.84 show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the `show ip bgp neighbors` command.

```
show ip bgp neighbors [ip-address] [received-routes | routes | advertised-routes]
```

#### Parameter

parameter	description
<i>ip-ddress</i>	IP address of a neighbor. If this parameter is omitted, information about all neighbors is displayed.
<i>received-routes</i>	Displays all received routes (both accepted and rejected) from the specified neighbor.
<i>routes</i>	Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the <code>received-routes</code> keyword.
<i>advertised-routes</i>	Displays all routes that have been advertised to neighbors.

## Command mode

EXEC

## Instruction

Use the `show ip bgp neighbors` command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

## Related commands

`show ip bgp`

`show ip bgp community`

`show ip bgp paths`

`show ip bgp prefix-list`

`show ip bgp regexp`

`show ip bgp summary`

### *56.1.85 show ip bgp paths*

To display all the BGP paths in the database, use the `show ip bgp paths` command in EXEC mode.

`show ip bgp paths`

## Parameter

none

## Command mode

EXEC

## Instruction

This command is used to display statistics information of BGP paths structure.

## Related commands

`show ip bgp`

`show ip bgp community`

`show ip bgp neighbors`

`show ip bgp prefix-list`

`show ip bgp regexp`

```
show ip bgp summary
```

### 56.1.86 show ip bgp prefix-list

To display information about a prefix list or prefix list entries, use the show ip prefix-list command.

```
show ip bgp prefix-list {prefix-list name}
```

Parameter

parameter	description
<i>prefix-list name</i>	<b>Name of prefix-list</b>

Command mode

EXEC

Instruction

This command specifies prefix-list to filter display of the show ip bgp command. Only the routes matching the prefix-list will be displayed.

Related commands

```
show ip bgp
```

```
show ip bgp community
```

```
show ip bgp neighbors
```

```
show ip bgp prefix-list
```

```
show ip bgp regexp
```

```
show ip bgp summary ip prefix-list
```

```
ip prefix-list description
```

```
ip prefix-list sequence-number
```

```
show ip prefix-list
```

```
clear ip prefix-list
```

### 56.1.87 show ip bgp regexp

To display routes matching the autonomous system path regular expression, use the show ip bgp regexp command in EXEC mode.

```
show ip bgp regexp regular-expression
```

Parameter

parameter	description
<i>regular-expression</i>	<b>Regular expression to match the BGP autonomous system paths.</b>

## Command mode

EXEC

## Instruction

This command specifies the regular expression to filter the display of the `show ip bgp` command. Only the routes matching the regular expression will be displayed.

## Related commands

`show ip bgp`

`show ip bgp community`

`show ip bgp neighbors`

`show ip bgp prefix-list`

`show ip bgp regexp`

`show ip bgp summary`

### *56.1.88 show ip bgp summary*

To display the status of all Border Gateway Protocol (BGP) connections, use the `show ip bgp summary` command.

`show ip bgp summary`

## Parameter

This command has no parameters or keywords.

## Command mode

EXEC

## Instruction

The `show ip bgp summary` command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

BGP attribute and cache entries are displayed individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

## Example

The following is sample output from the `show ip bgp summary` command:

```
router bgp 4
```

```
BGP local AS is 4
```



Router ID is 192.168.20.72

IGP synchronization is enabled

Distance: external 20 internal 200

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/Pref
192.168.20.12	4	5	0	0	0	0	0	never	Connect

#### Related commands

**show ip bgp**

**show ip bgp community**

**show ip bgp neighbors**

**show ip bgp paths**

**show ip bgp prefix-list**

**show ip bgp regexp**

**show ip bgp summary**

#### *56.1.89 synchronization*

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the synchronization command in address family or router configuration mode. Use the no form of this command to disable this function.

**synchronization**

**no synchronization**

**Parameter**

none

**Default**

enabled

**Command mode**

BGP configuration mode

**Instruction**

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the software to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

IGP function is enabled by default.

To enable to advertise a network route without waiting for the IGP, use the no form of this command.

## Example

The following example enables router to advertise the route without waiting for IGP synchronization.

```
router bgp 120
no synchronization
```

## Related commands

**router bgp**

### 56.1.90 table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the table-map command in address family or router configuration mode. To disable this function, use the no form of the command.

**table-map** <name>

**no table-map** <name>

## Parameter

parameter	description
name	Route map name from the route-map command.

## Default

none

## Command mode

BGP configuration mode

## Instruction

This command adds the route map name defined by the route-map command to the IP routing table. This command is used to set the tag name and the route metric to implement redistribution.

## Example

none

## Related commands

none

### 56.1.91 timers

To adjust BGP network timers, use the timers bgp command. To reset the BGP timing defaults, use the no form of this command.

**timers bgp** <keepalive> <holdtime>

**no timers bgp** <keepalive> <holdtime>

## Parameter

parameter	description
<i>keepalive</i>	Frequency (in seconds) with which the software sends keepalive messages to its peer.
<i>holdtime</i>	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead.

## Default

Keepalive: 60 seconds

Holdtime: 180 seconds

## Command mode

BGP configuration mode

## Instruction

Configure BGP neighbor clock in global configuration mode to modify default clock configuration. The configuration towards neighbor is prior to global configuration.

## Example

The following example changes the keepalive timer to 10 seconds and the hold-time timer to 40 seconds:

```
router bgp 100
timers bgp 10 40
```

## Related commands

**neighbor timers**

# Chapter 57 Ripng Commands

## 57.1 aggregate-address

To designate the aggregation route of the RIPNG instances, run the following first one of the commands:

```
aggregate-address X:X:X::X/<0-128>
no aggregate-address X:X:X::X/<0-128>
```

## Parameter

*X:X:X::X/<0-128>* Designates the prefix of IPv6 aggregation network.

## Default value

There is no aggregation route.

## Command mode

RIPNG configuration mode

**Instruction**

None

**Example**

The following example shows how to aggregate the sub-route of 2006:4:5::/35 :

```
Router_config_ripng_r1#aggregate-address 2006:4:5::/35
```

**Related command**

None

**57.2 debug ipv6 rip**

To open the RIPNG debug switch, run the first one of the following two commands:

```
debug ipv6 rip [word] [ events | send | receive | database | all ]
```

```
no debug ipv6 rip
```

**Parameter**

<i>word</i>	<b>Stands for the name of the RIPNG instance.</b>
<i>events</i>	
<i>Displays the RIP event.</i>	
<i>send</i>	<b>Displays the transmitted RIP packets.</b>
<i>receive</i>	<b>Displays the received RIP packets.</b>
<i>database</i>	<b>Displays the detailed change of the RIPNG route.</b>
<i>all</i>	<b>Opens all debug items.</b>

**Default value**

All debug items are disabled.

**Command mode**

EXEC

**Instruction**

This command can be used to trace the main procedures of RIPNG.

**Example**

```
router# debug ipv6 rip r1 event
```

The example shows how to enable the debugging switch of the RIPNG event.

**Related command**

None

### 57.3 *default-information*

To notify the default route, run the following command:

```
default-information {only | originate} [metric_value]
```

```
no default-information {only | originate} [metric_value]
```

Parameter

<i>metric_value</i>	It is an optional parameter, which is used to specify the default metric value of the default route.
---------------------	--

Default value

There is no default route and the default metric value is 1.

Command mode

RIPNG configuration mode

Instruction

No matter whether a default route exists in the main routing table, another default route will be generated in the RIPNG routing table; and if the following parameters exist, you have to know their meaning respectively:

only: only the default route is notified.

originate: both the current route and the default route are notified.

Example

The following example shows how to generate the default route and how to notify only the default route:

```
Router_config_ripng_r1# default-information only
```

Related command

None

### 57.4 *default-metric*

To designate the default metric of the forward-route, run the first one of the following commands:

```
default-metric value
```

```
no default-metric
```

Parameter

value

It is used to specify the default metric value of the forward-route, which ranges between 1 and 15. .

Default value

The default metric of the forward-route is 1.

### Command mode

RIPNG configuration mode

### Instruction

The metric ranges between 1 and 15 and it is used to specify the default metric when RIPNG forwards other protocols and RIPNG instances.

### Example

```
Router_config_ripng_r1#default-metric 3
```

The above-mentioned example shows how to set the metric of route forwarding to 3.

### Related command

redistribute

## **57.5 connect-metric**

To specify the default metric of the directly-connected route, run the first one of the following commands:

**connect-metric value**

**no connect-metric**

### Parameter

value

It is used to specify the default metric value of the directly-connected route, which ranges between 1 and 15. .

### Default value

The default metric the directly-connected route is 1.

### Command mode

RIPNG configuration mode

### Instruction

The metric ranges between 1 and 15 and is used to specify the default metric of the RIPNG directly-connected route.

### Example

```
Router_config_ripng_r1#connect-metric 3
```

The above-mentioned example shows how to set the metric of the directly-connected route to 3.

### Related command

redistribute

## 57.6 *distance*

To set the management distance, run the first one of the following two commands:

```
distance weight [ X:X:X:X::X/<0-128> [Acc-list_name]
```

```
no distance weight [ X:X:X:X::X/<0-128> [Acc-list_name]
```

Parameter

parameter	Remarks
<i>Weight</i>	<b>Stands for the management distance, ranging between 1 and 255. It is recommended to set it to a value between 10 and 255. If the parameter is used alone, the router will take it as the default management distance if the router does not have relative regulations about a routing information. When the management distance of a route is 255, this route will not be added to the routing table.</b>
<i>X:X:X:X/&lt;0-128&gt;</i>	<b>This parameter is optional. It stands for the prefix of the source IPv6.</b>
<i>Acc-list_name</i>	<b>This parameter is optional. It stands for the IP access control list.</b>

Default value

The default RIPNG management distance is 120.

Command mode

RIPNG configuration mode

Instruction

The management distance is an integer from 0 to 255. In general, the bigger the value is, the more incredible the value is. If the optional parameter, access-list-name, is used in the command, the access control list is applied when a one-hop route is added to the routing table. In this way, you can filter the paths of some network according to the address of the router provided by the routing information.

Example

The following example shows that the distance of the route received from network **af::/64** is set to 100.

```
router ripng r1
distance 100 af::/64
```

Related command

None

## 57.7 *filter*

To set the filtration for RIPNG route reception and transmission, run the first one of the following two commands.

```
filter interface-type interface-number {in | out} access-list | gateway | prefix-list
```

**no filter** *interface-type interface-number* {**in** | **out**} *access-list* | *gateway* | *prefix-list*

#### Parameter

parameter	Remarks
<i>interface-type</i>	Designates the interface type.
<i>interface-number</i>	Designates the port ID.
<i>in</i>	Filters the input RIPng routes.
<i>out</i>	Filters the output RIPng routes.
<i>access-list</i>	Uses the ACL to filter routes.
<i>gateway</i>	Uses the ACL to filter gateways.
<i>prefix-list</i>	Uses the prefix list to filter routes.

#### Default value

None

#### Command mode

RIPNG configuration mode

#### Instruction

This command is used to filter those received and to-be-transmitted RIPng routes.

#### Example

The following example shows how the routes, received by the RI instance from interface e1/1, are filtered by ACL and added to the routing table if they meet the already configured condition or deleted if they do not meet the above-mentioned condition.

```
Router_config_ripng_r1#filter e1/1 in acc acc-name
```

#### Related command

None

### 57.8 **ipv6 rip enable**

To enable a RIPng instance on a port, run the first one of the following two commands:

**ipv6 rip** *word* **enable**

**no ipv6 rip** *word* **enable**

#### Parameter

*word*

It stands for the name of the routing process instance.

#### Default value

None



**Command mode**

Port configuration mode

**Instruction**

This command is used to enable a RIPng instance on a port. If no RIPng instance exists and the number of the current instances is less than the maximum, a new instance will be generated and then be enabled.

**Example**

```
Router_config# int e2/1
```

```
Router_config_e2/1# ipv6 rip r1 enable
```

**Related command**

```
Show ipv6 rip
```

**57.9 ipv6 rip passive**

To set the passive port and cancel route update on a port, run the first one of the following two commands:

**ipv6 rip passive****no ipv6 rip passive****Parameter**

None

**Default value**

None

**Command mode**

Port configuration mode

**Instruction**

If a port is set to be a passive one, the transmission of update packets will be canceled on this port and the update packets will continually be transmitted out from other ports.

**Example**

The following example shows how to set port e2/1 to be the passive port to receive updated routes but not to transmit them.

```
R142_config_e2/1# ipv6 rip passive
```

**Related command**

None

**57.10 ipv6 rip poison-reverse**

To apply poison reverse on a port, run the first one of the following two commands:

**ipv6 rip poison-reverse**

**no ipv6 rip poison-reverse**

Parameter

word

It stands for the name of the routing process instance. poison-reverse

It means to enable poison reverse on a port.

Default value

The poison reverse is disabled by default.

Command mode

Port configuration mode

Instruction

This command is used to enable the word RIPng instance to enable poison reverse on this port.

Example

The following example shows that the R1 RIPng instance enables poison reverse on port e2/1:

```
R142_config_e2/1# ipv6 rip poison-reverse
```

Related command

None

### **57.11 ipv6 rip split-horizon**

To apply horizontal split on a port, run the first one of the following two commands:

**ipv6 rip split-horizon**

**no ipv6 rip split-horizon**

Parameter

<i>word</i>	<b>Standing for the name of the routing process instance</b>
<i>split-horizon</i>	<b>Meaning to apply horizontal split on a port</b>

Default value

The horizontal split is enabled by default.

Command mode

Port configuration mode

Instruction

In the default settings, all instances enable the horizontal split.

### Example

The following example shows that the R1 RIPng instance enables the horizontal split on port e2/1:

```
R142_config_e2/1# ipv6 rip split-horizon
```

### Related command

None

## **57.12 router ripng**

To set a RIPng instance globally, run the first one of the following two commands:

```
router ripng word
```

```
no router ripng word
```

### Parameter

Word            Standing for the name of the RIPng instance

### Default value

None

### Command mode

Global configuration mode

### Instruction

In the default settings, up to 4 RIPng instances can be generated.

After the configuration command is entered, the router prompt changes to **Router\_config\_ripng\_r1#**.

### Example

```
Router_config#router ripng r1
```

```
Router_config_ripng_r1#
```

### Related command

```
ipv6 rip word enable
```

## **57.13 max-path**

To set the number of equivalent routes allowed by the RIPng instance, run the first one of the following two commands:

```
max-path value
```

```
no max-path
```

### Parameter

Value

Setting the number of equivalent routes allowed by the RIPng instance

Default Value

4

Command mode

RIPNG configuration mode

Instruction

This command is used to set the maximum of equivalent routes in a RIPng instance and the maximum of equivalent routes is 6.

Example

The following example shows how to set the maximum of equivalent routes in the R1 RIPng instance to 5.

```
Router_config_ripng_r1#max-path 5
```

Related command

None

### 57.14 neighbor

To specify a neighbor and transmit updates to this specified neighbor, run the first one of the following two commands:

```
neighbor ipv6-addr interface interface-number
```

```
no neighbor ipv6-addr interface interface-number
```

Parameter

<i>ipv6-addr</i>	<b>Standing for the IPv6 address</b>
<i>interface</i>	<b>Designating an interface</b>
<i>interface-number</i>	<b>Standing for a port ID</b>

Default value

None

Command mode

RIPNG configuration mode

Instruction

You can use this command to specify an address to be the neighbor of a specific interface and then the routing information transmitted from this port will be sent in the unicast form to the neighbor.

## Example

The following example shows how to set neighbor fe::2 on port f0/0.

```
Router_config# router ripng r1
```

```
Router_config_ripng_r1#neighbor fe::2 f0/0
```

## Related command

None

## 57.15 offset

To set the in/out metric of a RIPng instance on a port, run the first one of the following two commands:

```
offset interface-type interface-number {in | out} acl-name value
```

```
no offset interface-type interface-number {in | out}
```

## Parameter

parameter	Remarks
<i>interface-type</i>	<b>Designates the interface type.</b>
<i>interface-number</i>	<b>Designates the port ID.</b>
<i>in</i>	<b>Adds the metric for an incoming RIPng route.</b>
<i>out</i>	<b>Adds the metric for an outgoing RIPng route.</b>
<i>acl-name</i>	<b>Stands for the IP access control list.</b>
<i>value</i>	<b>Adds the specified metric for the received RIPng route.</b>

## Default value

The default value of the in parameter is 1.

The default value of the out parameter is 0.

## Command mode

RIPNG configuration mode

## Instruction

This command is used to specify the metric for those received and to-be-transmitted RIPng routes.

## Example

The following example shows that the routes received by the R1 instance from port e1/1 are added with a metric, 8, after ACL filtration and then added to the routing table.

```
Router_config_ripng_r1#offset e1/1 in acc 8
```

## Related command

None

**57.16 port**

To set a specific UDP port for the RIPng instance, run the following command:

```
port port-number
```

**Parameter**

*port-number*

Standing for the UDP port ID, which is a value between 521 and 65535

**Default value**

521

**Command mode**

RIPNG configuration mode

**Instruction**

You can use this command to specify the UDP port of the Ripng instance. The default value of the UDP port ID is 521. When two instances are enabled on a same port, the UDP port cannot be the same.

**Example**

The following example shows how to set the ID of the UDP port of the R1 instance to 555:

```
Router_config# router ripng r1
```

```
Router_config_rip_r1# port 555
```

**Related command**

None

**57.17 redistribute**

To enable other routing domains to forward routes to RIPng, run the first one of the following two commands:

```
redistribute protocol [ protocol-id | instance name ] [route-map map-name]
```

```
no redistribute protocol [ protocol-id | instance name ] [route-map map-name]
```

**Parameter**

<i>Protocol</i>	<b>Standing for the type of the forwarded protocol</b>
<i>protocol-id</i>	<b>Standing for the ID of the forwarded process</b>
<i>instance name</i>	<b>Standing for the name of the forwarded RIPng instance</b>

**Default value**

disable

## Command mode

RIPNG configuration mode

## Instruction

This command is used to forward the routes from other routing domains and other RIPng instances. The metric of a forwarded route is set by the default-metric command and its default value is 1.

## Example

The following example shows how to forward the BGP route whose AS ID is 4.  
Router\_config\_ripng\_r1#redis bgp 4 route-map rm

## Related command

None

## 57.18 show ipv6 rip

To display the RIPng related information, run the following command:

```
show ipv6 rip [name] [database | summary | interface]
```

## Parameter

<i>Name</i>	Standing for the name of the RIPng instance
<i>Database</i>	Displaying the detailed information about the routes of a designated RIPng instance
<i>summary</i>	Displaying the detailed statistics information about the routes of a designated RIPng instance
<i>interface</i>	Displaying where the RIPng instance is enabled

## Default value

None

## Command mode

Any non-user mode

## Instruction

None

## Example

The following example shows on which port the R1 instance is enabled:

```
router#sho ipv6 rip r1 interface
```

```
ripng instance r1/1 enable on: FastEthernet0/0 , FastEthernet0/1
```

## Related command

None

### 57.19 timers

To adjust the timeout value in each clocks in RIPng, run the first one of the following two commands:

**timers** *update/holddown/garbage* value

**no timers** *update/holddown/garbage*

Parameter

<i>Update</i>	<b>Standing for the interval of regular updates</b>
<i>Holddown</i>	<b>Standing for the timeout time of the invalid timer</b>
<i>Garbage</i>	<b>Standing for the waiting time of route deletion</b>

Default value

Update 30s

Holddown 180s

Garbage 120s

Command mode

RIPNG configuration mode

Instruction

Do not adjust the value of each timer randomly. If necessary to do so, you have to note the relationships between 3 timers.

Example

None

Related command

None



## Chapter 58 OSPFv3 Configuration Commands affects ONLY PXT-S2790G/2795G or Higher

### 58.1 OSPFv3 Configuration Commands

The OSPFv3 configuration commands include:

- area default-cost
- area nssa
- area range
- area stub
- area virtual-link
- debug ipv6 ospf
- debug ipv6 ospf events
- debug ipv6 ospf ifsm
- debug ipv6 ospf lsa
- debug ipv6 ospf n fsm
- debug ipv6 ospf nsm
- debug ipv6 ospf packet
- debug ipv6 ospf route
- default-information originate
- default-metric
- filter
- ipv6 ospf area
- ipv6 ospf cost
- ipv6 ospf database-filter all out
- ipv6 ospf dead-interval
- ipv6 ospf hello-interval
- ipv6 ospf mtu-ignore
- ipv6 ospf neighbor
- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay

- passive-interface
- redistribute
- router ospfv3
- router-id
- show ipv6 ospf
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbor
- show ipv6 ospf route
- show ipv6 ospf virtual-link
- summary-prefix
- timers delay
- timers hold

### 58.1.1 area default-cost

To specify the cost of the default summary route in the NSSA or STUB area, run the first one of the following two commands:

**area *area-id* default-cost *cost***

**no area *area-id* default-cost**

Parameter

parameter	Description
<i>area-id</i>	Means the ID of the NSSA or STUB area.
<i>cost</i>	Means the cost of the default summary route.

Default value

The default value is 1.

Command mode

Routing configuration mode

Instruction

The command is helpful only when it is used on the boundary router connecting the NASSA area or the STUB area.

After the **area stub default-information-originate** command is configured, the cost configured by this command will be used in LSA to set the corresponding cost.

Example

The following example shows how to set the default cost of stub domain 36.0.0.0 to 20:

```
interface vlan 1
ipv6 enable
ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
router-id 2.2.2.2
area 36.0.0.0 stub
area 36.0.0.0 default-cost 20
```

#### Related command

```
area nssa
area stub
```

#### 58.1.2 area nssa

To configure a NSSA area, run the first one of the following two commands:

```
area area-id nssa [default-information-originate [metric value] [metric-type {1 | 2}]]
[interval value] [no-redistribute] [no-summary] [range {ipv6-prefix/prefix-length}] [advertise
| not-advertise]] [translator {always|candidate}]
```

```
no area area-id nssa [default-information-originate [metric value] [metric-type {1 | 2}]]
[interval value] [no-redistribute] [no-summary] [range {ipv6-prefix/prefix-length}] [advertise
| not-advertise]] [translator {always|candidate}]
```

#### Parameter

parameter	Description
<i>area-id</i>	Sets the ID of the NSSA area. It can be a decimal number or an IP address.
<i>default-information-originate</i>	Means to send the default route to the NSSA area.
<i>metric value</i>	Stands for the cost of the default route, which ranges from 1 to 16777214.
<i>metric-type</i> {1   2}	Means the cost type of the default route.
<i>interval value</i>	Means the stable time of the NSSA translator role, which ranges from 1 to 65535.
<i>no-redistribute</i>	Means not to redistribute a route to the NSSA area.
<i>no-summary</i>	Forbids the ABR router to send the summary link to the NSSA area.
<i>range</i>	Means to conduct summary when type-7 LSA is translated into type-5 LSA.
<i>translator</i>	Stands for the NSSA translator role; if the parameter “always” is used, it means it is always the translator, and if it is the parameter “candidate”, it means it can be chosen as a translator.

**Default value**

Non-NSSA area

**Command mode**

Routing configuration mode

**Instruction**

All routers and access servers in the NSSA area will be configured by the **area nssa** command.

To decrease the number of LSA's, you can run **no summary** on the ABR router to forbid the summary LSA to enter the NSSA area.

The parameter "no-distribute" is always used for ABR and its purpose is to stop redistributed routes from being sent to the NSSA area.

**Example**

The following example shows how to set the NSSA area of 36.0.0.0:

```
interface vlan 1
ipv6 enable
ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
router-id 2.2.2.2
area 36.0.0.0 nssa
!
```

**Related command****area stub****58.1.3 area range**

To summarize the routes at the field boundary, run **area area-id range {ipv6-prefix /prefix-length} [advertise | not-advertise]**. To cancel the previous settings, run **no area range**.

```
area area-id range {ipv6-prefix /prefix-length} [advertise | not-advertise]
```

```
no area area-id range {ipv6-prefix /prefix-length} [advertise | not-advertise]
```

**Parameter**

parameter	Description
<i>area-id</i>	Means the fields where the fields will be summarized. It can be a decimal number or an IPv6 address.
<i>ipv6-prefix</i>	Means the prefix of the IPv6 address.
<i>prefix-length</i>	Means the length of the IPv6 address' prefix.

<i>advertise</i>	<b>Means that the routes are released after they are summarized.</b>
<i>not-advertise</i>	<b>Means that the routes are not released after they are summarized.</b>

### Default value

The command has no effect by default.

### Command mode

Routing configuration mode

### Instruction

The **area range** command is not run on the ABR router, enabling ABR to be broadcast to other routers through a summary route. In this way, the route of the field boundary is miniaturized. As to the outside of the area, each address range has only one summary route.

The command can be configured on the routers in multiple areas, and OSPF, hence, can summarize many address ranges.

### Example

The following example shows how to set the prefix of the summarized IPv6 address in area 1, 2001:0DB8:0:1::/64:

```
interface vlan 1
no ip address
ipv6 enable
ipv6 ospf 1 area 1
!
router ospfv3 1
router-id 192.168.255.5
log-adjacency-changes
area 1 range 2001:0DB8:0:1::/64
```

#### 58.1.4 area stub

To configure a STUB area, run the first one of the following two commands. To cancel the configuration, run the other command.

```
area area-id stub [no-summary]
```

```
no area area-id stub [no-summary]
```

### Parameter

parameter	Description
<i>area-id</i>	<b>Sets the ID of the STUB area. It can be a decimal number or an IP address.</b>

<i>no-summary</i>	<b>Forbids the ABR router to send the summary link to the STUB area.</b>
-------------------	--

### Default value

Non-stub area

### Command mode

Routing configuration mode

### Instruction

All routers and access servers in the STUB area will be configured by the **area stub** command. The ABR router adopts the **default-cost** option to set the cost from the internal router to the STUB area.

To decrease the number of LSA's, you can run **no summary** on the ABR router to forbid the summary LSA to enter the STUB area.

### Example

The following example shows how to set the STUB area of 36.0.0.0:

```
interface vlan 1
ipv6 enable
ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
router-id 2.2.2.2
area 36.0.0.0 stub
!
```

### Related command

**area nssa**

#### **58.1.5 area virtual-link**

To configure a virtual link, run the first one of the following two commands.

```
area area-id virtual-link neighbor-ID [dead-interval dead-value] [hello-interval hello-value] [retransmit-interval retrans-value] [transmit-delay dly-value]
```

```
no area area-id virtual-link neighbor-ID
```

### Parameter

parameter	Description
<i>area-id</i>	<b>Specifies the transit-area of the virtual link.</b>

<i>neighbor-id</i>	<b>OSPF router ID of the peer router of virtual link</b>
<i>dead-value</i>	<b>Stands for the interval for the local router to regard that the neighbor dies, whose unit is second. The values configured at the two terminals of the virtual link must be same.</b>
<i>hello-value</i>	<b>Stands for the interval for the router to transmit the HELLO packet on the virtual link, whose unit is second. The values configured at the two terminals of the virtual link must be same.</b>
<i>retrans-value</i>	<b>Interval for the router to transmit the re-transmit packet on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same.</b>
<i>dly-value</i>	<b>Delay value which is reported by the router to LSA on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same. The values configured at the two terminals of the virtual link must be same.</b>

### Default value

The virtual link is not configured.

The default values of other parameters are shown in the following:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s

### Command mode

Routing configuration mode

### Instruction

In order to create a virtual link, you have to perform configuration at the two terminals of the virtual link. If only one terminal need be configured, the virtual link cannot function.

The **area-id** parameter cannot be zero because the transit area of the virtual link must not be the backbone area. The area-id configured at the two terminals of the virtual link must be same.

Parameters configured at the two terminals of the virtual link must be same.

After the virtual link is created (the neighborhood is in the FULL state), the virtual link works in the Demand Circuit mode, that is, the periodical Hello packet and the LSA refresh packet are not transmitted.

You can run **no area area-id virtual-link neighbor-ID** to cancel the previous configuration of the virtual link.

You also can run **show ip ospf virtual-link** to check the state of the virtual link.

### Example

The following example shows how to create a virtual link between router A and router B.

Configuration on router A (router-id: 200.200.200.1) :

!

```
interface vlan 1
no ip address
ipv6 enable
ipv6 ospf 1 area 1
!
router ospfv3 1
router-id 200.200.200.1
area 1 virtual-link 200.200.200.2
!
Configuration on router B (router-id: 200.200.200.2) :
!
interface vlan 1
no ip address
ipv6 enable
ipv6 ospf 1 area 1
!
router ospfv3 1
router-id 200.200.200.2
area 1 virtual-link 200.200.200.1
!
```

#### Related command

**show ipv6 ospf virtual-link**

#### *58.1.6 debug ipv6 ospf*

To open all debugging switches of the OSPFv3 module, run the first one of the following two commands:

**debug ipv6 ospf**

**no debug ipv6 ospf**

#### Parameter

None

#### Default value

None

#### Command mode



EXEC

### Instruction

This command can be used to collect all debugging information about the OSPFv3 for the R&D engineers and technical support staff.

### Example

```
Router# debug ipv6 ospf
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to
Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]:   consider   flooding
    through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]:   Intra-Area-Prefix-
LSA(0x38110c0)
originated
VLINK[VLINK1]: local address is 101::1VLINK[VLINK1]: peer 200.200.200.2 link
upLSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link
FastEthernet0/0
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1   *]:   Link-
LSA(0x381ec40) originated
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]:   consider   flooding
    through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x381ec20) originated
IFSM[FastEthernet0/0]: Down (InterfaceUp)
IFSM[FastEthernet0/0]: Status change Down -> Waiting SPF[0.0.0.0]: Calculation timer
scheduled [delay 5 secs]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]:   consider   flooding
    through interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x38297e0) originated
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point ROUTER[1]: Change status to ABR
IFSM[FastEthernet0/0]: Hello timer expire
Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5) OSPFv3 Header
Version 3 Type 1 (Hello) Packet length 36
```

```
Router ID 200.200.200.1
```

```
Area ID 0.0.0.1
```

```
Checksum 0x0000 Instance ID 0 OSPFv3 Hello
```

```
Interface ID 4
```

```
RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6) HelloInterval 10 RtrDeadInterval 40
```

```
DRouter 0.0.0.0 BDRouter 0.0.0.0
```

```
# Neighbors 0
```

```
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER. OSPF6D: Received ospfv3
message: OSPFV3_MSG_RCV_EVENT. OSPF6D: Received ospfv3 message:
OSPFV3_MSG_RCV_SOCKET.
```

```
.....
```

### 58.1.7 debug ipv6 ospf events

To enable the event debug switch of the OSPFv3 module, run the first one of the following two commands:

```
debug ipv6 ospf events {abr|asbr|vlink|os|router}
```

```
no debug ipv6 ospf events { abr|asbr|vlink|os|router }
```

Parameter

parameter	Description
<i>abr</i>	Opens the state change debug switch of ABR.
<i>asbr</i>	Opens the state change debug switch of ASBR.
<i>vlink</i>	Opens the state change debug switch of the virtual link.
<i>os</i>	Opens the state change debug switch of socket.
<i>router</i>	Opens the debug switch of OSPF.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can check the OSPF port and the neighbor trigger event.

Example

```
Router# debug ip ospf events
```

```
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
ROUTER[1]: Change status to ABR  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
VLINK[VLINK1]: peer 200.200.200.2 link downROUTER[1]: Change status to non-ABR  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
ROUTER[Process:1]: GC timer expire  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.  
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
```

```

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.
ROUTER[Process:1]: GC timer expire
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.
join AllDRouters on FastEthernet0/0
OSPF6D: Received ospfv3 message:
OSPFV3_MSG_RCV_EVENT. OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.
.....

```

### 58.1.8 debug ipv6 ospf ifsm

To enable the state machine's debug switch of the OSPFv3 module, run the first one of the following two commands:

```
debug ipv6 ospf ifsm {status|events|timers}
```

```
no debug ipv6 ospf ifsm {status|events|timers}
```

Parameter

parameter	Description
<i>status</i>	Opens the state debug switch of the interface state machine.
<i>events</i>	Opens the event debug switch of the interface state machine.
<i>timers</i>	Opens the timer debug switch of the interface state machine.

Default value

None

Command mode

EXEC

## Instruction

According to the information exported by the command, you can check the whole process of the state machine of the OSPF interface.

## Example

```
Router# debug ipv6 ospf ifsm
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: Down (InterfaceUp)
IFSM[FastEthernet0/0]: Status change Down -> Waiting
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[VLINK1]: Hello timer expire
IFSM[VLINK1]: ifsm_ignore called
IFSM[VLINK1]: Point-To-Point (NeighborChange)
IFSM[FastEthernet0/0]: ifsm_ignore called
IFSM[FastEthernet0/0]: Waiting (NeighborChange)
IFSM[VLINK1]: LS ack timer expire
IFSM[VLINK1]: LS ack timer expire
IFSM[VLINK1]: Point-To-Point (InterfaceDown)
IFSM[VLINK1]: Status change Point-To-Point -> Down
IFSM[VLINK1]: ifsm_ignore called
IFSM[VLINK1]: Down (NeighborChange)
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: Wait timer expire
IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.2
IFSM[FastEthernet0/0]: DR-Election[1st]: DR 200.200.200.2
IFSM[FastEthernet0/0]: Waiting (WaitTimer)
IFSM[FastEthernet0/0]: Status change Waiting -> DROther
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.1
```

```

IFSM[FastEthernet0/0]: DR-Election[1st]: DR 200.200.200.2
IFSM[FastEthernet0/0]: DR-Election[2nd]: Backup 200.200.200.1
IFSM[FastEthernet0/0]: DR-Election[2nd]: DR 200.200.200.2
IFSM[FastEthernet0/0]: DROther (NeighborChange)
IFSM[FastEthernet0/0]: Status change DROther -> Backup
IFSM[FastEthernet0/0]: Hello timer expire
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Hello timer expire
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Point-To-Point (InterfaceDown)
IFSM[VLINK1]: Status change Point-To-Point -> Down
IFSM[VLINK1]: Down (InterfaceUp)
IFSM[VLINK1]: Status change Down -> Point-To-Point
IFSM[FastEthernet0/0]: LS ack timer expire
IFSM[VLINK1]: Hello timer expire
.....

```

### 58.1.9 debug ipv6 ospf lsa

To enable the LSA-related debug switch of the OSPFv3 module, run the first one of the following two commands:

```

debug ipv6 ospf lsa { flooding|install|maxage|refresh}
no debug ipv6 ospf lsa { flooding|install|maxage|refresh}

```

Parameter

parameter	Description
<i>flooding</i>	Opens the debug switch of LSA exchange.
<i>install</i>	Opens the debug switch of LSA installation.
<i>maxage</i>	Opens the debug switch of LSA timeout.
<i>refresh</i>	Opens the debug switch of LSA-Refresh.

Default value

None

Command mode

EXEC

## Instruction

According to the information exported by the command, you can browse the operation that OSPF performs to LSA and related events.

## Example

```
router# debug ipv6 ospf lsa
```

```
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]:   consider flooding through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]:   Intra-Area-Prefix-LSA(0x3824ba0) originated
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]:   consider flooding through interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]:   consider flooding to neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3819be0) originated
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link FastEthernet0/0
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1*]:   Link-LSA(0x3819bc0) originated
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3824740) originated
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: instance(0x380bf60) created with Link State Update
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: instance(0x38246c0) created with Link State Update
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: flood started
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]:
interface[VLINK1]   consider   flooding   through
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: neighbor[200.200.200.2] consider flooding to
```

```
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: neighbor is not Full state
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: flood started

LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]:
interface[VLINK1] consider flooding through
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]:
neighbor[200.200.200.2] consider flooding to
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: neighbor is not Full state
LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: Install Inter-Area-Prefix-LSA to Area
0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding to
neighbor[200.200.200.2]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: added to
neighbor[200.200.200.2]'s
retransmit-list
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: sending update to
interface[VLINK1]
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA refreshed OSPFv3 LSA
Header LS age 0
LS type 0x2001 (Router-LSA) Advertising Router 200.200.200.1 Link State ID 0.0.0.0
LS sequence number 0x80000002 LS checksum 0x5ff7 length 40
LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[VLINK1]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through
interface[FastEthernet0/0]
LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA refreshed
OSPFv3 LSA Header
LS age 0
LS type 0x2001 (Router-LSA)
Advertising Router 200.200.200.1
Link State ID 0.0.0.0
LS sequence number 0x80000002
```



LS checksum 0x5382

length 24

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 \*]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 \*]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 \*]: Intra-Area-Prefix-LSA refreshed  
OSPFv3 LSA Header

LS age 0

LS type 0x2009 (Intra-Area-Prefix-LSA)

Advertising Router 200.200.200.1

Link State ID 0.0.0.1

LS sequence number 0x80000002

LS checksum 0x3631

length 64

.....

### 58.1.10 debug ipv6 ospf nfsm

To enable the state machine's debug switch of the OSPFv3 neighbor, run the first one of the following two commands:

**debug ipv6 ospf nfsm** {status|events|timers}

**no debug ipv6 ospf nfsm** {status|events|timers}

Parameter

parameter	Description
<i>status</i>	Opens the state debug switch of the neighbor state machine.
<i>events</i>	Opens the event debug switch of the neighbor state machine.
<i>timers</i>	Opens the timer debug switch of the neighbor state machine.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can check the whole process of the OSPF neighbor's state machine.

### Example

```
router# debug ipv6 ospf nfsm
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]:nfsm_ignore called
NFSM[200.200.200.2-00000004]: Full
(2-WayReceived)
NFSM[200.200.200.2-00000004]: Down (HelloReceived)
NFSM[200.200.200.2-00000004]: Status change Down -> Init
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Init (1-WayReceived)
NFSM[200.200.200.2-00000004]: Init (HelloReceived)
NFSM[200.200.200.2-00000004]: Init (2-WayReceived)
NFSM[200.200.200.2-00000004]: Status change Init -> 2-Way
NFSM[200.200.200.2-00000004]: 2-Way (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: 2-Way (2-WayReceived)
NFSM[200.200.200.2-00000004]: 2-Way (AdjOK?)
NFSM[200.200.200.2-00000004]: Status change 2-Way -> ExStar t
NFSM[200.200.200.2-00000004]: ExStart (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: ExStart (2-WayReceived)
NFSM[200.200.200.2-00000004]: DD Retransmit timer expire
NFSM[200.200.200.2-00000004]: ExStart (NegotiationDone)
NFSM[200.200.200.2-00000004]: Status change ExStart -> Exchange
NFSM[200.200.200.2-00000004]: Exchange (ExchangeDone)
NFSM[200.200.200.2-00000004]: Status change Exchange -> Loading
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Loading (LoadingDone)
NFSM[200.200.200.2-00000004]: Status change Loading -> Full
NFSM[200.200.200.2-80000001]: Down (HelloReceived)
```

```
NFSM[200.200.200.2-80000001]: Status change Down -> Init
NFSM[200.200.200.2-80000001]: Init (2-WayReceived)
NFSM[200.200.200.2-80000001]: Status change Init -> ExStart
NFSM[200.200.200.2-80000001]: ExStart (NegotiationDone)
NFSM[200.200.200.2-80000001]: Status change ExStart -> Exchange
NFSM[200.200.200.2-80000001]: Exchange (ExchangeDone)
NFSM[200.200.200.2-80000001]: Status change Exchange -> Loading
NFSM[200.200.200.2-80000001]: nfsm_ignore called
NFSM[200.200.200.2-80000001]: Loading (LoadingDone)
NFSM[200.200.200.2-80000001]: Status change Loading -> Full
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: Full (AdjOK?)
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
NFSM[200.200.200.2-80000001]: Full (HelloReceived)
NFSM[200.200.200.2-80000001]: nfsm_ignore called
NFSM[200.200.200.2-80000001]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: Full (HelloReceived)
NFSM[200.200.200.2-00000004]: nfsm_ignore called
NFSM[200.200.200.2-00000004]: Full (2-WayReceived)
NFSM[200.200.200.2-00000004]: LS update timer expire
NFSM[200.200.200.2-80000001]: LS update timer expire
.....
```

#### ***58.1.11 debug ipv6 ospf nsm***

To open the debug switch of information transmission between the IPv6 routing table's management module and the OSPFv3 module, run the first one of the following two commands:

```
debug ipv6 ospf nsm { redistribute | interface }
```

```
no debug ipv6 ospf nsm { redistribute | interface }
```

## Parameter

parameter	Description
<i>redistribute</i>	<b>Opens the debug switch of routing information forwarding.</b>
<i>interface</i>	<b>Opens the debug switch of interface events.</b>

## Default value

None

## Command mode

EXEC

## Instruction

According to the information exported by this command, you can browse information exchange between OSPF and routing management module.

## Example

```
router# debug ipv6 ospf nsm
```

```
Sep 17 16:43:53 OSPFv3: Received
[NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
```

```
Sep 17 16:43:53 OSPFv3: Received
[NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
```

```
Sep 17 16:43:53 OSPFv3: Received
[NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
```

```
Sep 17 16:43:53 OSPFv3: Received
[NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message
```

```
Sep 17 16:43:53 OSPFv3: Receive [NSM_MSG_GLBL_ENAIPV6] message
```

```
.....
```

**58.1.12 debug ipv6 ospf packet**

To enable the debug switch of OSPFv3 transmission and reception, run the first one of the following two commands:

```
debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack }
```

```
no debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack }
```

## Parameter

parameter	Description
<i>hello</i>	<b>Opens the debug switch of Hello packets.</b>
<i>dd</i>	<b>Opens the debug switch of DD packets.</b>
<i>ls-request</i>	<b>Opens the debug switch of IS-REQUEST packets.</b>

<i>ls-update</i>	<b>Opens the debug switch of IS-Update packets.</b>
<i>ls-ack</i>	<b>Opens the debug switch of IS-Ack packets.</b>
<i>detail</i>	<b>Observes the details of packets.</b>

### Default value

None

### Command mode

EXEC

### Instruction

According to the information exported by the command, you can check the exchange of the OSPF packets.

### Example

```

router# debug ipv6 ospf packet
Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)
OSPFv3 Header
Version 3 Type 1 (Hello) Packet length 40
Router ID 200.200.200.1
Area ID 0.0.0.1
Checksum 0x0000 Instance ID 0 OSPFv3 Hello
Interface ID 4
RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)
HelloInterval 10 RtrDeadInterval 40
DRouter 200.200.200.2 BDRouter 200.200.200.1
# Neighbors 1
Neighbor 200.200.200.2
Packet[RECV]: src(101::2) -> dst(101::1)
OSPFv3 Header
Version 3 Type 1 (Hello) Packet length 40
Router ID 200.200.200.2
Area ID 0.0.0.0
Checksum 0x5774 Instance ID 0
OSPFv3 Hello

```

```
Interface ID 2147483649
RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)
HelloInterval 10 RtrDeadInterval 40
DRouter 0.0.0.0 BDRouter 0.0.0.0
# Neighbors 1
Neighbor 200.200.200.1
RECV[Hello]: Neighbor(200.200.200.2) declare 0.0.0.0 as DR, 0.0.0.0 as Backup
Packet[SEND]: src(101::1) -> dst(101::2)
OSPFv3 Header
Version 3 Type 1 (Hello) Packet length 40
Router ID 200.200.200.1
Area ID 0.0.0.0
Checksum 0x0000 Instance ID 0 OSPFv3 Hello
Interface ID 2147483649
RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)
HelloInterval 10 RtrDeadInterval 40
DRouter 0.0.0.0 BDRouter 0.0.0.0
# Neighbors 1
Neighbor 200.200.200.2
Packet[RECV]: src(fe80::2e0:fff:fe26:a8) -> dst(ff02::5)
OSPFv3 Header
Version 3 Type 1 (Hello) Packet length 40
Router ID 200.200.200.2
Area ID 0.0.0.1
Checksum 0xa8a8 Instance ID 0 OSPFv3 Hello
Interface ID 4
RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)
HelloInterval 10 RtrDeadInterval 40
DRouter 200.200.200.2 BDRouter 200.200.200.1
# Neighbors 1
Neighbor 200.200.200.1
```

```
RECV[Hello]: Neighbor(200.200.200.2) declare 200.200.200.2 as DR, 200.200.200.1 as
Backup Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)
```

OSPFv3 Header

Version 3 Type 1 (Hello) Packet length 40

Router ID 200.200.200.1

Area ID 0.0.0.1

Checksum 0x0000 Instance ID 0 OSPFv3 Hello

Interface ID 4

RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)

HelloInterval 10 RtrDeadInterval 40

DRouter 200.200.200.2 BDRouter 200.200.200.1

# Neighbors 1

Neighbor 200.200.200.2

.....

### 58.1.13 debug ipv6 ospf route

To enable the debug switch of OSPFv3 routing information, run the first one of the following two commands:

```
debug ipv6 ospf route { ase|install|spf|ia }
```

```
no debug ipv6 ospf route { ase|install|spf|ia }
```

Parameter

parameter	Description
<i>ase</i>	Opens the debug switch of exterior routing calculation.
<i>install</i>	Opens the debug switch of routing installation procedure.
<i>spf</i>	Opens the debug switch of SPF calculation.
<i>ia</i>	Opens the debug switch of between-domain routing calculation.

Default value

None

Command mode

EXEC

Instruction

According to the information exported by the command, you can browse the calculation, deletion and addition of OSPF routes.

## Example

```
router# debug ipv6 ospf route
Route[IA:0.0.0.0]: No SPF tree, schedule SPF calculationSPF[0.0.0.1]: SPF calculation timer
expire
SPF[0.0.0.1]: SPF calculation (1st STAGE)
SPF[0.0.0.1]: Vertex[200.200.200.1-0.0.0.0]
SPF[0.0.0.1]: SPF calculation (2nd STAGE)
SPF[0.0.0.1]: SPF calculation (END)
Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsRoute[IA:0.0.0.1]: Cleanup IA route
because of no ABRsSPF[0.0.0.1]: Calculation completed [0.170000 sec]
SPF[0.0.0.1]: Calculation timer scheduled [delay 9 secs]
SPF[0.0.0.1]: SPF calculation timer expire
SPF[0.0.0.1]: SPF calculation (1st STAGE)
SPF[0.0.0.1]: Vertex[200.200.200.1-0.0.0.0]
SPF[0.0.0.1]: SPF calculation (2nd STAGE)
SPF[0.0.0.1]: SPF calculation (END)
Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsSPF[0.0.0.1]: Calculation completed
[0.180000 sec]
SPF[0.0.0.1]: Calculation timer scheduled [delay 10 secs]
SPF[0.0.0.0]: Calculation timer scheduled [delay 5 secs]
Route[IA:0.0.0.1]: 888::/64 calculating Network routeRoute[IA:0.0.0.1]: 888::/64 Can't find
route to ABR (200.200.200.2)Route[IA:0.0.0.0]: No SPF tree, schedule SPF
calculationSPF[0.0.0.0]: SPF calculation timer expire
SPF[0.0.0.0]: SPF calculation (1st STAGE)
SPF[0.0.0.0]: Vertex[200.200.200.1-0.0.0.0]
SPF[0.0.0.0]: Link[0] (200.200.200.2-128.0.0.1): Virtual-Link
SPF[0.0.0.0]: Calculate nexthop for (200.200.200.2-0.0.0.0)
Route[0.0.0.0:SPF]: ADD Stub Route for (200.200.200.2)SPF[0.0.0.0]:
Vertex[200.200.200.2-0.0.0.0]
SPF[0.0.0.0]: Link[0] (200.200.200.1-128.0.0.1): Virtual-Link
SPF[0.0.0.0]: LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *] is already in SPF tree
SPF[0.0.0.0]: SPF calculation (2nd STAGE)
SPF[0.0.0.0]: SPF calculation (END)
SPF[0.0.0.0]: Calculation completed [0.580000 sec]
```



.....

### 58.1.14 default-information originate

To introduce the default route to the OSPFv3 routing domain, run the following command:

```
default-information originate [ always | metric value | metric-type {1 | 2} | tag tag ]
```

```
no default-information originate
```

Parameter

parameter	Description
<i>Always</i>	<b>Generates and releases an ASE-LSA, which describes the default route, or just releases it out if the default route exists in the routing table.</b>
<i>metric value</i>	<b>Stands for the cost of the default route, which ranges from 1 to 16777214.</b>
<i>metric-type</i>	<b>Means the cost type of the default route.</b>
<i>tag tag</i>	<b>Means the routing identifier, which ranges from 0 to 4294967295.</b>

Default value

No default route is introduced.

Command mode

Routing configuration mode

Instruction

The redistribute command cannot introduce the default route, and if you want to introduce the default route, you can use this command.

If the always parameter is set, no matter whether the default route exists in the current routing table, ASE-LSA, describing the default route, will be released out; if the always parameter is not set, ASE-LSA will be released out only when the default route exists in the current routing table.

Example

The following example shows how to introduce the default route from the OSPFv3 autonomous system.

```
router ospfv3 1
router-id 2.2.2.2
default-information originate always
```

Related command

```
redistribute
```

### 58.1.15 *default-metric*

To set the default weight of the introduced route, run the first one of the following two commands:

**default-metric** *value*

**no default-metric**

Parameter

parameter	Description
<i>value</i>	Stands for the to-be-set route weight, ranging between 1 and 16777214.

Default value

The default route weight is 10.

Command mode

Routing configuration mode

Instruction

The default-metric command is used to set the default routing weight when the route of other routing protocol is guided into the OSPF packet. When the redistribute command is used to guide the route of other routing protocol, the default routing weight designated by the default-metric command will be guided the specific routing weight will not be specified.

Example

The following example shows how to introduce the static route and set the default route weight of other routing protocol to 3:

```
interface vlan 1
ipv6 enable
ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
router-id 2.2.2.2
default-metric 3
redistribute static
```

Related command

**redistribute**

### 58.1.16 *filter*

To set the routing filtration table, run **filter {interface-type interface-number | \*} {in | out} {access-list access-list-name | gateway access-list-name | prefix-list prefix-list-name}**. To

resume the default settings, run **no filter** {*interface-type* *interface-number* | \*} {*in* | *out* } {*access-list* *access-list-name* | *gateway* *access-list-name* | *prefix-list* *prefix-list-name*}.

**filter** {*interface-type* *interface-number* | \*} {*in* | *out* } {*access-list* *access-list-name* | *gateway* *access-list-name* | *prefix-list* *prefix-list-name*}

**no filter** {*interface-type* *interface-number* | \*} {*in* | *out*} {*access-list* *access-list-name* | *gateway* *access-list-name* | *prefix-list* *prefix-list-name*}

#### Parameter

<i>interface-type</i>	<b>Interface type</b>
*	<b>All interfaces</b>
<i>In</i>	<b>Filtrates the received OSPF routes.</b>
<i>out</i>	<b>Filters the transmitted routes, which is not for a specific interface but for all interfaces.</b>
<i>access-list-name</i>	<b>Name of the IP access control list</b>
<i>access-list-name</i>	<b>Name of the IP access control list</b>
<i>prefix-list-name</i>	<b>Name of the prefix list</b>

#### Default value

None

#### Command mode

Routing configuration mode

#### Example

The following example shows how to filter the received routes according to the mylist ACL.

```
router ospfv3 1
filter * in access-list mylist
```

#### Related command

None

#### 58.1.17 ipv6 ospf area

To enable the OSPFv3 protocol on an interface and specify an area for this interface, run the first one of the following two commands:

```
ipv6 ospf process-id area area-id [instance instance-id]
no ipv6 ospf process-id area area-id [instance instance-id]
```

#### Parameter

parameter	Description
<i>process-id</i>	Stands for the OSPF process.
<i>area-id</i>	Stands for the OSPF area ID, which is specified by the interface.
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

#### Default value

None

#### Command mode

Interface configuration mode

#### Example

The following example shows how to enable OSPFv3 process 1 for interface vlan1 and set its area ID to 0.

```
interface vlan 1
ipv6 enable
ipv6 ospf 1 area 0
!
router ospfv3 1
router-id 2.2.2.2
```

#### Related command

None

#### 58.1.18 *ipv6 ospf cost*

To designate the cost for the OSPFv3 protocol running on the interface, run **ipv6 ospf cost cost**. To resume the default settings, run **no ipv6 ospf cost**.

```
ipv6 ospf cost cost [instance instance-id]
```

```
no ipv6 ospf cost cost [instance instance-id]
```

#### Parameter

parameter	Description
<i>cost</i>	Cost for the OSPF protocol, which is an integer between 1 and 65535
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

#### Default value

The default cost for the OSPFv3 protocol running on the interface is obtained based on the rate of the port.

**Command mode**

Interface configuration mode

**Example**

The following example shows how to set the cost for the OSPFv3 protocol running on interface vlan1 to 2:

```
interface vlan 1
ipv6 ospf cost 2
```

**Related command**

None

**58.1.19 ipv6 ospf database-filter all out**

To designate an interface to filter those to-be-transmitted LSA, run the first one of the following two commands:

```
ipv6 ospf database-filter all out [instance instance-id]
no ipv6 ospf database-filter all out [instance instance-id]
```

**Parameter**

parameter	Description
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

**Default value**

The interface does not filter those to-be-transmitted LSAs.

**Command mode**

Interface configuration mode

**Example**

The following example shows how to set interface vlan 1 to filter those to-be-transmitted LSAs:

```
interface vlan 1
ipv6 ospf database-filter all out
```

**Related command**

None

**58.1.20 ipv6 ospf dead-interval**

To designate the dead interval of the neighboring router, run **ipv6 ospf dead-interval seconds**. To resume the default value, run **ipv6 ospf dead-interval**.

```
ipv6 ospf dead-interval seconds [instance instance-id]
```

**ipv6 ospf dead-interval** seconds [instance instance-id]

#### Parameter

parameter	Description
<i>seconds</i>	Value of the dead interval for the neighboring router, which ranges from 1 to 2147483647 seconds
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

#### Default value

The dead interval for the neighboring router is four times of hello-interval by default.

#### Command mode

Interface configuration mode

#### Instruction

The value of the dead-interval parameter will be written to the HELLO packet and will be transmitted along with the HELLO packet. It must be ensured that the dead-interval parameter must be identical with that between the neighboring routers and the value of the dead-interval parameter must be four times of the value of the hello-interval parameter.

#### Example

The following example shows how to set the dead interval of the neighboring router on interface vlan1 to 60 seconds.

```
interface vlan 1
```

```
ipv6 ospf dead-interval 60
```

#### Related command

None

### 58.1.21 ipv6 ospf hello-interval

To designate the interval for transmitting the HELLO packet on the interface, run **ipv6 ospf hello-interval seconds**. To resume the default settings, run **no ipv6 ospf hello-interval**.

**ipv6 ospf hello-interval** seconds [instance instance-id]

**no ipv6 ospf hello-interval** seconds [instance instance-id]

#### Parameter

parameter	Description
<i>seconds</i>	Transmission interval of the HELLO packet, ranging from 1 to 65535 seconds
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

#### Default value

The interval for the P2P or Broadcast interface to send Hello packets is 10 seconds, while the interval for the P2MP or NBMA interface to send Hello packets is 30 seconds.

### Command mode

Interface configuration mode

### Instruction

The value of the dead-interval parameter will be written to the HELLO packet and will be transmitted along with the HELLO packet. The smaller the hello-interval is, the sooner the change of the network topology will be found. However, much more path cost will be paid. It must be ensured that the parameter must be identical with that between the neighboring routers.

### Example

The following example shows that the interval for transmitting the HELLO packet on interface vlan1 is set to 20 seconds.

```
interface vlan 1
ipv6 ospf hello-interval 20
```

### Related command

**ipv6 ospf dead-interval**

#### 58.1.22 *ipv6 ospf mtu-ignore*

To set the MTU value of the transmitted DD packet to 0 on an interface and meanwhile omit the checkup of the MTU domain of the received DD packet, run the first one of the following two commands:

```
ipv6 ospf mtu-ignore [instance instance-id]
no ipv6 ospf mtu-ignore [instance instance-id]
```

### Parameter

parameter	Description
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

### Default value

The value of the MTU domain of the DD packet is set to be the MTU value of this interface and MTU checkup is not omitted.

### Command mode

Interface configuration mode

### Instruction

OSPF judges whether the MTU value of the network segment, where an interface belongs, is consistent by checking the MTU value of the exchanged DD packet. If the MTU value of the

received DD packet is bigger than the MTU value of this interface, the OSPF neighborhood cannot be set up.

### Example

The following example shows how to set interface vlan1 to omit MTU checkup.

```
interface vlan 1
ipv6 ospf mtu-ignore
```

### Related command

None

### 58.1.23 *ipv6 ospf neighbor*

To set the OSPF neighbor on the non-broadcast network interface, run the first one of the following two commands:

```
ipv6 ospf neighbor router-id ipv6-address [cost number] [database-filter all out] [poll-interval seconds] [priority number] [instance instance-id]
```

```
no ipv6 ospf neighbor router-id ipv6-address [cost number] [database-filter all out] [poll-interval seconds] [priority number] [instance instance-id]
```

### Parameter

parameter	Description
<i>router-id</i>	Means the router ID of a neighbor.
<i>ipv6-address</i>	Means the local address of the neighbor's link.
<i>cost number</i>	Means the neighbor's cost, whose value ranges from 1 to 65535.
<i>database-filter all out</i>	Filters the transmitted LSAs.
<i>poll-interval seconds</i>	Means the query interval of a neighbor.
<i>priority number</i>	Means the neighbor's priority, whose value ranges from 0 to 255.
<i>instance instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

### Default value

No neighbors are set.

### Command mode

Interface configuration mode

### Instruction

You shall specify a neighbor manually on the non-broadcast network. If neighbors invalidates, the Hello packet should be sent to this neighbor in poll interval.

### Example



The following example shows how to set the neighbor of interface vlan1.

```
interface vlan 1
ipv6 ospf neighbor 1.1.1.1 fe80::1
```

#### Related command

None

#### 58.1.24 ipv6 ospf network

To set the network type for the interface, run the first one of the following two commands.

```
ipv6 ospf network { broadcast | non-broadcast | point_to_multipoint | point-to-point} [instance instance-id]
```

```
no ip ospf network { broadcast | nonbroadcast | point_to_multipoint | point-to-point} [instance instance-id]
```

#### Parameter

parameter	Description
<i>broadcast</i>	Sets the network type of the interface to broadcast.
<i>nonbroadcast</i>	Sets the network type of the interface to NBMA.
<i>point-to-multipoint</i>	Sets the network type of the interface to point-to-multipoint.
<i>point-to-point</i>	Sets the network type of the interface to point-to-point.
<i>instance instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.
<i>priority number</i>	Means the neighbor's priority, whose value ranges from 0 to 255.
<i>instance instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

#### Command mode

Interface configuration mode

#### Instruction

The interface in the broadcast network without multi-address access should be set to NBMA. In the NBMA network, the network should be set to point-to-multipoint if any two routers cannot be ensured to be directly reachable.

#### Example

The following example shows how to set interface vlan1 to NBMA.

```
interface vlan 1
ipv6 ospf network non-broadcast
```

#### Related command

None

### 58.1.25 *ipv6 ospf priority*

To configure the priority for the interface to choose the router, run **ipv6 ospf priority priority**. To resume the default value, run **no ipv6 ospf priority**.

```
ipv6 ospf priority priority [instance instance-id]
```

```
no ipv6 ospf priority [instance instance-id]
```

Parameter

parameter	Description
<i>priority</i>	Priority to choose the router, ranging between 0 and 255
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

Default value

The default priority for the interface to choose the routers is 1.

Command mode

Interface configuration mode

Instruction

When two routers in the same network segment want to be the selection router, the router with higher priority will be selected. If the priority of the two routers is the same, the router with a larger ID is selected. When the priority of a router is 0, the router cannot be selected as the designated router or the standby designated router. The priority is effective only on the networks except the nonpoint-to-point network.

Example

The following example shows how to set the priority to 8 when interface vlan1 selects the selection router.

```
interface vlan 1
ipv6 ospf priority 8
```

Related command

None

### 58.1.26 *ipv6 ospf retransmit-interval*

To designate the retransmission interval for transmitting LSA between the interface and the neighboring router, run **ipv6 ospf retransmit-interval seconds**. To resume the default value, run **no ipv6 ospf retransmit-interval**.

```
ipv6 ospf retransmit-interval seconds [instance instance-id]
```

```
no ipv6 ospf retransmit-interval seconds [instance instance-id]
```

Parameter

parameter	Description
<i>seconds</i>	Transmission interval for transmitting the link state broadcast between the interface and the neighboring router, ranging between 1 and 3600 seconds
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

### Default value

The default interval for transmitting the link state broadcast between the interface and the neighboring router is 5 seconds.

### Command mode

Interface configuration mode

### Instruction

When a router transmits the link-state broadcast to its neighbor, the command will maintain the link-state broadcast until the peer receives the acknowledgement. If the link-state broadcast is not received during the transmission interval, it will be retransmitted. The value of the seconds parameter must be larger than the round-trip time for a packet transmitting between two routers.

### Example

The following example shows how the default interval for transmitting the link-state broadcast between interface vlan1 and the neighboring router is set to 8 seconds.

```
interface vlan 1
ipv6 ospf retransmit-interval 8
```

### Related command

None

### 58.1.27 ipv6 ospf transmit-delay

To set the delay for the link-state broadcast to be transmitted on the interface, run **ipv6 ospf transit-delay time**. To resume the default value, run **no ipv6 ospf transit-delay**.

```
ipv6 ospf transit-delay time [instance instance-id]
```

```
no ipv6 ospf transit-delay time [instance instance-id]
```

### Parameter

parameter	Description
<i>time</i>	Means the delay of link state broadcast transmission on an interface, which ranges from 1 to 3600 seconds.
<i>instance-id</i>	Specifies the OSPF instance ID of the interface, whose default value is 0.

### Default value

The default delay for the link-state broadcast to be transmitted on the interface is 1 second.

### Command mode

Interface configuration mode

### Example

The following example shows how to set the delay for transmitting the link-state broadcast on interface vlan1 to 3 seconds.

```
interface vlan 1
```

```
ipv6 ospf transit-delay 3
```

### Related command

None

### 58.1.28 passive-interface

To forbid a designated interface to transmit or receive the OSPFv3 packets, run the first one of the following two commands:

```
passive-interface { interface-type interface-number | all }
```

```
no passive -interface { interface-type interface-number | all }
```

### Parameter

parameter	Description
<i>interface-type</i> <i>interface-number</i>	<b>Means the interface type and the interface ID.</b>
<i>all</i>	<b>Means all interfaces.</b>

### Default value

The interface is allowed to transmit or receive the OSPFv3 packets.

### Command mode

Routing configuration mode

### Instruction

Different processes can forbid a same interface to transmit or receive the OSPFv3 packets, but the passive-interface command takes effect only on the OSPFv3 interface.

### Example

The following example shows how to forbid interface vlan1 to receive and transmit the OSPFv3 packets in the OSPFv3 process.

```
router ospfv3 100
```

```
passive -interface vlan 1
```

### Related command

None

### 58.1.29 redistribute

To configure the route where OSPF forwards other routing protocols, run **redistribute**. To resume the default settings, run **no redistribute**.

**redistribute** *protocol* [*as-number*] [*route-map map-tag*]

**no redistribute** *protocol* [*as-number*] [*route-map map-tag*]

Parameter

parameter	Description
<i>protocol</i>	Means to forward the learned original protocol.
<i>as_number</i>	Means the number of the autonomous system which is not for the connect, rip or static parameter.
<i>map-tag</i>	Means the name of the route map.

Default value

Not forward

Command mode

Routing configuration mode

Instruction

None

Example

The following example shows how to forward the static route in OSPF process 1:

```
interface vlan 1
ipv6 enable
ipv6 ospf 1 area 0
!
router ospfv3 1
router-id 2.2.2.2
redistribute static
```

### 58.1.30 router ospfv3

To enable OSPFv3 and enter the OSPFv3 configuration view, run the first one of the following two commands:

**router ospfv3** *process-id*

**no router ospfv3** *process-id*

## Parameter

parameter	Description
<i>process-id</i>	<b>Identifies the OSPF process. It is a positive integer distributed by the local router.</b>

## Default value

None

## Command mode

Global configuration mode

## Instruction

One router may have multiple OSPFv3 processes.

## Example

The following example shows how to set an OSPFv3 process, whose process ID is 109:

```
router ospfv3 109
```

## Related command

**ipv6 ospf area**

**58.1.31 router-id**

To set the router ID in the autonomous system for the router on which the OSPFv3 protocol is running, run the first one of the following two commands:

**router-id *router-id***

**no router-id *router-id***

## Parameter

parameter	Description
<i>router-id</i>	<b>Means the identifier of the router, which is in the IPv4 address format.</b>

## Default value

If an IPv4 address has already configured on a router before OSPFv3 is enabled, the router will automatically choose an IPv4 address as its ID.

## Command mode

Routing configuration mode

## Instruction

The router ID is the unique identifier of a OSPFv3-running router in the autonomous system, so the router IDs of two routers in the autonomous system are different. If a router has no router ID, the OSPFv3 process cannot go on.

## Example

The following example shows how to set the router ID of OSPFv3 process 1 to 2.2.2.2:

```
router ospfv3 1
router-id 2.2.2.2
```

### 58.1.32 show ipv6 ospf

To display the main OSPFv3 information, run the following command:

```
show ipv6 ospf [process-id]
```

#### Parameter

parameter	Description
<i>process-id</i>	Means the OSPF process ID.

#### Default value

None

#### Command mode

EXEC

#### Instruction

The information exported by the command can help checking the OSPFv3 faults. If the process-id parameter follows the command, the information about the global configuration of the OSPFv3 process is displayed.

## Example

The following example shows that the configuration information about all OSPFv3 processes will be displayed.

```
router# show ipv6 ospf
```

```
Routing Process "OSPFv3 0" with ID 1.2.3.4
```

```
SPF schedule delay 5 secs, Hold time between SPFs 10 secs Minimum LSA interval 5 secs,
```

```
Minimum LSA arrival 1 secs Number of external LSA 3. Checksum Sum 0x2CD6F
```

```
Number of areas in this router is 1 Area BACKBONE(0)
```

```
Number of interfaces in this area is 1
```

```
SPF algorithm executed 3 times
```

```
Number of LSA 4. Checksum Sum 0x2A6AC
```

```
router#
```

Relative fields are explained in the following table:

Domain	Description
--------	-------------

<i>Routing Process "OSPFv3 0"</i>	<b>ID of the process</b>
<i>with ID 1.2.3.4</i>	<b>ID of the router</b>
<i>SPF schedule delay 5 secs, Hold time between two SPF's 10 secs</i>	<b>Two timer values relative with OSPF</b>
<i>Number of areas is 1</i>	<b>Number of the currently-configured fields, and parameters configured in each field</b>
<i>Number of LSA 4</i>	<b>Quantity of LSAs in the database</b>
<i>Number of external LSA 3</i>	<b>Quantity of ASE LSAs in the database</b>
<i>SPF algorithm executed 3 times</i>	<b>SPF algorithm execution statistics</b>

### 58.1.33 show ipv6 ospf database

To display the database information about the OSPFv3 connection state, run the following command:

```
show ipv6 ospf database { router | network | inter-prefix | inter-router | external | link | intra-prefix } [ ADVROUTER ]
```

#### Parameter

<b>Parameter</b>	<b>Description</b>
<i>router</i>	<b>Means the LSA type is the router.</b>
<i>network</i>	<b>Means the LSA type is the network.</b>
<i>inter-prefix</i>	<b>Means the LSA type is the inter-domain route.</b>
<i>inter-router</i>	<b>Means the LSA type is the inter-domain router.</b>
<i>external</i>	<b>Means the LSA type is the exterior route.</b>
<i>link</i>	<b>Means the LSA type is the link.</b>
<i>intra-prefix</i>	<b>Means the LSA type is the inside-domain route.</b>
<i>ADVROUTER</i>	<b>Means to declare the router ID.</b>

#### Default value

None

#### Command mode

EXEC

#### Instruction

The information exported by the command can help to check the database information about the OSPFv3 connection state and to find the reason of the faults.

#### Example

```
router#
```



```

router#show ipv6 ospf database

Link-LSA (Interface eth0)

Link State ID ADV Router Age Seq# CkSum Prefix
0.0.0.3 1.2.3.4 104 0x80000004 0x889e 0
0.0.0.5 5.6.7.8 142 0x80000003 0xab70 2

Router-LSA (Area 0.0.0.0)

Link State ID ADV Router Age Seq# CkSum Link
0.0.0.1 1.2.3.4 94 0x80000014 0xaea 1
0.0.0.1 5.6.7.8 105 0x80000019 0x8a32 1

Network-LSA (Area 0.0.0.0)

Link State ID ADV Router Age Seq# CkSum
0.0.0.5 5.6.7.8 105 0x80000001 0xa441

Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID ADV Router Age Seq# CkSum Prefix Reference
0.0.0.1 5.6.7.8 104 0x80000001 0x8d4f 2 Network-LSA

AS-external-LSA

Link State ID ADV Router Age Seq# CkSum
0.0.0.1 5.6.7.8 1229 0x80000002 0xe92d
0.0.0.2 5.6.7.8 1229 0x80000002 0xef25
0.0.0.3 5.6.7.8 1229 0x80000002 0xf51d

router#

```

Relative fields are explained in the following table:

Domain	Description
<i>AREA: 1</i>	<b>Current area</b>
<i>Router Link States/Net Link States/Summary Net Link States</i>	<b>LSA type</b>
<i>Link ID</i>	<b>LSA ID</b>
<i>ADV Router</i>	<b>Releases the router.</b>
<i>Age</i>	<b>Releases the age.</b>
<i>Seq #</i>	<b>Generates the sequence ID.</b>
<i>Checksum</i>	<b>Means the checksum.</b>

### 58.1.34 show ipv6 ospf interface

To display the information about the OSPFv3 interface, run the following command:

```
show ipv6 ospf interface [ type ] [ index ]
```

Parameter

Parameter	Description
<i>type</i>	Port type
<i>index</i>	Port number

Default value

None

Command mode

EXEC

Instruction

According to the information displayed by the command, you can check the OSPFv3 configuration and its running state, which helps you to detect the OSPFv3 faults.

Example

```
router#show ipv6 ospf interface
ethernet0/1 is up, line protocol is up
Interface ID 3, Instance ID 0, Area 0.0.0.0
IPv6 Link-Local Address fe80::248:54ff:fec0:f32d/10
Router ID 1.2.3.4, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State Backup, Priority 1
Designated Router (ID) 5.6.7.8
Interface Address fe80::203:47ff:fe4c:776e
Backup Designated Router (ID) 1.2.3.4
Interface Address fe80::248:54ff:fec0:f32d
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Neighbor Count is 1, Adjacent neighbor count is 1
router#
```

Relative fields are explained in the following table:

Domain	Description
--------	-------------

<i>IPv6 Link-Local Address</i>	<b>Address of port IPv6 link-local</b>
<i>Nettype</i>	<b>Network type of the OSPF interface</b>
<i>OSPF process is</i>	<b>ID of the OSPF process</b>
<i>AREA</i>	<b>Current area</b>
<i>Router ID</i>	<b>ID of the router where the process belongs</b>
<i>Cost</i>	<b>Cost of the OSPF interface of the router</b>
<i>Transmit Delay is</i>	<b>Transmission delay</b>
<i>Priority</i>	<b>Priority for the interface of the router</b>
<i>Hello interval</i>	<b>Transmission interval of the Hello packet</b>
<i>Dead timer</i>	<b>Dead time</b>
<i>Retransmit</i>	<b>Retransmission interval</b>
<i>OSPF INTF State is</i>	<b>State of the OSPF port</b>
<i>Designated Router id</i>	<b>ID of the designated router and the IP address of its port</b>
<i>Backup Designated router id</i>	<b>ID of the backup designated router and the IP address of its port</b>
<i>Neighbor Count is</i>	<b>Number of the neighboring routers</b>
<i>Adjacent neighbor count is</i>	<b>Number of neighbors that have established the neighborhood relation</b>
<i>Adjacent with neighbor</i>	<b>Neighbor lists that have established the neighborhood relation</b>

### 58.1.35 show ipv6 ospf neighbor

To display the information about OSPFv3 neighbor, run the following command.

**show ipv6 ospf neighbor [interface\_type interface\_number | router-id | detail]**

Parameter

<b>Parameter</b>	<b>Description</b>
<i>interface_type</i>	<b>Port type</b>
<i>interface_number</i>	<b>Port number</b>
<i>router-id</i>	<b>Router ID</b>
<i>detail</i>	<b>Displays the detailed information.</b>

Default value

None

Command mode

EXEC

Instruction

The information displayed by the command can help you to check whether the OSPFv3 neighbor configuration is right and to detect the OSPFv3 faults.

### Example

```
router#show ipv6 ospf neighbor
OSPFv3 Process 1
Area 1
Neighbor ID Pri State Dead Time Interface Instance ID
5.6.7.8 1 Full/DR 00:00:38 eth0 0
```

Relative fields are explained in the following table:

Domain	Description
<i>OSPFv3 process</i>	<b>ID of the OSPF process</b>
<i>AREA</i>	<b>Local area</b>
<i>Neighbor</i>	<b>ID of a neighbor</b>
<i>Pri</i>	<b>Priority of a neighbor</b>
<i>State</i>	<b>Connection state related with the neighbor</b>
<i>DeadTime</i>	<b>Time of neighbor invalidation</b>
<i>Address</i>	<b>IP address of the neighbor</b>
<i>Interface</i>	<b>Interface used by a router to reach its neighbor</b>

### 58.1.36 show ipv6 ospf route

To display the information about the OSPFv3 routing table, run the following command:

```
show ipv6 ospf route
```

#### Parameter

None

#### Default value

None

#### Command mode

EXEC

#### Instruction

The information displayed by the command can help you browse the OSPFv3 routing table and confirm whether the OSPFv3 trouble diagnosis is correctly carried out.

### Example

```
router#show ipv6 ospf route
```

Destination Metric

Next-hop Interface

3ffe:1:1::/48 10

-- eth0

3ffe:2:1::/48 10

-- eth0

3ffe:2:2::/48 10

-- eth0

3ffe:3:1::/48 10

-- eth0

3ffe:3:2::/48 10

-- eth0

3ffe:3:3::/48 10

-- eth0

E2 3ffe:100:1::1/128 10/20

fe80::203:47ff:fe4c:776e eth0

E2 3ffe:100:2::1/128 10/20

fe80::203:47ff:fe4c:776e eth0

E2 3ffe:100:3::1/128 10/20

fe80::203:47ff:fe4c:776e eth0

IA 3ffe:101:1::/48 20

fe80::203:47ff:fe4c:776e eth0

IA 3ffe:101:2::/48 20

fe80::203:47ff:fe4c:776e eth0

IA 3ffe:101:3::/48 20

fe80::203:47ff:fe4c:776e eth0

Relative fields are explained in the following table:

Domain	Description
<i>Destination</i>	<b>Destination network segment</b>
<i>Metric</i>	<b>Cost of a route</b>
<i>Next-hop</i>	<b>Address of the next hop</b>
<i>Interface</i>	<b>Interface of the next hop</b>

### 58.1.37 show ipv6 ospf virtual-link

To display the information about the OSPFv3 virtual link, run the following command:

```
show ipv6 ospf virtual-link
```

#### Parameter

None

#### Default value

None

#### Command mode

EXEC

#### Instruction

According to the information exported by the command, you can check the state of the OSPFv3 virtual link.

You can run **show ipv6 ospf neighbor** to check the detailed information about the adjacent neighbor.

#### Example

```
router#show ipv6 ospf virtual-link
```

```
Virtual Link VLINK1 to router 5.6.7.8 is up
```

```
Transit area 0.0.0.1 via interface eth0, instance ID 0
```

```
Local address 3ffe:1234:1::1/128
```

```
Remote address 3ffe:5678:3::1/128
```

```
Transmit Delay is 1 sec, State Point-To-Point,
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Hello due in 00:00:01
```

```
Adjacency state Up
```

Relative fields are explained in the following table:

Domain	Description
<i>neighbor ID</i>	Neighbor ID of the peer
邻居状态	Neighborhood state for the neighbor
<i>TransArea</i>	Transmission area
<i>cost</i>	Minimum cost for reaching the peer in the transmission area If the value of the cost is 0, it means that the peer is unreachable.

<i>Hello Interval</i>	<b>Current transmission interval for the Hello packet</b>
<i>DeadTime</i>	<b>Time of neighbor invalidation</b>
<i>Retrans</i>	<b>Retransmission interval</b>
<i>Adjacency state</i>	<b>State of the virtual link interface</b>

#### Related command

**area virtual-link**

**show ipv6 ospf neighbor**

#### 58.1.38 summary-prefix

To configure the address for OSPFv3 to create the route aggregation, run **summary-prefix**. To cancel the address of route aggregation, run **no summary-prefix**.

**summary-prefix** *ipv6-prefix /prefix-length*

**no summary-prefix** *ipv6-prefix /prefix-length*

#### Parameter

<b>Parameter</b>	<b>Description</b>
<i>ipv6-prefix</i>	<b>Aggregation address with the designated address range</b>
<i>prefix-length</i>	<b>Subnet mask of the aggregation route</b>

#### Default value

None

#### Command mode

Routing configuration mode

#### Instruction

Multiple groups of addresses are summarized. Routes learned from other routing protocols can also be summarized. After the aggregation, all covered networks cannot be transmitted to other routing fields. The cost of the summary route is the minimum value among the cost values of all summary routes. The command cannot be used to reduce the size of the routing table.

The command is used by OSPFv3 to enable the ASBR to notify an external route of being an aggregation route to replace all external routes. The command is only used to aggregate the OSPFv3 routes of other routing protocols. You can run **area range** in OSPFv3 to summarize the routes.

#### Example

In the following example, the summary address 2001::/64 stands for addresses such as 2001::/80, 2001::1/64 and so on, and only address 2001::/64 is broadcasted.

```
summary-address 2001::/64
```

### Related command

**area range**

### 58.1.39 timers delay

To designate a delay interval between OSPF receiving a topology change and starting a shortest path priority calculation, run `timers delay spf-delay`. To resume the default settings, run `no timers delay`.

**timers delay** *spf-delay*

**no timers delay**

### Parameter

Parameter	Description
<i>spf-delay</i>	Delay between the topology change and calculation start. Its default value is 5 seconds. If the value is 0, there is no delay. That is, the calculation will be promptly started if changes occur.

### Default value

`spf-delay: 5 seconds`

### Command mode

Routing configuration mode

### Instruction

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time.

### Example

The following example shows how to set the time for OSPF to start calculating the delay is 10 seconds.

```
timers delay 10
```

### 58.1.40 timers hold

To set the interval between two continuous SPF calculations, run `timers hold`. To resume the default settings, run `no timers hold`.

**timers hold** *spf-holdtime*

**no timers hold**

### Parameter

Parameter	Description
<i>spf-holdtime</i>	Minimum value between two continuous calculations



	It ranges between 0 to 65535 seconds. Its default value is 10 seconds; when it is 0, there is no interval between the two continuous calculations.
--	--

### Default value

spf-holdtime: 10 seconds

### Command mode

Routing configuration mode

### Instruction

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time.

### Example

The following example shows how to set the interval between two successive SPF calculations to 20 seconds:

```
timers hold 20
```

## Chapter 59 BFD Configuration Commands affects ONLY PXT-S2790G/2795G or Higher

BFD configuration commands are shown as follows:

- bfd init-mode
- bfd slow-timers
- bfd demand enable
- bfd echo enable
- bfd enable
- bfd neighbor
- bfd min\_echo\_rx\_interval
- bfd authentication-mode
- show bfd

### 59.1.1 bfd init-mode

To enable the initial BFD mode, run the following command:

```
bfd init-mode [active | passive]
```

```
no bfd init-mode
```

### Parameter

Parameter	Description
-----------	-------------

<i>active</i>	Means that the BFD neighbor sends the control packets actively to establish the BFD connection.
<i>passive</i>	Means that the BFD neighbor won't send any BFD packets when BFD neighbor is down.

#### Default value

The value of the **init-mode** parameter is **active**.

#### Command mode

Global configuration mode

#### Explanation

The BFD connection requires one terminal to be active in its initial mode, or the BFD connection cannot be set up.

#### Example

The following example shows how to set the BFD mode of local system to passive.

```
Switch#
```

```
Switch#conf
```

```
Switch_config#bfd init-mode passive
```

#### Related command

#### **bfd slow-timers**

#### 59.1.2 *bfd slow-timers*

To set the slow timer of BFD, run **bfd slow-timers**; to resume the default settings, run **no bfd slow-timers**.

```
bfd slow-timers <value>
```

```
no bfd slow-timers
```

#### Parameter

Parameter	Description
<i>value</i>	It ranges between 1000ms and 30000ms.

#### Default value

The default value of slow-timers is 1.

#### Command mode

Global configuration mode

#### Explanation

This command is used to set the BFD slow-timers, which is 1 second by default. The BFD neighbor transmits control packets at an interval of this configured time before it is up. This is mainly to prevent those not-up sessions from consuming too much bandwidth.

When the echo function is activated, echo packets are responsible for conducting real connectivity checkup. Hence, BFD control packets are not frequently forwarded and the system takes this configured slow-timers as the interval for transmitting control packets.

### Example

The following example shows how to set the slow-timers of BFD to 2 seconds:

```
Switch#  
Switch#conf  
Switch_config#bfd slow-timers 2000
```

### Related command

#### **bfd init-mode**

#### *59.1.3 bfd demand enable*

To activate the BFD query mode, run **bfd demand enable**; to disable the BFD query mode, run **no bfd demand enable**.

#### **bfd demand enable**

#### **no bfd demand enable**

#### Parameter

N/A

#### Default value

The BFD query mode is not activated by default.

#### Command mode

Interface configuration mode

#### Explanation

In query mode, we suppose that each system has an independent method to confirm its connection with other systems. Once a BFD session is conducted, the system stops transmitting BFD control packets unless a certain system requires explicit connectivity checkup. In a system where explicit connectivity checkup is required, the system transmits short-sequence BFD control packets and claims the session is down if it doesn't receive the response packets in the checkup period.

### Example

The following example shows how to enable the VLAN1 BFD query mode.

```
Switch_config#  
Switch_config# interface vlan 1
```

```
Switch_config_v1#bfd enable
```

```
Switch_config_v1#bfd demand enable
```

Related command

**bfd enable**

#### 59.1.4 bfd echo enable

To activate BFD echo, run **bfd echo enable**; to disable BFD echo, run **no bfd echo enable**.

```
bfd echo enable <cr>|<number>
```

**no bfd echo enable**

Parameter

Parameter	Description
<i>number</i>	Stands for the allowable maximum number of dropped echo packets, which is 3 by default and ranges from 3 to 10.

Default value

The BFD echo is not activated by default.

Command mode

Interface configuration mode

Explanation

After BDF echo is activated, connectivity checkup is conducted by the echo packets.

Example

The following example shows how to activate VLAN1 BFD echo and set the allowable maximum number of echo packet losses to 4.

```
Switch_config#
```

```
Switch_config#int vlan1
```

```
Switch_config_v1#bfd enable
```

```
Switch_config_v1#bfd echo enable 4
```

Related command

**bfd enable**

**bfd min\_echo\_rx\_interval**

#### 59.1.5 bfd enable

To activate BFD on a port, run **bfd enable**; to disable BFD on a port, run **no bfd enable**.

```
bfd enable <cr> | [min_tx_interval <tx_value> min_rx_interval <rx_value>
```

**multiplier** *<m\_value>*]

**no bfd enable**

Parameter

Parameter	Description
<i>tx_value</i>	Sets the minimum interval of transmitting control packets, which ranges from 10ms to 999ms and the default value of which is 50ms.
<i>rx_value</i>	Sets the minimum interval of receiving control packets, which ranges from 10ms to 999ms and the default value of which is 50ms.
<i>m_value</i>	Sets the checkup coefficient of BFD control packets, which ranges from 3 to 50 and the default value of which is 3.

Default value

The BFD function is not activated on ports.

Command mode

Interface configuration mode

Explanation

The precondition for activating BFD on a port is that the IP address of this port must exist.

Note:

Both **min\_tx\_interval** and **min\_rx\_interval** are used as references for the local BFD and the peer BFD. They are not real intervals of packet reception and transmission. The multiplier has no role in the local BFD, but is used for the peer BFD to calculate the checkup time.

Example

The following example shows how to enable VLAN1 BFD, set the minimum intervals of both transmitting and receiving control packets to **80ms** and the checkup coefficient to **5**.

```
Switch_config#
```

```
Switch_config#int vlan1
```

```
Switch_config_v1#bfd enable min_tx 80 min_rx 80 multi 5
```

Related command

**ip address**

### 59.1.6 bfd neighbor

To set the static BFD neighbor, run **bfd neighbor**; to delete the static BFD neighbor, run **no bfd neighbor**.

```
bfd neighbor <ip-add>
```

```
no bfd neighbor <ip-add>
```

## Parameter

Parameter	Description
<i>ip-add</i>	Stands for the to-be-configured IP address.

## Default value

No static BFD neighbor exists on the port.

## Command mode

Interface configuration mode

## Explanation

BFD is a two-way checkup protocol. If it is used to check the unidirectional paths such as static route, a problem may arise that no BFD neighbor exists on the peer end. Hence you have to use this command to set a static neighbor. Of course, you can solve this problem through dynamic protocol.

## Example

The following example shows how to set static BFD 172.16.1.100 on interface vlan1.

```
Switch_config#
Switch_config#int vlan1
Switch_config_v1#bfd enable
Switch_config_v1#bfd neighbor 172.16.1.100
```

## Related command

**bfd enable****59.1.7 bfd min\_echo\_rx\_interval**

To set the minimum interval of receiving BFD echo packets, run **bfd min\_echo\_rx\_interval**; to resume the default settings, run **no bfd min\_echo\_rx\_interval**.

**bfd min\_echo\_rx\_interval** <value>

**no bfd min\_echo\_rx\_interval**

## Parameter

Parameter	Description
<i>value</i>	<10-999>, unit: millisecond

## Default value

The default value of **min\_echo\_rx\_interval** is 50ms.

## Command mode

Interface configuration mode

### Explanation

This command is used to set the minimum interval of receiving BFD echo packets. Because echo packets are locally transmitted and locally received, the echo packet transmission interval in the local system is also set via this command.

### Example

The following example shows how to activate BFD echo on interface vlan1 and set the minimum interval of receiving BFD echo packets to 80ms.

```
Switch_config#
Switch_config#int vlan1
Switch_config_v1#bfd enable
Switch_config_v1#bfd echo enable
Switch_config_v1#bfd min_echo_rx_interval 80
```

### Related command

**bfd enable**

**bfd echo enable**

#### 59.1.8 bfd authentication-mode

To set the authentication of BFD packets, run **bfd authentication-mode**; to disable the authentication of BFD packets, run **no authentication-mode**.

**bfd authentication-mode** [*md5* | *meticulous md5* | *simple* ] <key id> <key>

**no bfd authentication-mode**

### Parameter

Parameter	Description
<i>md5</i>	<b>MD5 authentication</b>
<i>meticulous md5</i>	<b>Securer MD5 authentication</b>
<i>simple</i>	<b>Simple password authentication</b>
<i>key id</i>	<b>Authentication ID</b>
<i>key</i>	<b>Authentication password (up to 16 characters)</b>

### Default value

The authentication function is not enabled.

### Command mode

Interface configuration mode

### Explanation

After BFD authentication is configured, BFD will transmit control packets with the authentication field. Normal link checkup can be performed only when two BFD terminals have the same authentication configuration.

Note: Those BFD neighbors in UP state are not subject to authentication changes.

### Example

The following example shows how to enable BFD MD5 authentication on interface VLAN1:

```
Switch_config#  
Switch_config#int vlan1  
Switch_config_v1#bfd enable  
Switch_config_v1#bfd authentication-mode md5 1
```

### Related command

**bfd enable**

#### 59.1.9 show bfd

To display the BFD-related information, run the following command:

```
show bfd interfaces [details] | neighbors [details]
```

### Parameter

N/A

### Default value

### Command mode

Global configuration mode

### Explanation

This command is used to set the BFD-related information.

### Example

N/A

### Related command

**bfd enable**

**bfd neighbor**



## Chapter 60 IP Hardware Subnet Routing Configuration Commands

### 60.1 *ip exf*

Syntax	Default value
[no] <i>ip exf</i>	N/A
Parameter	Command mode
N/A	Global configuration mode

#### Remarks

The IP hardware subnet routing function can be enabled through this command. If this function is not enabled, the hardware forwarding items can still be configured but they invalidate.

#### Example

The following example shows how to enable the IP hardware subnet route.

```
Switch_config#ip exf
```

### 60.2 *ip exf down-up-threshold*

#### Syntax

***ip exf down-up-threshold rate***

***no ip exf down-up-threshold***

#### Parameter

Name	Remarks
<i>down-up-threshold rate</i>	<b>Stands for the trigger value (percent) of hardware subnet routing switch.</b>

#### Default value

90

#### Command mode

Global configuration mode

#### Remarks

When the number of software routes exceeds the trigger value of hardware subnet routing, the hardware subnet routing will be shut down; when the number of software routes lowers to be less than the trigger value, the hardware subnet routing will be opened again.

#### Example

The following example shows how to enable the hardware subnet routing on a L3 switch and set the trigger value to 80%.

```
ip exf down-up-threshold 80
```

### 60.3 *debug ip exf*

Syntax	Default value
<code>[no] debug ip exf</code>	N/A
Parameter	Command mode
N/A	EXEC

#### Remarks

It is used to enable or disable the debugging switch of IP EXF.

#### Example

The following are common examples of debugging information output.

```
2004-7-30 15:50:40 [EXF]: EXF entry(destination 2.10.0.0/16) delete from hardware table, EXF disabled
```

It means that user enters the **no ip exf** command and all **exf** items invalidate.

```
2004-7-30 15:50:44 [EXF]: EXF entry(destination 2.10.0.0/16) add to hardware, NAT enabled, nexthop CPU
```

It means that the NAT function is enabled at the port where the next hop of the configured **exf** item belongs. In this case, the packet of the **exf** item is transmitted to CPU for processing.

```
2004-7-30 15:52:03 [EXF]: EXF entry(destination 2.9.0.0/16) add to hardware, no ARP, nexthop CPU
```

It means that the ARP of the IP address of the next hop of the configured **exf** item is not learned. In this case, the packet of the **exf** item is transmitted to CPU for processing.

```
2004-7-30 15:50:44 [EXF]: EXF entry(destination 2.3.0.0/16) add to hardware sucessfully
```

It means that the EXF entry is configured successfully.

```
2004-7-30 15:56:00 [EXF]: EXF entry(destination 2.2.0.0/16) delete from hardware table by command
```

It means that the EXF entry is deleted through the corresponding command.

```
2004-7-30 15:56:59 [EXF]: EXF entry(destination 2.3.0.0/16) delete from hardware table, delete by interface
```

It means that the interface for the next hop of the configured EXF entry is down or the EXF entry becomes invalid because of NAT settings.

## Chapter 61 IP-PBR Configuration Commands affects ONLY PXT-S2790G/2795G or Higher

IP-PBR configuration commands include:

- `ip pbr`
- `show ip pbr`
- `show ip pbr policy`
- `show ip pbr exf`
- `debug ip pbr`

### 61.1.1 *ip pbr*

Description

**ip pbr**

**no ip pbr**

Parameter

None

Default value

The IP-PBR function is disabled by default.

Description

It is used to enable or disable the IP-PBR function. The **no ip pbr** command is used to resume the default value.

Example

```
switch(config)# ip pbr
```

```
switch(config)#
```

### 61.1.2 *show ip pbr*

Description

**show ip pbr**

Parameter

Default value

None

None

Description

It is used to display the information about RIP configuration.

Example

The following example shows how to display the information about IP-PBR running.

```
switch(config)# show ip pbr
IP policy based route state: enabled
No equiv exf apply item
VLAN3 use route-map ddd, and has 1 entry active.
```

```
-----
Entry sequence 10, permit
Match ip access-list:
ac1
Set Outgoing nexthop
90.0.0.3
switch(config)#
```

### 61.1.3 show ip pbr policy

#### Description

#### show ip pbr policy

Parameter	Default value
None	None

#### Description

It is used to display the information about RIP configuration.

#### Example

The following example shows how to display the information about IP-PBR policy routing configuration.

```
IP policy based route state: enabled
VLAN3 use route-map ddd, and has 1 entry active.
```

```
-----
Entry sequence 10, permit
Match ip access-list:
ac1
Set Outgoing nexthop
90.0.0.3
switch(config)#
```

### 61.1.4 *show ip pbr exf*

#### Description

**show ip pbr exf**

Parameter	Default value
None	None

#### Description

It is used to display the information about IP-PBR equivalent routing.

#### Example

The following example shows how to display the information about IP-PBR equivalent routing.

```
switch(config)# show ip pbr exf
IP policy based route state: enabled
Equiv EXF has 1 entry active.
```

```
-----
Entry sequence 1, handle c1f95b0
Dest ip: 1.1.0.0/16
90.0.0.3
192.168.213.161
switch(config)#
```

### 61.1.5 *debug ip pbr*

#### Description

**debug ip pbr**

**no debug ip pbr**

Parameter	Default value
None	None

#### Description

It is used to enable or disable the debugging switch of IP-PBR.

#### Example

The following example shows how to enable the debugging switch of IP-PBR.

```
switch(config)# debug ip pbr
switch(config)#
```

## Chapter 62 VRRP Configuration Commands affects ONLY PXT-S2790G/2795G or Higher

### 62.1 VRRP Configuration Commands

The VRRP protocol (RFC2338) is supported, and the extended track and preempt delay functions are added.

#### 62.1.1 vrrp associate

To configure basic IP and secondary IP of the VRRP group, and activate VRRP, run **vrrp associate**. To cancel the configured IP and stop VRRP group, run **no vrrp associate**.

**[no] vrrp associate** *group-number ip-address netmask* [**secondary**]

**no vrrp associate**

Parameter

Parameter	Description
<i>group-number</i>	Added VRRP group numberIts default value is 0.
<i>ip-address</i>	Added IP address
<i>netmask</i>	Network address mask
<i>secondary</i>	Means that the currently-configured IP is a secondary IP.

Default

There is no default value.

Command mode

Interface configuration mode

Explanation

The added virtual IP address of VRRP can be the basic IP address of VRRP or the VRRP secondary IP address. This IP address (basic IP or secondary IP) cannot belong to the network segment where any other interface's IP lies, or cannot belong to the network segment where any interface module's IP or global application module's IP lies. Except that basic VRRP IP can be same to the basic IP of the interface where basic vrrp IP lies, the configured VRRP IP cannot be same to the IP of any current interface. However, the IP of the current interface and the configured VRRP IP can be in the same network segment.

You can run **no vrrp [group-number] associate** to cancel all VRRP IP addresses of the current interface group.

When an IP address of a VRRP group is same to the basic IP address of the current interface, VRRP enters the owner state, which is a special master state. The owner state has the following attributes: the precedence of the group is automatically changed to 255; this group must be in master state; the configured track gets ineffective in this case.

Example

The following example shows how to configure basic IP address and secondary IP address on interface ethernet1/0:

```
interface ethernet1/0
vrrp 3 associate 100.1.1.1
vrrp 3 associate 100.1.1.2 secondary
```

### 62.1.2 vrrp description

To configure the description of the interface, run **vrrp *group-number* description WORD**. To cancel the description of the interface, run **no vrrp description WORD**.

**vrrp *group-number* description WORD**

**no vrrp description WORD**

Parameter

Parameter	Description
<i>group-number</i>	Group number, whose default value is 0
<i>WORD</i>	Configures the description character string of the group.

Default

There is no default value.

Command mode

Interface configuration mode

Explanation

This command is just to configure a description for an interface and has no effect on other functions of the interface.

Example

```
vrrp 3 description Shanghai_dial
```

### 62.1.3 vrrp priority

To configure the priority of a group, run **vrrp [*group-number*] priority <1-254>**. To cancel the configured priority of the group and resume its default value, run **no vrrp [*group-number*] priority**.

**vrrp [*group-number*] priority <1-254>**

**no vrrp [*group-number*] priority**

Parameter

Parameter	Description
<i>group-number</i>	Group number, whose default value is 0

<1-254>	A value between 1 and 254
---------	---------------------------

### Default

The default value is 100.

### Command mode

Interface configuration mode

### Explanation

When the priority of a group is configured in the owner state, the priority can be configured but cannot be used currently for the current priority is 255. When the group is in owner state, its priority automatically changes to 255.

### Example

**vrrp 3 priority 180**

#### 62.1.4 vrrp preempt

To configure the preemption mode of a group, run **vrrp *group-number* preempt**. The preemption delay can also be configured.

**[no] vrrp *group-number* preempt**

**[no] vrrp *group-number* preempt delay <1-255>**

### Parameter

Parameter	Description
<i>group-number</i>	Group number, whose default value is 0
<1-255>	Configured preemption delay, whose unit is second

### Default

It is the preemption mode by default.

### Command mode

Interface configuration mode

### Explanation

When this group receives an advertise packet with a lower priority in preemption mode, this group would not update the master down timer and the preemption will occur later. If the preemption mode is not configured, the master down timer will carry on update even if this group's priority is higher than the packet's.

The preemption delay means the minimum time which has to wait before the preemption. When a packet with comparatively lower priority is received by this group, the master down timer will be updated as the delay value if the master down timer is shorter than the configured preempt delay.



The preemption is canceled and the preemption delay is set to 0.

### Example

```
vrp 3 preempt
```

```
vrp 3 preempt delay 10
```

### 62.1.5 vrrp track

To track an interface, run **vrrp group-number track interface interface-number <1-255>**.

When the tracked interface changes, you can justify its priority.

```
[no] vrrp group-number track interface interface-number <1-255>
```

### Parameter

Parameter	Description
<i>group-number</i>	Group number, whose default value is 0
<i>interface-number</i>	Interface-number, such as f0/0
<1-255>	Configured preemption delay, whose unit is second

### Default

There is no default value.

### Command mode

Interface configuration mode

### Explanation

When a group is configured with a track function and the protocol of the tracked interface changes to **down**, the priority of the group decreases to the configured value; if the protocol of the tracked interface changes to **up**, the priority of the group increases to the configured value.

Currently only the state of the link protocol of the interface can be tracked. The following actions will lead the change of the protocol state: the cut-off of the network cable that the interface connects, interface's shutdown and link protocol's disconnection.

When the group is in owner state, the configured track function will automatically get ineffective.

### Example

```
vrp 3 track interface ethernet2/1 20
```

```
no vrrp 3 track interface ethernet2/1
```

### 62.1.6 vrrp authentication

To configure the authentication character string of the VRRP group, run **vrrp**

***group-number* authentication WORD.**

**[no] vrrp *group-number* authentication WORD**

Parameter

Parameter	Description
<i>group-number</i>	Group number, whose default value is 0
WORD	An eight-byte authentication string

Default

The authentication string is null by default and the authentication is not performed.

Command mode

Interface configuration mode

Explanation

The packet received by a VRRP group is effective only when its authentication string is same to the configured authentication string. Pay attention that multiple masters will exist concurrently if different authentication strings appear in the same group during configuration.

Example

```
vrrp 3 authentication
```

```
no vrrp 3 authentication
```

### 62.1.7 vrrp timers

To configure the value of advertisement timer of the VRRP group, run **vrrp timers**.

**[no] vrrp *group-number* timers advertise <1-255>**

**[no] vrrp *group-number* timers advertise dsec <5-360>**

**[no] vrrp *group-number* timers learn**

Parameter

Parameter	Description
<i>group-number</i>	Group number, whose default value is 0
<1-255>	Configured time of advertise, whose unit is second
<5-360>	Configured time of advertise, whose unit is 0.1 second
<i>learn</i>	Configures the learning mode of advertise.

Default

The default value of the timer is 1 second. The learning does not perform by default.

## Command mode

Interface configuration mode

## Explanation

This command is used to configure the value of the advertise timer in second. The value of master down timer is calculated through the advertise timer, and the value is  $[3 * \text{advertise}, 3 * \text{advertise} + 256 / (256 - \text{priority})]$ .

Only when a group has no configured timer value and the learning ability has been set can the group learn the advertise timer value from the master-transmitted packets.

When using this command, you are recommended to use the same value.

## Example

```
vrp 3 timers advertise 3
```

```
vrp 3 timers advertise dsec 15
```

```
no vrp 3 timers advertise
```

```
vrp 3 timers learn
```

### 62.1.8 show vrrp

To display the current running state of VRRP, run the following command:

```
show vrrp interface interface-numeric [ detail ]
```

```
show vrrp brief
```

```
show vrrp detail
```

## Parameter

detail : Displays the details about the running state.

## Default

There is no default value.

## Command mode

Interface command mode/configuration mode/privileged mode

## Explanation

This command is used to display the running state of the currently-configured VRRP.

The brief mode is to display only the simple state, and the group in init state will not be displayed.

However, the detail mode can display more information about the configured group.

## Example

```
show vrrp interface e2/1 detail
```

```
show vrrp brief
```

### 62.1.9 debug vrrp

To debug VRRP, run the following commands:

```
debug vrrp interface interface-number group-number all | packets | errors | events
```

```
debug vrrp all | packets | errors | events
```

```
no debug vrrp
```

Parameter

Parameter	Description
<i>interface-number</i>	Interface number
<i>group-number</i>	Number of the group

Default

Command mode

There is no default value.

Privileged mode

Explanation

This command can be used to export the debugging information about the error, packet and event of VRRP. The all parameter means that all three events will be exported.

Example

```
debug vrrp interface e2/1 3 all
```

```
no debug all
```

## Chapter 63 Basic Multicast Commands affects ONLY PXT-S2790G/2795G or Higher

### 63.1 Basic Multicast Commands

#### 63.1.1 debug ip mpacket

If you want to track the process for the multicast packet, you can use this command “**debug ip mpacket**”, and use the “no” form of the command to close debug information.

```
debug ip mpacket access-list group-address detail
```

```
no debug ip mpacket
```

Parameter

Parameter	Description
<i>access-list</i>	Range for tracked multicast packets
<i>group-address</i>	The tracked multicast packet group address
<i>detail</i>	Details for multicast packet processing

## Default

Close debug information output

## Command mode

Supervisor mode

## Explanation

You can use this command to track the main process for igmp-host end protocol.

## Example

The following example shows some situations for multicast packet processing.

You have received the (100.168.20.151,224.1.1.1) packet on e0/1 port, and the packet length is 112 bytes.

You have sent the (192.168.20.99,224.0.0.5) packet on e0/1 port, and the packet length is 64 bytes.

```
router#debug ip mpacket
```

```
MINPUT : IP Ethernet0/1 (100.168.20.151,224.1.1.1) , len=112
```

```
MOUTPUT : IP Ethernet0/1 (192.168.20.99,224.0.0.5) , len=64
```

### *63.1.2 debug ip mrouting*

Use this command “debug ip mrouting” to enable “mrouting” tracking function, then you can see the change from the multicast transfer list. In addition, use the “no” forma of the command to close debug information.

## Syntas

**debug ip mrouting**

**no debug ip mrouting**

## Parameter

None

## Default

Close all tracking functions.

## Command mode

Supervisor mode

## Explanation

You can use this command to see the change from the multicast transfer list, such as (S, G)/(\*,G) adding/deleting and downstream interface adding/deleting.

## Example

The following example shows you some changes from the multicast transfer list. First the (192.168.20.110, 239.0.0.100) item is created, and then Loopback0 is added for downstream interface. Finally, the item is deleted due to timeout.

```
router#debug ip mrouting
MBR: create (192.168.20.110, 239.0.0.100)
MBR: w/ oif Loopback0
MBR: delete (192.168.20.110, 239.0.0.100)
```

### Relevant command

#### ip multicast-routing

##### 63.1.3 debug ip mroute-cache

Use this command “debug ip mrouting” to enable “mroute-cache” tracking function, then you can see the change from the multicast routing cache. In addition, you can use the “no” format of the command to close the tracking.

### Syntas

**debug ip mroute-cache** *group-address*

**no debug ip mroute-cache**

### Parameter

Parameter	Description
<i>group-address</i>	<b>The tracked multicast routing cache group address</b>

### Default

Close all tracking functions.

### Command mode

Supervisor mode

### Explanation

You can use this command to see the change of the adding/deleting of multicast routing cache.

### Example

The following example shows you some changes on the multicast routing cache, and the creating and timeout of (192.168.20.97,230.0.0.1) cache.

```
router#debug ip mroute-cache
MRC: create (192.168.20.97,230.0.0.1) mroute-cache
MRC: expired (192.168.20.97,230.0.0.1) mroute-cache
```

### 63.1.4 debug ip multicast

You can use this command “**debug ip multicast**” to enable multicast event tracking function, and then see the interaction between the multicast protocol and mrouting. you can use the “**no**” format of the command to close the function.

#### Syntas

**debug ip multicast [alert | border-router]**

**no debug ip multicast [alert | border-router]**

#### Parameter

Parameter	Description
<i>alert</i>	Track the alert interaction among multicast routing components
<i>border-router</i>	Track related events of multicast border router MBR

#### Default

Close all tracking functions.

#### Command mode

Supervisor mode

#### Explanation

Defining some standard events between multicast routing protocol and mrouting indicates “alert”, for example: creation alert/deletion alert which related (S,G). You can use “debug ip multicast alert” to see these alerts.

' s multicast routing protocol supports MBR, and each multicast routing protocol is a “component”. You can use “debug ip multicast border-router” to see the component’s running information.

#### Example

In the following example, the alert router is turned on for output:

```
router#debug ip multicast alert
```

```
MBR: [(S, G) deletion alert], originated by OLNK, sent to all components
```

```
MBR: [(S, G) creation alert], originated by NONE, sent to all components
```

```
MBR: src = 192.168.20.110, grp = 239.0.0.100
```

```
MBR:    sent to owner OLNK first
```

```
MBR: [(S, G) join alert], originated by NONE, sent to OLNK
```

```
MBR: src = 192.168.20.110, grp = 239.0.0.100
```

```
MBR: [(S, G) firstuse alert], originated by NONE, sent to OLNK
```

```
MBR: src = 192.168.20.110, grp = 239.0.0.100
```

MBR: [(S, G) deletion alert], originated by OLNK, sent to all components

MBR: src = 192.168.20.110, grp = 239.0.0.100

### 63.1.5 ip mroute

Use the command “ip mroute” to configure the static multicast routing, and use “no ip mroute” to delete the configured static multicast routing.

#### Syntas

**ip mroute** *source-address mask [rpf-address type-number [distance]]*

**no ip mroute** *source-address mask [rpf-address type-number [distance]]*

#### Parameter

Parameter	Description
<i>source-address</i>	<b>Multicast source IP address</b>
<i>mask</i>	<b>Multicast source IP address mask</b>
<i>rpf-address</i>	<b>RPF address of Static multicast routing</b>
<i>type-number</i>	<b>RPF interface of Static multicast routing</b>
<i>distance</i>	<b>Optional management distance</b>

#### Default

The default management distance is 0.

#### Command mode

global configuration mode

#### Explanation

This command allows you to manually configure the location information for the multicast source. It is used when the multicast and unicast topologies are not identical.

#### Example

The following example will configure a static multicast routing through the specified interface:

```
router_config#ip mroute 100.1.1.0 255.255.255.0 192.1.1.1 f0/0
```

#### Relevant command

**show ip mroute static**

### 63.1.6 ip mroute-cache

Use this command “ip mroute-cache” to configure a multicast routing cache on the port, and “no ip mroute-cache” to disable the multicast routing cache.

#### Syntas



**ip mroute-cache**

**no ip mroute-cache**

Parameter

None

Default

The default is to use the multicast routing cache on the port.

Command mode

interface configuration mode

Explanation

Use the command when a port uses the multicast routing cache to receive/send the packet, ip will search the cache when a multicast packet is received. If there is no routing information in the cache, the port will ask for multicast routing module.

Example

The following example will enable multicast routing cache on interface e1/0.

```
router_config_e1/0#ip mroute-cache
```

Relevant command

**show ip mroute-cache**

### ***63.1.7 ip multicast-routing***

Use this command “ip multicast-routing” to enable IP multicast packet transferring function, and “no ip multicast-routing” to disable the function.

Syntas

**ip multicast-routing**

**no ip multicast-routing**

Parameter

none

Default

The default is not to transfer multicast packets.

Command mode

global configuration mode

Explanation

If you disable this function, the router will no longer transfer multicast packets, meanwhile, the multicast routing list and the multicast cache will be empty.

Example

The following example will configure the router to transfer multicast packets:

```
router_config#ip multicast-routing
```

Relevant command

```
show ip mroute mfc
```

### 63.1.8 ip multicast route-limit

Use this command “ip multicast route-limit” to configure the maximum number of multicast routing item, and “no ip multicast route-limit” to un-limit the number.

Syntas

```
ip multicast route-limit size
```

```
no ip multicast route-limit size
```

Parameter

Parameter	Description
<i>size</i>	Maximum number of multicast routing item

Default

The default multicast routing item number is unlimited.

Command mode

global configuration mode

Explanation

If you have configured this function, the multicast routing item number will be limited.

Example

The following example will configure the maximum number of multicast routing list to 2000:

```
router_config#ip multicast route-limit 2000
```

Relevant command

```
show ip mroute mfc
```

### 63.1.9 ip multicast boundary

Use this command “ip multicast boundary” to manage the range for the port allowed processing multicast packets; it is valid for input/output packets on the port. use “no ip multicast boundary” to cancel this command.

Syntas

```
ip multicast boundary access-list
```

```
no ip multicast boundary
```

Parameter

Parameter	Description
<i>access-list</i>	<b>the access-list name used to specify the range for processing multicast packets.</b>

### Default

Process all multicast packets.

### Command mode

interface configuration mode

### Explanation

If the function is configured, the range for the port allowed processing multicast packets will be limited.

### Example

The following example will configure the range for the port e1/0 allowed processing multicast packets to the range limited by the access-list testacl:

```
router_config_e1/0#ip multicast boundary testacl
```

#### 63.1.10 ip multicast helper-map

Use this command “ip multicast helper-map” to configure the connection of two broadcast networks with the multicast routing on the multicast network, and “no ip multicast helper-map” to cancel this command.

```
ip multicast boundary helper-map {group-address | broadcast} {broadcast-address | multicast-address } access-list
```

```
no ip multicast boundary helper-map {group-address | broadcast}
```

```
{broadcast-address | multicast-address } access-list
```

### Parameter

Parameter	Description
<i>group-address</i>	<b>The multicast packet group address which needed to be converted to the broadcast packet. it is used with the broadcast-address keyword.</b>
<i>broadcast</i>	<b>It can convert the broadcast packet to the multicast packet. it is used with the multicast-address keyword.</b>
<i>broadcast-address</i>	<b>The target address of broadcast packet which is sent after converting. it is used with the group-address keyword.</b>
<i>multicast-address</i>	<b>The target address of multicast packet which is sent after converting. It is used with the broadcast keyword.</b>
<i>access-list</i>	<b>IP extended access-list name. You can use it to specify the port number for packet converting.</b>

### Default

Not perform the conversion between any multicast packets and broadcast packets.

### Command mode

interface configuration mode

### Explanation

If two broadcast networks are connected with a multicast network, you can convert the broadcast flow to multicast flow on the first hop router connected with the source broadcast network, and then convert the multicast flow to broadcast flow on the last hop router connected with the target broadcast network. Thus, you can utilize the multicast network's multicast characteristic between the two broadcast networks which are required to be connected with each other. Furthermore, it can prevent the packets between two broadcast networks from being sent repeatedly, and utilize the "quick forward" characteristic on the multicast network.

Before using "ip multicast helper-map", you should have configured this command "ip directed-broadcast" on the port.

### Example

Configuration on the router is as follow:

if you configure command "ip directed-broadcast" on port e0 of the first hop router, it will be allowed to process the link broadcast packets.

If you have configured "ip multicast helper-map broadcast 230.0.0.1 testacl1", you can convert the udp broadcast packet, whose port number is 4000("ip forward-protocol" command specified) and the source address is 192.168.20.97/24 (testacl1 specified) ,to multicast packet whose target address is 230.0.0.1 ("ip multicast helper-map" command specified).

if you configure command "ip directed-broadcast" on port e1 of the last hop router, it will be allowed to process the link broadcast packets.

If you have configured "ip multicast helper-map broadcast 230.0.0.1 172.10.255.255 testacl2", you can convert the multicast packet, whose port number is 4000("ip forward-protocol" command specified), the source address is 192.168.20.97/24 (testacl2 specified) and target address is 230.0.0.1 ,to broadcast packet whose target address is 170.10.255.255 ("ip multicast helper-map" command specified).

On the first hop router which is connected with the source broadcast network:

```
interface ethernet 0
```

```
ip directed-broadcast
```

```
ip multicast helper-map broadcast 230.0.0.1 testacl
```

```
ip pim dense-mode
```

```
!
```

```
ip access-list extended testacl permit udp 192.168.20.97 255.255.255.0 any
```

```
ip forward-protocol udp 4000
```

On the last hop router which is connected with the target broadcast network:

```
interface ethernet 1
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim dense-mode
!
ip access-list extended testacl2
permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000
```

Relevant command

**ip forward-protocol**

**ip directed-broadcast**

### 63.1.11 ip multicast rate-limit

Use this command “**ip multicast rate-limit**” to limit the multicast packet flow receiving and sending in the range of a source/group on the port, and “**no ip multicast rate-limit**” to cancel this flow limitation.

Syntas

**ip multicast rate-limit** {in | out} [**group-list** *access-list*] [**source-list** *access-list*] kbps

**no ip multicast rate-limit** {in | out} [**group-list** *access-list*] [**source-list** *access-list*]

Parameter

Parameter	Description
<i>in</i>	Limit the input packet flow on the port.
<i>out</i>	Limit the output packet flow on the port.
<i>group-list</i> <i>access-list</i>	(optional) Limit the multicast packet flow for the group address in access-list.
<i>source-list</i> <i>access-list</i>	(optional) Limit the multicast packet flow for the source address in access-list.
<i>kbps</i>	(optional) Allowed maximum flow. If its value is 0, no packet will be allowed to pass.

Default

No limitation to the flow.

Command mode

interface configuration mode

## Explanation

The packet flow in specified range has exceeded the limit at last second. You have to discard the packet, or the packet will be forwarded.

## Example

The maximum output packet flow rate on port s0 (192.168.20.97 , 230.0.0.1) is limited to 64kbps.

```
interface serial 0
ip multicast rate-limit out group-list gacl source-list sacl 64
ip access-list standard sacl
permit 192.168.20.97 255.255.255.255
ip access-list standard gacl
permit 230.0.0.1 255.255.255.255
```

### 63.1.12 ip multicast ttl-threshold

Use this command “ip multicast ttl-threshold” to configure the maximum threshold value of multicast packet ttl on the port, and “no ip multicast ttl-threshold” to restore default.

## Syntas

**ip multicast ttl-threshold** *ttl-value*

**no ip multicast ttl-threshold**

## Parameter

Parameter	Description
<i>ttl-value</i>	The multicast packet ttl threshold value on the port.

## Default

The default ttl threshold value on the port is 1.

## Command mode

interface configuration mode

## Explanation

The ttl value of receiving/sending packet should be largerer than the specified threshold value on the port, you can use this command to configure a router to border router.

## Example

The ttl threshold value configured on port s0 is 200, it means only the multicast packet with ttl value more than 200 is allowed to be received/sent on the port.

```
interface serial 0
```

```
ip multicast ttl-threshold 200
```

### 63.1.13 show ip mflow

You can use this command “show ip mflow” to display global flow information processed by system and multicast flow information processed on the port.

#### Syntas

```
show ip mflow [group-address | source-address]interface
```

#### Parameter

Parameter	Description
<i>group-address</i>	<b>The displayed multicast flow information group address.</b>
<i>source-address</i>	<b>The displayed multicast flow information source address.</b>
<i>interface</i>	<b>The displayed port multicast flow information.</b>

#### Default

none

#### Command mode

Supervisor mode

#### Explanation

Display the processed packet number from the multicast flow, wrong incoming interface packet number, and current flow value.

#### Example

The following example will display global multicast flow information:

```
router#show ip mflow
```

```
IP Multicast Flow
```

```
(100.168.20.151,224.1.1.1)
```

```
total process : 0 wrong_if_count : 0 curr-flux : 0.00
```

```
(192.167.20.131,239.1.1.1)
```

```
total process : 0 wrong_if_count : 0 curr-flux : 0.00
```

The following example will display port multicast flow information:

```
router#show ip mflow interface e0/1
```

```
IP Multicast Flow
```

```
(192.168.20.97,230.0.0.1)
```

```
total rcv : 21180 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
```

```
(100.168.20.151,224.1.1.1)
```

```
total rcv : 16822400 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
```

```
(192.168.20.97,232.0.0.1)
```

```
total rcv : 240 total send : 0 curr-in-flux : 0.00 curr-out-flux : 0.00
```

```
(192.167.20.131,239.1.1.1)
```

```
total rcv : 103264 total send : 0 curr-in-flux : 0.90 curr-out-flux : 0.00
```

### 63.1.14 show ip mroute-cache

use this command “show ip mroute-cache” to display the information on the multicast routing cache.

#### Syntas

```
show ip mroute-cache [group-address]
```

#### Parameter

Parameter	Description
<i>group-address</i>	The displayed multicast routing cache group address

#### Default

none

#### Command mode

Supervisor mode

#### Explanation

MRC (Multicast Route Cache) is a global multicast routing cache, and every MRC item contains the (S, G)/ (\*, G) information, upstream/downstream interface information received from the multicast routing.

#### Example

The following example will display multicast routing list information:

```
router#show ip mroute-cache
```

```
IP Multicast Route Cache
```

```
(192.168.20.97, 230.0.0.1)|(192.168.20.97,230.0.0.1)
```

```
Incoming interface: Ethernet0/2, Last used : 00:00:34
```

```
Outgoing interface list:
```

```
Loopback0
```

```
(192.168.20.97, 230.0.0.2)|(192.168.20.97,230.0.0.2)
```



Incoming interface: Ethernet0/2, Last used : 00:00:12

Outgoing interface list:

Loopback1

### 63.1.15 show ip mroute mfc

You can use this command “show ip mroute mfc” to display the multicast forwarding list information, and then activate the multicast function.

Syntas	Default
<b>show ip mroute mfc</b>	none
Parameter	Command mode
none	Supervisor mode

#### Explanation

MFC (Multicast Forwarding Cache) is a global multicast forwarding list, and the multicast packet is forwarded by it. Every MFC item has (S, G)/ (\*, G) information and upstream/downstream interface information.

#### Example

The following example will display multicast routing list information:

```
router#show ip mroute mfc
```

```
IP Multicast Forwarding Cache
```

```
(192.168.20.110/32, 239.0.0.100/32)
```

```
Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
```

```
Outgoing interface list:
```

```
Loopback0, owned by OLNK
```

```
(192.168.20.110/32, 239.0.0.101/32)
```

```
Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
```

```
Outgoing interface list:
```

```
Loopback0, owned by OLNK (192.168.20.138/32, 239.1.1.1/32)
```

```
Incoming interface: Ethernet0/2, RPF nbr 0.0.0.0, owned by OLNK
```

```
Outgoing interface list:
```

```
Loopback0, owned by OLNK
```

#### Relevant command

```
show ip mroute olnk
```

```
show ip mroute static
```

## Chapter 64 IGMP Configuration Commands

### 64.1 IGMP Configuration Commands

#### 64.1.1 clear ip igmp group

If you want to clear the multicast group member information saved in multicast router that supports IGMP, you can use the command “clear ip igmp group”.

##### Syntas

```
clear ip igmp group type-number group-address
```

##### Parameter

Parameter	Description
<i>type-number</i>	port type and port number.
<i>group-address</i>	Multicast group’s group address to clear information.

##### Default

None

##### Command mode

Supervisor mode

##### Explanation

Using this command, you can clear the multicast group member information saved in router when the saved multicast group information has a problem.

##### Example

The following example shows you how to clear the information of multicast group 233.33.1.1 on e1/0 port.

```
clear ip igmp group e1/0 233.33.1.1
```

##### Relevant command

None

#### 64.1.2 debug ip igmp

If you want to track the process for igmp-router end protocol, you can use this command “debug ip igmp”, and use the “no” forma of the command to close debug information.

##### Syntas

```
debug ip igmp
```

```
no debug ip igmp
```

##### Parameter

None

### Default

Close debug information output

### Command mode

Supervisor mode

### Explanation

You can use this command to track the main process for igmp-router end protocol to find the reason for protocol processing failure.

### Example

igmp-router function module's debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information.

#### *64.1.3 debug ip igmp-host*

If you want to track the process for igmp-host end protocol, you can use this command "debug ip igmph", and use the "no" forma of the command to close debug information.

### Syntas

**debug ip igmph** *group-address*

**no debug ip igmph**

### Parameter

None

### Default

Close debug information output

### Command mode

Supervisor mode

### Explanation

You can use this command to track the main process for igmp-host end protocol to find the reason for protocol processing failure.

### Example

Igmp-host function module's debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information.

#### *64.1.4 ip igmp helper-address*

If you want a port to transit IGMP packet, you can use this command to configure the port. One port can configure the command only once time, so the next configured command will overwrite the original command.

### Syntas

**ip igmp helper-address** *destination-address*

**no ip igmp helper-address** *destination-address*

#### Parameter

Parameter	Description
<i>destination-address</i>	<b>The destination address of transitting IGMP packet.</b>

#### Default

The port will not transit IGMP packet

#### Command mode

interface configuration mode

#### Explanation

Use this command “ip igmp helper-address” to transit all received igmp packets.

#### Example

```
ip igmp helper-address 192.168.20.10
```

### 64.1.5 ip igmp join-group

If you want to add a multicast group on the port, you can use this command to perform it.

#### Syntas

**ip igmp join-group** *group-address* [{include|exclude} *source-address*]

**no ip igmp join-group** *group-address* [{include|exclude} *source-address*]

#### Parameter

Parameter	Description
<i>group-address</i>	<b>The multicast group required to be added to the port</b>
<i>include</i>	<b>The mode of SSM needed to add a multicast group is “include”.</b>
<i>exclude</i>	<b>The mode of SSM needed to add a multicast group is “exclude”.</b>
<i>source-address</i>	<b>Source filter address whose port is added to multicast group.</b>

#### Default

No multicast group will be added to the port.

#### Command mode

interface configuration mode

#### Explanation

Use this command “ip igmp join-group” to dynamically add a multicast group to the port.

### Example

```
ip igmp join-group 230.0.0.1
```

```
ip igmp join-group 230.0.0.1 exclude 192.168.20.10
```

### 64.1.6 ip igmp immediate-leave group-list

If you want the router port running IGMP version 2 to run the multicast group function “Exit Now”, you can use this command “**ip igmp immediate-leave group-list**” to perform configuring. In addition, you can use the “no” format of the command to forbid the IGMP host to “exit now”.

### Syntas

```
ip igmp immediate-leave group-list list-name
```

```
no ip igmp immediate-leave group-list
```

### Parameter

Parameter	Description
<i>list-name</i>	Pre-configured ip standard access-list name

### Default

The IGMP host is not allowed to run “Exit Now” function.

### Command mode

global configuration mode/interface configuration mode

### Explanation

This command is available only for the port of running IGMP version 2. it can be used when the network connecting with the port has only one IGMP host. Through configuring this command, the host can immediately exit from a multicast group without the process for packet exchanging and delaying from the router. Besides, you can configure this command in “global configuration mode” and “interface configuration mode”, but this command configured in “global configuration mode” will be prior to the command configured in “interface configuration mode”. If you have configured the command in “global configuration mode”, the next command configured in “interface configuration mode” will be ignored. On the other hand, the command configured in “global configuration mode” will overwrite the original command configured in “interface configuration mode”.

### Example

Prefer to “Configure multicast routing”.

### Relevant command

```
ip access-list
```

### 64.1.7 *ip igmp last-member-query-interval*

To change the query interval of last group member I on the current port, use this command “**ip igmp last-member-query-interval**”. You can use the “no” format of the command to restore default settings.

Syntas

**ip igmp last-member-query-interval** *time*

**no ip igmp last-member-query-interval**

Parameter

Parameter	Description
<i>time</i>	The value of last member query interval configured on the port. Its unit is millisecond.

Default

The default of the last group member query interval on the port is 1000ms.

Command mode

interface configuration mode

Explanation

You can use this command “ip igmp last-member-query-interval” to modify the last group member query interval on the port.

Example

The following example will modify the last member query interval on the port to 2 seconds.

```
interface ethernet 0/0
```

```
ip igmp last-member-query-interval 2000
```

### 64.1.8 *ip igmp querier-timeout*

you can use this command “**ip igmp querier-timeout**” to modify other routers for IGMP querier timeout,.use the “**no**” f ormat of this command to restore default.

Syntas

**ip igmp querier-timeout** *time*

**no ip igmp querier-timeout**

Parameter

Parameter	Description
<i>time</i>	other querier timeout. Its unit is second.

Default

125 seconds

#### Command mode

interface configuration mode

#### Explanation

You can use this command “ip igmp querier-timeout” to modify other routers for querier timeout. This command is available only for the port which running IGMP version 2.

#### Example

The following example shows that the querier-timeout specified on interface Ethernet 0/0 is 100 seconds.

```
interface ethernet 0/0
ip igmp querier-timeout 100
```

#### 64.1.9 ip igmp query-interval

To set the interval for IGMP General Query packet sending on the port, you can use this command “ip igmp query-interval”. Use the “no” format of this command to restore default.

#### Syntas

**ip igmp query-interval** *time*

**no ip igmp query-interval**

#### Parameter

Parameter	Description
<i>time</i>	Interval of sending general query packet. Its unit is second.

#### Default

60 seconds

#### Command mode

interface configuration mode

#### Explanation

you can use this command “ip igmp query-interval” to set the interval for IGMP General Query packet sending on the port,

#### Example

The following example shows that the interval of sending general query packet on Ethernet 0/0 port is specified to 50 seconds.

```
interface ethernet 0/0
ip igmp query-interval 50
```

### 64.1.10 *ip igmp query-max-response-time*

To specify the maximum interval for IGMP host to respond General Query packet, you can use this command “**ip igmp query-max-resposne-time**”. Use the “**no**” format of this command to restore default.

#### Syntas

**ip igmp query-max-response-time** *time*

**no ip igmp query-max-response-time**

#### Parameter

Parameter	Description
<i>time</i>	Value of the maximum response time configured on the port.

#### Default

10 seconds

#### Command mode

interface configuration mode

#### Explanation

you can use this command “ip igmp query-max-resposne-time” to specify the maximum interval for IGMP host to respond General Query packet. This command is available only for the port which running IGMP version 2 and 3.

#### Example

The following example will set the IGMP maximum response time on Ethernet 0/0 port as 15 seconds.

```
interface ethernet 0/0
```

```
ip igmp query-max-response-time 15
```

### 64.1.11 *ip igmp static-group*

If you want to configure a static multicast group on the port, you can use this command “**ip igmp static-group**” to perform it. Use the “**no**” format of this command to restore default.

#### Syntas

**ip igmp static-group** { \* | *group-address* } {**include** *source-address* }

**no ip igmp static-group** { \* | *group-address* } {**include** *source-address* }

#### Parameter

Parameter	Description
*	All multicast groups.
<i>group-address</i>	specified multicast group address.
<i>source-address</i>	specified host source address.



## Default

In default, no multicast group is static configured on the port.

## Command mode

interface configuration mode

## Explanation

Configure the static IGMP multicast group information on the current port.

## Notes:

For the same group-address, you can configure several “include source-address” commands for the corresponding static multicast group to have several source-addresses existing. However, for the same group-address, you can’t configure both commands with/without “include source-address”.

## Example

Refer to “Configure multicast routing”

### 64.1.12 ip igmp version

To set the IGMP version number running on the port, you can use this command “**ip igmp version**”. use the “**no**” format of the command to restore default.

## Syntas

**ip igmp version** *version-number*

**no ip igmp version**

## Parameter

Parameter	Description
<i>version-number</i>	The value <b>1.2</b> or <b>3</b> indicates separately the IGMP version number <b>1,2</b> or <b>3</b> .

## Default

If you don’t configure this command, the default version number for IGMP-Router end protocol running on the port is 3.

## Command mode

interface configuration mode

## Explanation

Use this command “**ip igmp version**” can set the IGMP version number running on the port,

## Example

The following example will specify the IGMP version number running on Ethernet 0/0 port as 2.

```
interface ethernet 0/0
```

```
ip igmp version 2
```

### 64.1.13 show ip igmp groups

You can use the following command to see the multicast group member information that is saved on the current router.

#### Syntas

```
show ip igmp groups {interface | group-address | detail}
```

#### Parameter

Parameter	Description
<i>interface</i>	The port where you want to see the multicast group information. If you don't add this parameter, all multicast groups information on the port will be displayed.
<i>group-address</i>	The multicast group address to see. If you don't add this parameter, all multicast groups information on the router will be displayed.
<i>detail</i>	The router whether you want to see the multicast group information.

#### Default

None

#### Command mode

Supervisor mode/global configuration mode/interface configuration mode.

#### Explanation

You can use this command to see the multicast group member information that is saved on the router.

#### Example

```
show ip igmp groups e0/0 detail
```

Running this command will display the following message:

```
.....
```

```
Interface: Ethernet0/0
```

```
Group address: 233.33.1.3
```

```
Uptime: 00:03:46
```

```
Group status: Static
```

```
Group filter mode: INCLUDE
```

```
Last reporter: 0.0.0.0
```

```
Group source-list: (Flags: S-Static, R-Remote)
```

```
Source address:   Uptime      Timer      Fwd      Flags
192.168.20.5     00:03:46   stopped   Yes      S
```

Interface: Ethernet0/0

Group address: 233.33.1.1

Uptime: 00:03:46

Group status: Static

Group filter mode: INCLUDE

Last reporter: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

```
Source address:   Uptime      Timer      Fwd      Flags
192.168.20.5     00:03:46   stopped   Yes      S
192.168.20.3     00:03:46   stopped   Yes      S
192.168.20.1     00:03:46   stopped   Yes      S
```

.....

show ip igmp groups 233.33.1.1 detail

Running this command will display the following message:

Interface: Ethernet0/0

Group address: 233.33.1.1

Uptime: 00:02:42

Group status: Static

Group filter mode: INCLUDE

Last reporter: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

```
Source address:   Uptime      Timer      Fwd      Flags
192.168.20.5     00:02:42   stopped   Yes      S
192.168.20.3     00:02:42   stopped   Yes      S
192.168.20.1     00:02:42   stopped   Yes      S
```

show ip igmp groups

Running this command will display the following message:

```
Interface   Group address   Uptime   Expires   Last Reporter   Flags
Ethernet0/0 239.255.255.250 00:01:08 00:02:05 192.168.20.141  R
Ethernet0/0 224.2.127.254  00:01:09 00:02:00 32.1.1.67      R
```

Ethernet0/0	224.1.1.1	00:01:24	stopped	0.0.0.0	S
Ethernet0/0	233.33.1.5	00:01:24	stopped	0.0.0.0	S
Ethernet0/0	233.33.1.3	00:01:24	stopped	0.0.0.0	S
Ethernet0/0	233.33.1.1	00:01:24	stopped	0.0.0.0	S
Interface	Group address	Uptime	Expires	Last Reporter	Flags
Loopback10	239.255.255.250	00:01:08	00:02:05	192.168.20.141	R
Loopback10	224.2.127.254	00:01:09	00:02:00	32.1.1.67	R

### 64.1.14 *show ip igmp interface*

You can use this command to see information on the current router's port where IGMP is activated.

#### Syntas

**show ip igmp interface** *interface*

#### Parameter

Parameter	Description
<i>interface</i>	<b>The specified port to display information. If you don't add this parameter, all information on ports where IGMP is activated will be displayed.</b>

#### Default

None

#### Command mode

Supervisor mode/global configuration mode/interface configuration mode

#### Explanation

You can use this command to display information on the port where IGMP is activated.

#### Example

```
show ip igmp interface e0/0
```

Running this command will display the following information:

Ethernet0/0 is up, line protocol is up

Internet address is 192.168.20.167

Current IGMP router version is 3

Router plays role of querier on the interface now

IGMP is enable on the interface

IGMP query-interval is 60 seconds

IGMP max query response time is 10 seconds

IGMP Last member query response time is 1000 milliseconds

IGMP querier timeout is 125 seconds

Multicast routing is enabled on the interface

### 64.1.15 show ip igmp-host

You can use this command to see IGMP host information on the port of current router.

#### Syntas

**show ip igmp { *interface* } detail**

#### Parameter

Parameter	Description
<i>interface</i>	The specified port to display information.
<i>detail</i>	Display igmp host detailed information.

#### Default

none

#### Command mode

Supervisor mode/global configuration mode/interface configuration mode

#### Explanation

You can use this command to display basic IGMP host information on the port.

#### Example

```
show ip igmp interface e0/0
```

Running this command will display the following information:

IGMP host Mode is IGMP\_V3\_ROUTER

IGMP host Query Interval is 23 second

IGMP host Query Response Interval is 125

IGMP host Query Robustness Variable is 2

IGMP host Last Query Interval is 0

IGMP interface timer is 0

IGMP host group joined(number of users):

230.0.0.1(1)

## Chapter 65 PIM-DM Configuration Commands

### 65.1 PIM-DM Configuration Commands

#### 65.1.1 clear ip mroute pim-dm

Use the following command in supervisor mode to clear the (S,G) routing list items submitted by PIM-DM to mrouting:

#### Syntas

```
clear ip mroute pim-dm { * | group [source] }
```

#### Parameter

Parameter	Description
*	Delete all multicast routing list items submitted by pim-dm.
group	Delete all list items submitted by pim-dm and satisfied in the specified group.
source	(optional) Delete all list items submitted by pim-dm and satisfied in the specified group's source.

#### Default

None

#### Command mode

Supervisor mode

#### Explanation

The command will delete all or part of table lists of local multicast router table, and it is possible to affect the normal multicast packet forwarding. This command can only delete the (S,G) items, whose upstream port is created by PIM-DM multicast routing protocol, and inform mrouting, then mrouting will determine if it should re-establish the corresponding (S,G).

#### Example

Example1:

```
Router#clear ip mroute pim-dm *
```

All (S,G) items, whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared.

Example2:

```
Router#clear ip mroute pim-dm 239.1.1.1
```

All (S,G) items with the group address 239.1.1.1, whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared.

Example3:

```
Router#clear ip mroute pim-dm 239.1.1.1 192.168.20.131
```

All (S,G) items with the address (192.168.20.138, 239.1.1.1), whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared.

### 65.1.2 clear ip pim-dm interface

Reset the multicast packet statistic value forwarded through (S,G) on PIM-DM port. You can use the command in supervisor mode:

#### Syntas

```
clear ip pim-dm interface {count | type number}{count}}
```

#### Parameter

Parameter	Description
<i>count</i>	<b>(optional) Delete all multicast packet statistic values on PIM-DM port.</b>
<i>type number</i>	<b>(optional) Delete multicast packet statistic values on the specified port.</b>

#### Default

none

#### Command mode

supervisor mode

#### Explanation

This operation will reset the multicast packet number statistic values forwarded through PIM-DM port in local multicast routing list. This command can only reset the (S,G) items, whose upstream port is created by PIM-DM multicast routing protocol.

#### Example

Example1:

```
Router#clear ip pim-dm interface count
```

It will reset all multicast packet number statistic values forwarded by (S,G) items, whose upstream port is created by PIM-DM, on local MRT.

Example2:

```
Router#clear ip pim-dm interface Ethernet1/1 count
```

It will reset all multicast packet number statistic values forwarded by (S,G) items, whose upstream port is Ethernet1/1 and created by PIM-DM, on local MRT.

### 65.1.3 debug ip pim-dm

use this command to track input/output PIM packets and caused events. Set this command to "no" to stop tracking.

#### Syntas

```
debug ip pim-dm [group|alert]
```

## Parameter

Parameter	Description
<i>group</i>	(optional) Track the specified group status.
<i>alert</i>	(optional) Track the alert status received from mrouting.

## Default

none

## Command mode

supervisor mode

## Explanation

receive Alert from mrouting.

Send alert to other components.

## Example

Example 1, the output information is as follows:

Hello packet prompt sent to each port.

Hello packet prompt received from each port.

A new neighbor is found.

Delete neighbor.

Port sending status refresh packet.

Port receiving status refresh packet.

Port is sending Assert packet.

Port is receiving Assert packet.

Port is sending prune packet.

Port is receiving prune packet.

Port is sending graft ack packet.

Port is receiving graft ack packet.

Port is sending graft packet.

Port is receiving graft packet.

Port is sending join/prune packet.

Port is receiving join/prune packet.

When a new (S,G) is created

When deleting (S,G)



```
Router#debug ip pim-dm
```

```
2003-3-26 11:45:17 received V2 hello packet on Ethernet2/1 from 192.168.20.133(GenID = 3539)
```

```
2003-3-26 11:45:17 Ethernet2/1 create new nbr 192.168.20.133
```

```
2003-3-26 11:45:25 send hello packet to 224.0.0.13 on Loopback1
```

```
2003-3-26 11:50:29 Ethernet2/1 delete nbr 192.168.20.133
```

```
2003-3-26 11:50:51 received V2 hello packet on Ethernet2/1 from 192.168.20.152 2003-3-26 11:50:51 send hello packet to 224.0.0.13 on Ethernet2/1
```

```
2003-3-26 12:04:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success
```

```
2003-3-26 12:04:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful
```

```
2003-3-26 12:04:39 PIM-DM: ignored V2 packet on Ethernet2/1 from 192.168.10.204 (validate source address failed)
```

```
2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream:192.168.20.132
```

```
Adding in MRT success
```

```
2003-3-26 12:04:39 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT
```

Example 2, output received alert message:

```
Router#debug ip pim-dm alert
```

```
2003-3-26 12:09:51 receive alert_rt_change alert from mroute 2003-3-26 12:09:54 receive alert_rt_change alert from mroute 2003-3-26 12:11:08 PIM-DM: send sg_deletion alert
```

```
2003-3-26 12:11:19 receive alert_sg_creation alert from mroute
```

```
2003-3-26 12:11:20 receive alert_sg_prune alert from mroute 2003-3-26 12:11:56 receive alert_group_report alert from mroute 2003-3-26 12:11:56 receive alert_sg_join alert from mroute
```

Example 3, track the specified group status:

```
Router#deb ip pim-dm 239.1.1.1
```

```
Router#2003-3-26 12:35:27 PIM-DM: clear (192.168.20.138, 239.1.1.1) forwd pkt count success 2003-3-26 12:35:37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success
```

```
2003-3-26 12:35:37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful
```

```
2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream: 192.168.20.132
```

```
Adding in MRT success
```

```
2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 1.1.1.1 create success
```

```
2003-3-26 12:35:37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 192.167.20.13 create success
```

```
2003-3-26 12:35:42 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT
```

### 65.1.4 *ip pim-dm*

This command is used to run PIM-DM on the port. set this command to “no” to disable PIM-DM on the port.

#### Syntas

**ip pim-dm**

**no ip pim-dm**

#### Parameter

None

#### Default

None

#### Command mode

interface configuration mode

#### Explanation

1. If the “ip multicast-routing” is not configured before configuring this command, it will display the following warning: WARNING: "ip multicast-routing" is not configured, IP Multicast packets will not be forwarded
2. Once this function is disabled, PIMDM will no longer run on the port.but it will not affect other PIM-DM configurations. After rerun PIM-DM on the port, all PIM-DM configurations are still valid.
3. Enabling this function means it is available for forwarding multicast packet on the port, however, you have to enable the global multicast packet forwarding function first.

#### Example

```
Router_config#ip multicast-routing
Router_config#interface Ethernet1/1
Router_config_e1/1#ip pim-dm
```

#### Relevant command

**ip multicast-routing**

**show ip pim-dm interface**

### 65.1.5 *ip pim-dm dr-priority*

Set a router as the priority to specified router (DR). You can set this command to “no” to restore default DR priority on the port.

#### Syntas

**ip pim-dm dr-prioirty *priority***

**no pim-dm dr-prioirty**

## Parameter

Parameter	Description
<i>priority</i>	<b>Port DR priority. The larger the value is, the higher the priority is. Its range is from 0 to 4294967294, and the default is 1.</b>

## Default

default DR priority on PIM port is 1.

## Command mode

interface configuration mode

## Explanation

1. If all PIM neighbors support DR Priority on the port, select the one with the highest priority as DR. If all have the same priority, just select the one with the highest port IP value as DR.
2. If router didn't advertise its priority in Hello packet and there are several routers have the same situation, just select the router with the highest port IP value as DR.

**65.1.6 ip pim-dm hello-interval**

This command is used to configure the interval of regularly sent PIM-Hello packets on the port. You can set this command to "no" to restore default interval.

## Syntas

**ip pim-dm hello-interval *interval***

**no ip pim-dm hello-interval**

## Parameter

Parameter	Description
<i>interval</i>	<b>The interval of regularly sent PIM-Hello packets. Its range is from 0 to 65535, and the default is 30 seconds.</b>

## Default

30 seconds

## Command mode

interface configuration mode

## Explanation

Regularly sending Hello packets can check if the neighbor exists. Generally, if Hello packets is not received after the 3.5 times hello-interval timeout configured by neighbor, the neighbor will be considered disappeared.

For IGMP v1, you can select the specified router (DR) through PIM-DM Hello packet.

### Example

```
Router_config#interface Ethernet1/1
Router_config_e1/1#ip pim-dm hello-interval 30
```

### Relevant command

**ip igmp query-interval**

### 65.1.7 ip pim-dm state-refresh origination-interval

It allows the router to generate original PIM-DM state refresh packet and configure the state refresh interval. To cancel the generation for original PIM-DM state refresh packet, set this command to “no”.

### Syntas

**ip pim state-refresh origination-interval** [*interval*]

**no ip pim state-refresh origination-interval**

### Parameter

Parameter	Description
<i>interval</i>	<p>For the first port router connected with the source directly, it is the interval of regularly sending state refresh packet. For the following router, it is interval of allowed receiving and processing state refresh packet for the port.</p> <p>This parameter is configured optionally, and its range is from 4 to 100 seconds. The default is 60 seconds.</p>

### Default

This parameter is configured optionally. The default is 60 seconds.

### Command mode

interface configuration mode

### Explanation

Configure this command on the first router's, neighboring directly on the multicast source, incoming port. By default, it will generate original state refresh packet. During configuring this command on the following router's port, you can use interval to limit the process for received state refresh packet interval. By default, all routers where is running PIM-DM can process and forward state refresh packet.

### Example

```
Router_config_e1/1#ip pim-dm state-refresh origination-interval 80
```

### Relevant command

**ip pim-dm state-refresh disable**

### 65.1.8 *ip pim-dm neighbor-filter*

This command is used to prevent some routers from participating PIM-DM operation. Set this command to “no” to cancel the limit.

#### Syntas

**ip pim-dm neighbor-filter** *access-list-name*

**no ip pim-dm neighbor-filter** *access-list-name*

#### Parameter

Parameter	Description
<i>access-list-name</i>	<b>Standard access-list, whose definition is to deny PIM packets from the specified source.</b>

#### Default

No filter function.

#### Command mode

interface configuration mode

#### Explanation

You can use multiple filter lists. The router denied by anyone of the lists can't be a neighbor of local PIM-DM.

#### Example

```
router_config_e1/1#ip pim-dm neighbor-filter nbr_filter
router_config#ip access-list standard nbr_filter
router_config_std_nacl#deny 192.167.20.132 255.255.255.255
router_config_std_nacl#permit 192.168.20.0 255.255.255.0
```

#### Relevant command

**access-list**

### 65.1.9 *ip pim-dm state-refresh disable*

It will not allow running router process for PIM-DM multicast protocol or forward PIM-DM state refresh control message. You can set this command to “no” to restore the forwarding function.

#### Syntas

**ip pim-dm state-refresh disable**

**no ip pim-dm state-refresh disable**

#### Parameter

none

## Default

By default, it is allowed to run forwarding PIM dense mode state refresh control message.

## Command mode

Supervisor mode

## Explanation

After configuring this command to forbid processing and forwarding PIM-DM state refresh control message, the Hello message in PIM-DM will no longer contain state refresh control options and receive/send state refresh control packet.

## Example

The following command forbids forwarding state refresh control message to downstream neighbors of PIM dense mode.

```
ip pim-dm state-refresh disable
```

## Relevant command

**ip pim-dm state-refresh origination-interval**

### 65.1.10 show ip mroute pim-dm

Display PIM-DM multicast routing list information.

## Syntas

```
show ip mroute pim-dm group-address source
```

## Parameter

Parameter	Description
<i>group-address</i>	(optional) group address
<i>source</i>	(optional) source address

## Default

none

## Command mode

All modes except the user mode.

## Explanation

It can display all (S,G) or specified (S,G) only in local MRT.

## Example

Example1: Display all (S,G) in local MRT.

```
Router#show ip mroute pim-dm PIM-DM Multicast Routing Table Timers: Uptime/Expires
```

```
State: Interface state
```

```
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1),      00:00:03 /00:03:27
Incoming interface:
Ethernet2/1 Forwarding 0.0.0.0
Outgoing interface list:
Loopback1  NoInfo 00:00:07 /00:00:00
```

```
(192.168.20.138, 239.1.1.1),      00:00:03 /00:03:27
Incoming interface:
Ethernet2/1 Forwarding 0.0.0.0
Outgoing interface list:
Loopback1  NoInfo 00:00:07 /00:00:00
Ethernet1/1 NoInfo 00:02:43 /00:00:00
```

Example 2: Display the specified (S,G) in local MRT.

```
Router#show ip mroute pim-dm 224.1.1.1
PIM-DM Multicast Routing Table
Timers: Uptime/Expires
State: Interface state
RPF nbr: RPF neighbor address
(192.168.20.151, 224.1.1.1),      00:00:01 /00:03:29
Incoming interface:
Ethernet2/1 Forwarding 0.0.0.0
Outgoing interface list:
Loopback1  NoInfo 00:03:50 /00:00:00
```

Example3: Display the specified (S,G) in local MRT.

```
Router#show ip mroute pim-dm 224.1.1.1 192.168.20.131
PIM-DM Multicast Routing Table
```

### ***65.1.11 show ip pim-dm neighbor***

To display the PIM-DM neighbor and the selected DR, run the following command:

```
show ip pim-dm neighbor [interface-type interface-number]
```

## Parameter

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Type and ID of the interface, such as Ethernet1/1 and serial 11/0

## Default

None

## Command mode

All modes except the user mode

## Explanation

This command is used to check on which LAN routers PIM-DM or PIM-SM is configured.

## Example

Example 1:

```
Router#show ip pim-dm neighbor
```

```
PIM-DM Neighbor Table
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR	Prior/Mode
192.167.20.132	Ethernet1/1	03:13:34 / 00:00:00	v2	4/D	(DR)
1.1.1.1	Loopback1	03:52:30 / 00:00:00	v2	1/D	(DR)
192.168.20.132	Ethernet2/1	19:35:56 / 00:00:00	v2	1/D	
192.168.20.152	Ethernet2/1	00:00:04 / 00:01:41	v2	1/D	
192.168.20.204	Ethernet2/1	00:00:36 / 00:01:44	v2	20/D	(DR)

Example 2:

```
Router# show ip pim-dm neighbor Ethernet2/1
```

```
PIM-DM Neighbor Table
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR	Prior/Mode
192.168.20.132	Ethernet2/1	19:39:22 / 00:00:00	v2	1/D	
192.168.20.152	Ethernet2/1	00:00:30 / 00:01:15	v2	1/D	
192.168.20.204	Ethernet2/1	00:00:04 / 00:02:16	v2	20/D	(DR)

## Related command

```
ip pim-dm
```



**ip pim-dm dr-priority**

**ip pim-dm hello-interval**

**ip pim version**

**ip pim-dm neighbor-filter**

**show ip pim-dm interface**

### 65.1.12 show ip pim-dm interface

To display the state of the PIM-DM interface, run the following command:

**show ip pim-dm interface [*interface-type* *interface-number*] [*count*][*detail*]**

Parameter

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Type and ID of the interface, such as Ethernet1/1 and serial 11/0

Default

None

Command mode

All modes except the user mode

Explanation

Only the state of the PIM-DM interface can be displayed after this command is run. If the PIM-DM interface is not designated, the information about all PIM-DM interfaces' state will be displayed.

Example 1:

```
Router#show ip pim interface
```

```

address      Interface    Ver/  Nbr   Hello  DR    DR
Mode Count  intvl  Prior
192.167.20.132  Ethernet1/1 v2/D  0     30    4     192.167.20.132
1.1.1.1       Loopback1   v2/D  0     30    1     1.1.1.1
192.168.20.132  Ethernet2/1 v2/D  2     30    1     192.168.20.204

```

Example 2:

```
Router#show ip pim interface Ethernet2/1
```

```

address      Interface    Ver/  Nbr   Hello  DR    DR
Mode Count  intvl  Prior

```

```
192.168.20.132    Ethernet2/1 v2/D 2    30    1    192.168.20.204
```

**Related command****ip pim-dm****ip pim-dm dr-priority****ip pim-dm hello-interval****ip pim version****ip pim-dm neighbor-filter****show ip pim-dm neighbor****65.1.13 show ip rpf pim-dm**

To display how the multicast route conducts the Reverse Path Forwarding (RPF), run the following command:

```
show ip rpf pim-dm source-address
```

**Parameter**

Parameter	Description
<i>source-address</i>	<b>Displays the RFP information of the designated source address.</b>

**Default**

None

**Command mode**

All modes except the user mode

**Explanation**

The PIM-DM protocol can obtain the RPF information from multiple types of routing tables. This command tells you where the RPF information is obtained.

**Example**

```
Router#show ip rpf pim 4.1.1.1
RPF information for (4.1.1.1)
RPF interface: Ethernet2/1
RPF neighbor: 192.168.20.80
RPF route/mask: 192.168.20.0/24
RPF type: unicast
Metric preference: 120
Metric: 1
```

**Related command**

None

## Chapter 66 PIM-SM Configuration Commands

### 66.1 PIM-SM Configuration Commands

#### 66.1.1 *ip pim-sm*

Syntas

**ip pim-sm**

**no ip pim-sm**

Parameter

Default

None

Disable PIM-SM

Command mode

Interface configuration mode

Explanation

To enable PIM-SM function on an interface. You will enable PIM-SM when you configure the routers first in the router interface. You can cancel PIM-SM configuration in the last interface to stop PIM-SM running.

Relevant command

None

#### 66.1.2 *ip pim-sm admin-scope*

To configure the multicast administrator scope, run `ip pim-sm admin-scope gaddr gmask`. The designated multicast address ranges between 239.0.0.0 and 239.255.255.255. This command is configured only on the edge routers which interlace other SZs.

**ip pim-sm admin-scope gaddr gmask**

**no ip pim-sm admin-scope**

Parameter

Name	English prompt	Description
<i>admin-scope</i>	<b>admin-scope – pim-sm administrator scope</b>	<b>Only the C-BSRs and the ZBRs need to be configured to know about the existence of the scope zones. Other routers, including the C-RPs, learn of their existence from Bootstrap messages.</b>
<i>gaddr</i>	<b>A.B.C.D – private group address prefix</b>	<b>239.0.0.0 to 239.255.255.255</b>
<i>gmask</i>	<b>gmask – sz group mask</b>	

### Default value

The global domain is 224.0.0.0/4 by default.

### Command mode

Port configuration mode

### Instruction

This command is configured on the boundary of the PIM-SM administrator scope and used to check the BSM information which is received from the outside of the administrator scope. If the SZ scope of the received BSM information is smaller than or equal to the locally configured administrator scope, the received BSM information will be discarded. Otherwise, the received BSM information will enter the local administrator scope. When the BSM information is forwarded locally, the same principle is followed. At present, Huawei only supports the global domain and the private domain, but does not support the covering of the group address. RP in SZ1 will not notify the global SZ of the C-RP-ADV information. But the global BSM information can get in.

### Example

The following example shows how to configure the boundary scope on routerA to pim-sm sz1(239.1.1.1/24).

```
RouterA_config_f0/0#ip pim-sm admin-scope 239.1.1.1 255.255.255.0
```

```
RouterB_config_ps# c-bsr interface lo1
```

```
RouterB_config_ps# c-bsr admin-scope 239.1.1.1 255.255.255.0
```

### Related command

```
ip pim-sm bsr-border
```

```
c-bsr intf_type intf_name
```

### 66.1.3 ip pim-sm asrt-hold

To configure the holdtime for the assert state on the port corresponding to PIM-SM, run the following command.

```
ip pim-sm asrt-hold intvl
```

```
no ip pim-sm asrt-hold [intvl]
```

### Parameter

Name	English prompt	Description
<i>pim-sm</i>	<b>pim-sm - Enable PIM sparse mode operatioin</b>	<b>The default value is 180 seconds.</b>
<i>asrt-hold</i>	<b>asrt-hold – assert status hold timer</b>	
<i>intvl</i>	<b>&lt;7-65535&gt; - time value (second)</b>	

### Default value

180 seconds

Command mode

Port configuration mode

Instruction

Example

The following example shows how to configure the timeout time in assert state on port f0/0 to 200 seconds.

```
Router_config_f0/0#ip pim-sm holdtimer assert 200
```

#### 66.1.4 ip pim-sm bsr-border

Syntas

**ip pim-sm bsr-border**

**no ip pim-sm bsr-border**

Parameter

Default

None

Non-BSR boundary.

Command mode

Global configuration mode

Explanation

This command can set interface to BSR boundary.in this interface didn't send/receive BSM message ;use "no"command to recovery default .

This command change difinition BSR boundary to make BSM message can not effect each other in different PIM-SM domain.

Relevant command

None

#### 66.1.5 ip pim-sm dr-pri

Syntas

**ip pim-sm dr-pri pri-value**

**no ip pim-sm dr-pri pri-value**

Parameter

Name	English prompt
<i>dr-pri</i>	<b>dr-pri - pim-sm interface DR priority</b>
<i>Pri-value</i>	<b>&lt;0-4294967294&gt; - DR priority, preference given to larger value</b>

**Default**

DR priority is 1 by default in global mode.

**Command mode**

Interface configuration mode

**Explanation**

To change interface DR priority ,use “no”command to recovery default value.

The highest priority routers will be DR.if the priority is same,then the highest address is DR.

**Relevant command**

None

**66.1.6 ip pim-sm hello-intvl****Syntas**

**ip pim-sm hello-intvl** *seconds*

**no pim-sm hello-intvl** [*seconds*]

**Parameter**

Name	English prompt
<i>hello-intvl</i>	hello-intvl- pim-sm hello advertisement interval
<i>seconds</i>	<1-65535> - periodic pim hello message are sent(unit:s)

**Default**

The interval of sending Hello messages is 30s.

**Command mode**

Interface configuration mode

**Explanation**

To configure hello message sending interval ,use “no”command to renew default value.

To change the hold-time of neighbor router, hold-time is 3.5 times of hello message sending interval.

**Relevant command**

None

**66.1.7 ip pim-sm holdtime**

To configure the interval of the hello timer on the PIM-SM port, run the following first command. The value of the interval ranges between 4 and 65535.

**ip pim-sm holdtime** *seconds*

**no pim-sm holdtime** [*seconds*]

## Parameter

Name	English prompt	Remarks
<i>Holdtime</i>	<b>holdtime – keep alive time to neighbor</b>	
<i>seconds</i>	<b>&lt;4-65535&gt; - keep alive time value</b>	

## Default value

105 seconds

## Command mode

Interface configuration mode

## Instruction

This command is first run in port configuration mode and then in global configuration mode, or the default value is chosen. If the value of the holdtime is smaller than that of Hello interval, the configured value is then invalid. The value of the holdtime is  $\text{hello-intvl} * 3.5$ .

## Example

The following example sets the holdtime value to 100 for interface pimsm configuration:

```
Router_config#interface f0/0
```

```
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
```

```
Router_config_f0/0#ip pim-sm holdtime 100
```

## Related command

**ip pim-sm hold-intvl**

**intvl-time hello hlo-intvl**

### 66.1.8 ip pim-sm horizon-split

To configure the horizon split strategy of the BSM packets on a port, run the following first command.

**ip pim-sm horizon-split**

**no ip pim-sm horizon-split**

## Parameter

Name	English prompt	Remarks
<i>horizon-split</i>	<b>Horizon-split – permit interface horizon split</b>	

## Default value

The horizontal split is disabled by default.

## Command mode

Interface configuration mode

## Instruction

After this command takes effect, you can set the corresponding label bit of the PIM-SM port. The BSM packets that are received from a port will not be transmitted from the port.

## Example

The following example sets the DR priority value to 200 for the interface f0/0:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm horizon-split
```

## Related command

### bsm policy

### 66.1.9 ip pim-sm jp-hold

To configure the holdtime for the join-prune state on the port corresponding to PIM-SM, run the following first command.

**ip pim-sm jp-hold *intvl***

**no ip pim-sm jp-hold [*intvl*]**

## Parameter

Name	English prompt	Remarks
<i>pim-sm</i>	<b>pim-sm - Enable PIM sparse mode operation</b>	<b>The default value is 210 seconds.</b>
<i>jp-hold</i>	<b>Join-prune –join-prune status hold timer</b>	
<i>intvl</i>	<b>&lt;1-65535&gt; - time value (second)</b>	

## Default value

210 seconds

## Command mode

Port configuration mode

## Example

The following example shows how to configure the timeout time in join state on port f0/0 to 200 seconds.

```
Router_config_f0/0#ip pim-sm jp-hold 200
```



### 66.1.10 *ip pim-sm jp-intvl*

To set the interval of transmitting the join or prune packets periodically, run the following first command. The interval, whose unit is second, ranges between 1 and 65535.

**ip pim-sm jp-intvl** [*seconds*]

**no ip pim-sm jp-intvl**

Parameter

Name	English prompt	Remarks
<i>pim-sm</i>	<b>pim-sm - Enable PIM sparse mode operation</b>	The default value is 60 seconds.
<i>jp-intvl</i>	<b>jp-intvl – regular Join/Prune message interval (unit:s)</b>	
<i>Seconds</i>	<b>&lt;1-65535&gt; - time value (second)</b>	

Default value

60 seconds

Command mode

Port configuration mode

Instruction

At each configuration the PIM-SM database must be entirely searched for the (*s*, *g*) pairs or the (*\**, *g*) pairs; if the configured port is an upstream one, the interval of the *jp* timer of the corresponding (*s*, *g*) or (*\**, *g*) pair should be reset. The interval in port configuration mode is prior to the **join/prune** interval in global mode. If the **Join** packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast item will be shifted to the **prune** state. The default holdtime is 3 minutes. If this value is changed randomly, CPU shock and service-forwarding shock may be caused.

Example

The following example changes the PIM join message interval to 90 seconds:

```
Router_config_f0/0# ip pim-sm jp-intvl 90
```

Related command

**ip pim-sm jp-hold**

### 66.1.11 *ip pim-sm lan-delay*

To designate the prune delay time of the PIM-SM port, run the following first command.

**ip pim-sm lan-delay** *delay-intvl*

**no pim-sm lan-delay**

Parameter

Name	English prompt	Remarks
<i>lan-delay</i>	<b>lan-delay - pim-sm prune delay</b>	<b>The default value is 500 milliseconds.</b>
<i>delay-intvl</i>	<b>&lt;1-32767&gt; - prune delay time out interval(unit:ms)</b>	

#### Default value

500ms

#### Command mode

Interface configuration mode

#### Instruction

If the local port is the downstream port, the finally calculated prune delay time is based on all maximum values reported by downstream neighbors. In this case, the override timer of transmitting the **join** packets towards the upstream neighbors will be affected. If the **prune\_delay** option is not supported by all downstream neighbors, the default value will be used as the overtime interval of the **prune pending** timer. If the interval of the prune delay timer is locally set, it will be reported to upstream neighbors through the HELLO packets.

#### Example

The following example sets the prune delay value to 200 ms for the pim-sm interface f0/0:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm lan-delay 20
```

#### Related command

**ip pim-sm override**

#### 66.1.12 ip pim-sm nbma-mode

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information. ◦

**ip pim-sm nbma-mode**

**no ip pim-sm nbma-mode**

#### Parameter

Name	English prompt	Remarks
<i>nbma-mode</i>	<b>nbma-mode - Use Non-Broadcast Multi-Access (NBMA) mode on interface</b>	<b>Currently our products do not support this function.</b>

#### Default value

Disable

Command mode

Interface configuration mode

Instruction

Traditional NBMA networks (frame relay, ATM and SMDS) adopt the point-to-multipoint mode; when a sub-node need be pruned, it will report this information directly to the central node and other sub-nodes, however, can not receive this information. In this case, other sub-nodes cannot respond and the interface of the central node will be incorrectly pruned.

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information.

This command cannot be used in multicast LANs, such as Ethernet or FDDI.

Example

The following example configures an interface to be in NBMA mode:

```
Router_config#interface s1/0
```

```
Router_config_s1/0#ip address 10.0.1.2 255.255.255.0
```

```
Router_config_s1/0#ip pim-sm nbma-mode
```

Related command

### 66.1.13 ip pim-sm nbr-filter

To stop a device from being added to PIM, run the following first command; to cancel this function, run the following second command.

```
ip pim-sm nbr-filter acl-name
```

```
no ip pim-sm nbr-filter
```

Parameter

Name	English prompt	Remarks
<i>nbr-filter</i>	<b>nbr-filter - PIM peering filter</b>	
<i>acl-name</i>	<b>WORD – ip stand access list name</b>	

Default value

Disable

Command mode

Interface configuration mode

Instruction

If this command is configured, the neighbors need be filtered when Hello packets are received and then a new neighbor can be created. If it is in deny state, the corresponding new neighbor need not be created. Multiple neighbor access lists can be configured (New CISCO bin only allows to configure a neighbor access list; old bin allows to configure multiple neighbor access lists). Once a neighbor is filtered, the neighbor is then denied.

### Example

The following example shows how to configure stub multicast routing on router A and how router B uses access list 1 to filter all PIM information from router A.

#### Router A Configuration

```
Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.1 255.255.255.0
Router_config#interface f0/1
Router_config_f0/1# ip igmp-helper 10.0.0.2
```

#### Router B Configuration

```
Router_config# ip multicast-routing
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.0.2 255.255.255.0
Router_config_f0/0# ip pim-sm nbr-filter 1
Router_config#ip access-list standard 1
Router_config_std_nacl# deny 10.0.0.1
Router_config_std_nacl# permit any
```

### Related command

**ip pim-sm jp-intvl**

#### 66.1.14 ip pim-sm nbr-track

To forbid the limitation of the JOIN packets globally and enable neighbor tracking, run the following first command:

**ip pim-sm nbr-track**

**no ip pim-sm nbr-track**

### Parameter

Name	English prompt	Remarks
<i>nbr-track</i>	<b>nbr-track - pim-sm interface neighbor tracking</b>	

### Default value

If the global configuration mode is not configured, neighbor tracking is forbidden.

### Command mode

Interface configuration mode

### Instruction

This command is used to forbid the limitation function of the join packets and enable neighbor tracking.

### Example

The following example sets the DR priority value to 200 for the interface f0/0:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm nbr-track
```

### Related command

None

### 66.1.15 ip pim-sm override

To designate the prune deny time of the PIM-SM port, run the following first command.

**ip pim-sm override** *override-intvl*

**no ip pim-sm override**

### Parameter

Name	English prompt	Remarks
<i>override</i>	<b>override - pim-sm override timer</b>	
<i>override-intvl</i>	<b>&lt;1-65535&gt; - override time out interval(unit:100ms)</b>	

### Default value

2.5s

### Command mode

Interface configuration mode

### Instruction

The finally calculated prune deny time is based on the maximum value among all the values reported by all neighbors. If some neighbor does not support prune deny, the default value is selected. If OT is enabled, the value can be random. If the interval of the prune deny timer is locally set, it will be reported to upstream neighbors through the HELLO packets.

### Example

The following example sets the override value to 2000 ms for pim-sm interface f0/0 configuration:

```
Router_config#interface f0/0
Router_config_f0/0#ip address 10.0.1.2 255.255.255.0
Router_config_f0/0#ip pim-sm override 200
```

#### Related command

**ip pim-sm lan-delay**

#### 66.1.16 router pim-sm

To enter the global PIM-SM view, under which there is common attributes, run the following first command:

```
router pim-sm
no router pim-sm
```

#### Parameter

None

#### Default value

The system will not generate the PIM-SM view by default.

#### Command mode

Global configuration mode

#### Instruction

If the router pim-sm command is configured globally or the PIM-SM related configuration is first configured on the port, the global PIM-SM view will be created. If there is some PIM-SM related configuration on the port, the global view cannot be deleted.

#### Example

*The following command shows how to create the global PIM-SM view:*

```
Router_config#router pim-sm
Router_config_ps#
```

#### Related command

**ip pim-sm**

#### 66.1.17 hello-option

To configure in the global PIM-SM view, the global DR priority, the prune delay time, the transmission interval of HELLO packets, the prune deny time, neighbor tracking and neighbor timeout time, run the following command:

```
hello-option { dr-pri pri-value | lan-delay delay-intvl |
override override-intvl | nbr-track | holdtime hold-intvl }
```

**no hello-option [dr-pri | lan-delay | override | nbr-track | holdtime]**

#### Parameter

Name	English prompt	Remarks
<i>dr-pri</i>	<b>dr-pri - pim-sm global DR priority</b>	<b>If this command is not configured, the default DR priority of this process is 1. Configures the prune delay time. Configures the prune deny. The default prune delay time is 500ms. The default prune deny time is 2500ms. If this command is configured, the JOIN packets will not be limited.</b>
<i>pri-value</i>	<b>&lt;0-4294967294&gt; - DR priority, preference given to larger value</b>	
<i>lan-delay</i>	<b>lan-delay - pim-sm prune delay time</b>	
<i>override</i>	<b>Override – override for rcvd prune</b>	
<i>delay-intvl</i>	<b>&lt;0-32767&gt; – value for prune delay</b>	
<i>override-intvl</i>	<b>&lt;0-65535&gt; – value for override delay</b>	
<i>nbr-track</i>	<b>nbr-track – neighbor track enable</b>	

Name	English prompt	Remarks
<i>holdtime</i>	<b>holdtime – neighbor keep alive timer</b>	<b>In normal case, its value is 3.5 times larger than the Hello interval on a port. The default neighbor holdtime is 105 seconds.</b>
<i>hold-intvl</i>	<b>&lt;4-65535&gt; – value for neighbor timeout</b>	

#### Default value

See the table above.

#### Command mode

Global PIM-SM view

#### Instruction

If there is no corresponding configuration items on a port, the globally configured attributes will be used as the corresponding attributes on the port. The change of the global DR priority may affect the new DR selection.

The rules of DR selection are shown below:

1. The highest DR priority on a port will be selected as the DR of the network segment to which this port belongs; if there are many same DR values, the relatively large IP address among the main IP address on the local port and the main IP address of the neighbor will be selected as DR.
2. If there are neighbors on a port or the DR priority is not supported on a port, the relatively large mainaddress will serve as DR.

#### Example

The following example sets the DR priority value to 200 for global pimsm configuration:

```
Router_config#Router pim-sm
Router_config_ps#dr-priority 200
```

### 66.1.18 accept bsm-adv

You can run `accept bsm-adv` in global mode to set the filtration list. The filtration list settings is especially for filtrating specific BSM source addresses and receive the designated BSM source address. To cancel the filtration, you can run `no accept bsm-adv [list std-acl]`.

**accept bsm-adv list std-acl**

**no accept bsm-adv [list std-acl]**

Name	Prompt	Remarks
<i>accept</i>	<b>Accept – configure accept policy</b>	<b>It is used to limit the range of the BSM source address.</b>
<i>bsm-adv</i>	<b>bsm-adv- BSM packet source address accept filter</b>	
<i>list</i>	<b>list- IP access-list for bsm source-list</b>	
<i>std-acl</i>	<b>WORD -- stand access list name</b>	

#### Default value

This filtration is disabled by default.

#### Command mode

pim-sm global view

#### Instruction

Only one filtration command can be set.

#### Example

The following example shows that the BSM notifications only from network segment 192.2.2.0/30 can be received.

```
Router_config#router pim-sm
Router_config_ps#accept bsm-adv list adv-src
Router_config_ps#exit
Router_config#ip access-list stand adv-src
Router_config_std_nacl#permit 192.2.2.0 255.255.255.252
```

### 66.1.19 accept crp-adv

To set the filtration list specially for filtrating the address range of specific groups, limiting to receive the C-RP-ADV packets from specific candidate rp unicast, and specifying the



group address' range in the received packets through ACL. To cancel the filtration, you can run **no accept crp-adv \*.\*.\*.\* [std-acl]**.

**accept crp-adv \*.\*.\*.\* [std-acl]**

**no accept crp-adv \*.\*.\*.\* [std-acl]**

#### Parameter

Name	Prompt	Remarks
<i>accept</i>	<b>Accept – configure accept policy</b>	
<i>c-rp-adv</i>	<b>crp-adv – C-RP-ADV accept filter c</b>	
<i>A.B.C.D</i>	<b>A.B.C.D - IP address of candidate RP for group</b>	
<i>std-acl</i>	<b>WORD – ip stand access-list name for group</b>	

#### Default value

Disable (not filtrating C-RP-ADV from c-rp)

#### Command mode

pim-sm global view

#### Instruction

After this command is set, BSR only processes C-RP-ADV from RP. Additionally, the range of the group address must be allowed by the standard ACL.

#### Example

The following example states that the router will accept c-rp messages RP address is 100.1.1.1 for the multicast group 224.2.2.2:

```
Router_config#router pim-sm
```

```
Router_config_ps#accept crp-adv 100.1.1.1 grp-acl
```

```
Router_config#ip access-list stand grp-acl
```

```
Router_config_std_nacl#permit 224.2.2.2 255.255.255.255
```

#### 66.1.20 accept rp-addr

Run **accept-rp** in global configuration mode to set the filtration list to filter the specific group address range, deciding whether the join/prune of (\*, G) is acceptable and responding to the registration information of specific destination group addresses. To cancel this setting above, run the “no” form of this command.

**accept rp-addr A.B.C.D [std-acl]**

**no accept rp-addr A.B.C.D[std-acl]**

#### Parameter

Name	Prompt	Remarks
<i>accept</i>	<b>Accept – configure accept policy</b> <b>Accept – Configure the policy of packet reception.</b>	<b>If omitting it, the router will process all the PIM-SM message to any group which is mapped to the RP.</b>
<i>rp-addr</i>	<b>rp-addr - RP address accept filter</b> <b>rp-addr – Configure the acceptable RP address filter.</b>	
<i>A.B.C.D</i>	<b>A.B.C.D - IP address of RP for group</b> <b>A.B.C.D – Designate the RP address of a multicast group.</b>	
<i>std-acl</i>	<b>WORD – ip stand access-list name for group</b> <b>WORD – Stands for the standard access list that is used for multicast group filtration.</b>	

### Default value

Disable (All Join, Prune or Register packets will be processed)

### Command mode

pim-sm global view

### Instruction

After this command is set, the router processes only those Join packets which are mapped to the designated RP. Another point deserving attention is that the range of the group address must be allowed by the standard access list. The aggregation point of the corresponding group must be the calculated RP, and when the aggregation point matches up with the RP can the access filtration list be applied. If the group address is denied, RP will reject the Join and Register packets; after the Register packets are received, RP will return a Register Stop packet to the registration packet generator.

This command can be set many times if the **rp-addr** parameters in this command are different. If the RP that the group address is mapped to is not in the configured range, the RP will be denied directly.

### Example

The following example states that the router will accept join or prune messages destined for the RP at address 100.1.1.1 for the multicast group 224.2.2.2:

```
Router_config#router pim-sm
Router_config_ps#accept rp 100.1.1.1 no-ssm-range
Router_config#ip access-list extended no-ssm-range
Router_config_std_nacl#permit 224.2.2.2
%PIM-6-INVALID_RP_JOIN: Received (*, 238.1.1.1) Join from 192.17.20.173 for invalid
```

*RP 1.1.1.1*

```
Router#show ip mroute
```

```
(*, 238.1.1.1), 00:02:52/00:00:07, RP 1.1.1.1, flags: S
```

```
Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list:
```

```
FastEthernet0/0, Forward/Sparse, 00:02:52/00:00:07
```

It can be seen that the previous address, \*.238.1.1.1, ages after the filtration is set.

**66.1.21 accept register**

When the Register range list is set on C-RP, the selection is RP and the PIM-SM Register packet is received, the filtration list should be used to filter the Register packets. In this case, you should run **accept-register**, and if you want to cancel the filtration, run the “no” form of this command.

```
accept register {list ext-acl | route-map map-name}
```

```
no accept register [list ext-acl | route-map map-name]
```

## Parameter

Name	Prompt	Remarks
<i>accept</i>	<b>Accept – configure accept policy</b> <b>Accept – Configure the policy of packet reception.</b>	
<i>register</i>	<b>register - Registers accept filter</b> <b>Register – Stands for the filter of receiving the Register message.</b>	
<i>list</i>	<b>list – access list</b> <b>list – stands for the access list.</b>	
<i>route-map</i>	<b>Route-map – route map</b> <b>route-map – stands for the route map list.</b>	
<i>ext-acl</i>	<b>WORD – IP extend access list name</b> <b>WORD – stands for the name of the extensible IP access control list.</b>	
<i>map-name</i>	<b>WORD – route map name</b> <b>WORD – stands for the name of the route map list.</b>	

## Default value

The access list filtration or the route-map filtration will not be conducted to the Register packets.

## Command mode

```
pim-sm global view
```

### Instruction

This command is used to prevent those unauthenticated data source from sending the Register packets to RP. If an unauthenticated data source sends a Register packet to RP, RP will return a Register Stop packet at once. This command takes effect only on the machine that runs as RP.

### Example

The following example shows how to restrict the RP from allowing sources in the Source Specific Multicast (SSM) range of addresses to register with the RP.

```
Router_config#router pim-sm
Router_config_ps#accept register list no-ssm-range
Router_config#ip access-list extended no-ssm-range
Router_config_std_nacl#deny ip any 232.0.0.0 0.255.255.255
Router_config_std_nacl#permit ip any any
```

### Related command

**reg-src**

#### 66.1.22 anycast-rp

Through configuring **anycast-rp** and the corresponding neighbor address, you can specify the corresponding peer neighbor to share the load of RP. To cancel this setting above, run the “no” form of this command.

```
anycast-rp A.B.C.D nbr *.*.*.*
no anycast-rp A.B.C.D nbr *.*.*.*
```

### Parameter

Name	Prompt	Remarks
<i>anycast-rp</i>	<b>anycast-rp –anycast rp for pim-sm</b>	
<i>A.B.C.D</i>	<b>A.B.C.D – anycast rp address</b>	
<i>nbr</i>	<b>nbr – anycast rp neighbor</b>	
<i>*.*.*.*</i>	<b>A.B.C.D – anycast rp neighbor address</b>	

### Default value

This command takes no effect by default.

### Command mode

```
pim-sm global view
```

### Instruction

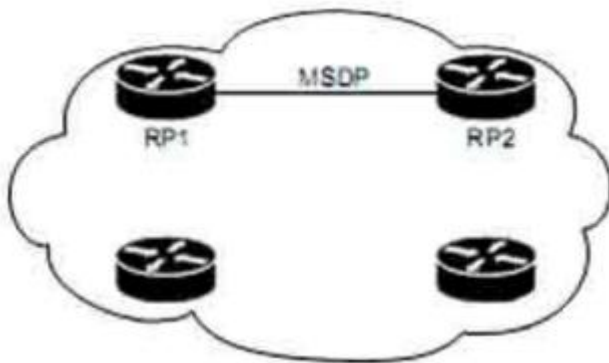
PIM-SM only regulates the standards of the single RP, but a big data flow can cause single RP overload easily. In this case, this command will be used to solve the overload of RP in the PIM-SM domain.

Note:

1. You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the mute terminal router that connects other PIM equipments in the PIM domain through dial-up.
2. If the inside-domain MSDP is not used, the machine that specifies anycast rp must at the same time specify the address of a neighbor with the same RP address so as to facilitate the processing of the register.
3. The command, **anycast-rp A.B.C.D nbr**, is used on those devices that have no MSDP settings and provide an address as the static RP. All peer neighbors need be specified. The neighbors are reachable to one another.
4. If MSDP is set, the device, if it has provided the static RP address, need not specify **anycast rp nbr**.

### Example

1. The following example shows how to set the anycast-rp address when MSDP is used.



RP1:

```
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
/
ip msdp peer 10.1.1.2 connect-source loopback 1
ip msdp originator-id loopback 1
```

RP2:

```
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm Interface loopback 1
ip address 10.1.1.2 255.255.255.255
/
ip msdp peer 10.1.1.1 connect-source loopback 1
ip msdp originator-id loopback 1
```

Designate the static RP address on other devices, for example, do it on router Ra:

Ra:

```
router pim-sm
static-rp 10.0.0.1
```

2. The following example shows how to make settings when the MSDP is not used.

RP1:

```
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm Interface loopback 1
ip address 10.1.1.1 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1
```

RP2:

```
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm Interface loopback 1
ip address 10.1.1.2 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1
```

Designate the static RP address on other devices, for example, do it on router Ra:

Ra:

```
router pim-sm
```

```
static-rp 10.0.0.1
```

Related command

### 66.1.23 reg-rate-limit

As to (s, g), if you want to set the regeneration rate limit of the PIM-SM registration packets per second, you should use the **reg-rate-limit** command; to cancel this settings , you can run **no reg-rate-limit [rate]**.

**reg-rate-limit** *rate*

**no reg-rate-limit** [*rate*]

Parameter

Name	Prompt	Remarks
<i>reg-rate-limit</i>	<b>reg-rate-limit - Rate limit for PIM data registers</b>	
<i>rate</i>	<b>&lt;1-65535&gt; Packets per second</b>	

Default value

The regeneration rate of the registration packets of any (s,g) can be limited to one packet per second.

Command mode

pim-sm global view

Instruction

*This command can be used to limit the regeneration rate of registration packets of (s.g) on the DR router. After this command is enabled, the load of the DR router will be limited. At the initial establishment of multicast path, the sudden eruption of large traffic of the multicast source may lead to packet loss due to the rate limit and the multicast receiver cannot receive all the multicast packets.*

Example

The following example shows how to do the corresponding settings to let each (s.g) generate two registration packets per second.

```
Router_config#router pim-sm
```

```
Router_config_ps#reg-rate-limit 2
```

### 66.1.24 reg-src

To specify an IP address of a port to run as the source address for DR to transmit the PIM-SM registration packets, replacing the default port's address that connects the data source,

run **reg-src**. If you use the **reg-src** command, the specified port must be active. To cancel this settings, you can run **no reg-src** [*intf-type intf-number*].

```
reg-src intf-type intf-number
```

```
no reg-src [intf-type intf-number]
```

#### Parameter

Name	Prompt	Remarks
<i>reg-src</i>	<b>reg-src - Source address for PIM Register</b>	<b>If a port has no main IP address or has no ID, the settings will take no effect. The L3 protocol of a designated port must be up.</b>
<i>intf-type intf-number</i>	<b>Type of the designated port and its name</b>	

#### Default value

By default, the port that connects DR and the data source will be used as the source address of the Register packet to conduct packet encapsulation.

#### Command mode

```
pim-sm global view
```

#### Instruction

When the default source address of the Register packet is not the only routable destination address for RP to return the Register Stop packet, you should use this command to set a new source address for the Register packet. For example, in cases that the source address of the Register packet will be filtered on RP by ACL or the source address is not the only IP address, the Register Stop packet returned by RP may not reach the corresponding DR correctly and then the PIM-SM registration finally may fail.

If the source address of the Register packet is not specified or the specified source address takes no effect, DR will choose the port, which connects the data source, as the source address of the Register packet. Therefore, it is recommended to set for the PIM-SM domain a unique routable address on the loopback port as the source address of the Register packet.

#### Example

The following example shows how to designate the address of the loopback3 port of DR as the source address of the Register packet.

```
Router_config#router pim-sm
```

```
Router_config_ps#reg-src loopback 3
```

#### 66.1.25 spt-threshold

To set the traffic threshold for a flow to switch over to the shortest path tree, run **spt-threshold** in PIM-SM configuration mode. To resume the default settings, run **no spt-threshold**.



```
spt-threshold {infinity/kbps} [stand-acl]
```

```
no spt-threshold
```

#### Parameter

Name	Prompt	Remarks
<i>spt-threshold</i>	<b>spt-threshold - Source-tree switching threshold</b>	
<i>infinity</i>	<b>Infinity - Never switch to source-tree</b>	
<i>kbps</i>	<b>&lt;0-4294967&gt; Traffic rate in kilobits per second</b>	
<i>stand-acl</i>	<b>stand-acl – ip standard access list name for group</b>	

#### Default value

There is no traffic limit for switchover. When the downstream receiver tries to join the data source, the data source will switch over to the SPT forwarding when it receives the data.

#### Command mode

```
pim-sm global view
```

#### Instruction

If the forwarding rate of a multicast source reaches or exceeds the designated threshold, the leaf node will send a (s,g) Join packet to the multicast source for constructing the source tree—the shortest path tree.

If the threshold is set to **infinity**, all multicast sources for the designated group take the sharing tree for packet forwarding. The group access list designates which groups use the configured threshold for SPT switchover. If the message flow from the data source is less than the designated threshold, the PIM-SM router of the leaf node will be switched back to the sharing tree after a period of time and then send the Prune message to the source tree.

#### Example

The following example sets a threshold of 4 kbps, above which traffic to a group from a source will cause the router to router to the shortest path tree to that source:

```
Router_config#router pim-sm
```

```
Router_config_ps# spt-threshold 4
```

#### Related command

None

#### 66.1.26 ssm

To set the range of a specific multicast group, run **ssm {default | range std-acl}**.

To cancel the designated SSM range, run **no ssm**.

```
ssm {default | range std-acl}
```

**no ssm**

## Parameter

Name	Prompt	Remarks
<i>ssm</i>	<b>ssm - Configure Source Specific Multicast</b>	
<i>Default</i>	<b>default - Use 232/8 group range for SSM</b>	
<i>Range</i>	<b>range - ACL for group range to be used for SSM</b>	
<i>std-acl</i>	<b>WORD - ip standard access list name</b>	

## Default value

disable

## Command mode

pim-sm global view

## Instruction

*When PIM-SM is enabled, the default or configured range of the multicast group address can be used. If the multicast group is in the designated SSM range, the locally corresponding (\*,g) must be canceled. This requires the same strategic SSM shall be set in the whole PIM-SM.*

**Note:**

1. The same SSM strategy shall be set in the whole PIM-SM, otherwise the configured SSM will take no effect on preventing (\*,g) Join for IGMPv3 can also specify the addition of (s,g) Join. Additionally, the (\*,g) collision may be caused.
2. PIM-SM cannot be used together with other protocols. The configuration of SSM prevents the transmission of (\*,g) Join and (\*,\*,rp) Join, and the PMBR device cannot send specific (s,g) Join to the upstream devices.
3. After SSM is set, MSDP cannot generate or receive SAs belonging to the designated range of the multicast group address. Our solution is that MSDP notification will be omitted if the group in the (S,G) items of PIM-SM is in the designated SSM group range,.
4. If the group range covers BIDIR group range, the previous configuration will be kept, and display error message to the later(not support now).

## Example

The following example shows how to configure SSM service for the IP address range defined by access list 4:

```
Router_config#router pim-sm
Router_config_ps# ssm range grp_range
Router_config#ip access-list stand grp_range
```

```
Router_config_std_nacl# permit 224.2.151.141
```

### Related command

None

### 66.1.27 c-bsr intf\_type intf\_name

To set a router to be a candidate BSR router, run the first of the following two commands; to cancel this settings, run the second one of the following two commands.

```
c-bsr intf_type intf_name [hash-length [priority]]
```

```
no c-bsr [intf_type][intf_name][hash-length][priority]
```

### Parameter

#### Default value

Dynamic BSR selection is disabled.

#### Command mode

pim-sm global view

### Instruction

After this command is set, the designated address of a port will be used as the BSR address and it will send BSM (bootstrap messages) to all PIM-SM neighbors on the local machine. Each neighbor will compare the previously received BSM with the currently received BSM, and if the BSR address in the current BSM is larger than or equal to that in the previously received BSM, the locally stored BSM will be updated and the current BSM will be forwarded; otherwise, the current BSM will be dropped directly. Before the candidate BSR receives the BSM with higher priority, it always regards itself as the BSM router in the corresponding management domain.

### Note:

1. You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the mute terminal router that connects other PIM equipments in the PIM domain through dial-up.
2. On accepting C-RP-Adv, BSR only accepts those contents that satisfy the SZ range; if the content exceeds the SZ range, it will be omitted.
3. You can specify only one port of a device as the BSR address; if multiple commands are set, the previously configured candidate BSRs will be replaced.
4. The condition for this command to be effective is that the IP address of the designated port is in PIM-SM state and the protocol is up.

### Example

The following example configures the IP address of the router on Ethernet interface 0 to be a candidate BSR with priority of 10:

```
Router_config# router pim-sm
```

```
Router_config_ps# c-bsr f0/0 10 100
```

### Related command

**c-bsr admin-scope {global | gaddr gmask} [hash-length [priority]]**

#### 66.1.28 c-bsr admin-scope

To set a candidate BSR in the administration domain, run the first one of the following two commands.

**c-bsr admin-scope {global | gaddr gmask} [hash-length [priority]]**

**no c-bsr admin-scope**

### Parameter

Name	Prompt	Remarks
<i>c-bsr</i>	<b>c-bsr –Candidate bootstrap router (candidate BSR)</b>	<b>224.0.0.0/255.0.0.0 239.0.0.0 to 239.255.255.255</b>
<i>admin-scope</i>	<b>admin-scope – pim-sm administrator scope</b>	
<i>global</i>	<b>global – global range</b>	
<i>gaddr</i>	<b>gaddr – sz group address</b>	
<i>gmask</i>	<b>gmask – sz group mask</b>	
<i>hash-length</i>	<b>&lt;0-32&gt; - Hash Mask length for RP selection</b>	
<i>Priority</i>	<b>&lt;0-255&gt; - Priority value for candidate bootstrap router</b>	

### Default value

The global domain is 224.0.0.0/4 by default.

### Command mode

pim-sm global view

### Instruction

This command is used to set the candidate BSR in the administration domain. This command corresponds to the **admin-scope** command in the domain boundary and is used to specify the range of the administration domain.

### Note:

1. If the command, c-bsr intf type intf name, is not configured, this command takes no effect.
2. It is recommended to set this command in the administration range (239.0.0.0--239.255.255.255).

### Example

The following example shows that C-BSR only takes effect in the administration domain 239.1.1.0/24:

```
Router_config# router pim-sm
```

```
Router_config_ps#c-bsr f0/0 10 250
```

```
Router_config_ps#c-bsr admoni-scope 239.1.1.1 255.255.255.0
```

Related command

```
c-bsr intf_type intf_name [hash-length [priority]]
```

### 66.1.29 *bsm-policy*

To set the BSM reception policy, run the first one of the following two commands in PIM-SM configuration mode. To resume the default settings, run the other command.

```
bsm-policy { unicast {rcvd | send}| forward-all | backward}
```

```
no bsm-policy { unicast {rcvd | send} | forward-all }
```

Parameter

Name	Prompt	Remarks
<i>bsm</i>	<b>bsm –bsm packet received</b>	<p>The default value allows the reception of the unicast BSM packets.</p> <p>The backward compatibility supports the transmission of unicast BSM.</p> <p>The horizontal division port will not forward all BSM packets, including unicast or no-forward-bit reset packets.</p>
<i>policy</i>	<b>Policy – the policy for BSM receive and forward</b>	
<i>unicast</i>	<b>unicast –unicast bsm packet</b>	
<i>rcvd</i>	<b>rcvd-permit receive bsm message</b>	
<i>forward-all</i>	<b>forward-all – forward all bsm packet</b>	
<i>backward</i>	<b>backward - backwards compatibility support send unicast BSM.</b>	

Default value

There is no BSM reception or transmission policy.

Command mode

pim-sm global view

Instruction

Refer to the description of this command.

Example

The following example configures the local router can receive bsm unicasted from neighbor:

```
Router_config# router pim-sm
```

```
Router_config_ps# bsm-policy unicast rcvd
```

Related command

None

### 66.1.30 static-rp

To set the static RP of PIM-SM, run the first one of the following two commands; to resume the default settings, run the other command.

```
static-rp rp-addr [std-acl] [override][bidir]
```

```
no static-rp rp-addr
```

Parameter

Name	Prompt	Remarks
<i>static</i>	<b>static</b> - configure static rp-address for pim-sm	<b>When static RP goes against dynamic RP, if the parameter is not designated, the dynamic RP will be chosen first, and if no dynamic RP exists or dynamic RP takes no effect can static RP take effect.</b>
<i>rp-addr</i>	<b>A.B.C.D</b> – pim-sm rp-address (Rendezvous Point)	
<i>std-acl</i>	<b>WORD</b> – IP stand access list	
<i>override</i>	<b>override</b> –If conflict,the static rp prevails over the dynamic RP	
<i>bidir</i>	<b>bidir</b> - Group range treated in bidirectional shared-tree mode It is not supported currently.	

Default value

disable

Command mode

pim-sm global view

Instruction

The designated IP address of static RP must be legal unicast address and cannot be the loopback address (127.0.0.0/8). If ACL is designated, the configured static RP will serve the matched multicast group; if ACL is not designated, the configured static RP will serve all multicast groups (224.0.0.0/4). When static RP goes against dynamic RP, the former will be first chosen.

In PIM-SM or BIDIR mode, each group will be provided with an RP. All routers in the same administration domain must follow the identical rule to set RP for the group. RP can be obtained through two mechanisms: static configuration of the RP address or the BSR mechanism's dynamic learning of RP address. The static rp-address command can be used to set an RP to be the aggregation point of multiple groups. The ACL configured by static RP defines the RP application range. If the standard ACL is not set, the designated static RP will be applied to all groups. One PIM router can use multiple RPs, but it can use the only RP for a specific group.

If multiple **static rp-address** commands are set, the matchup rules of group-to-rp are listed below:

1. If a group matches up with multiple static RP rules, suitable RPs can be chosen according to the longest match principle specified by the standard ACL. As to the static configuration without designated ACL, it can be applied to all groups, but the entries in the ACL must be first set.
2. If a group and multiple ACLs accord to the longest match principle, the IP addresses of RPs must be compared and those RPs with big IP addresses come prior in choice.
3. If the static RP configuration is adopted, the reachability test will not be conducted to the designated RP. If an RP is selected, the RP with a comparatively low RP will not be chosen even though the route of the selected RP does not exist locally.
4. Each command can be used to specify a static RP address. If the designated static RP address or ACL rule is same during configuration, the new configuration will replace the previous configurations.

In case static RP and dynamic RP are used together, the rules of group-to-rp are listed below:

1. When the override is not specified, the RPs, dynamically learned through the BSR mechanism, come prior to static RPs.
2. If dynamic RP is used, the **c-rp intf\_type intf\_name** command must be set.

**Note:**

1. The same RP cannot be used simultaneously on BIDIR and PIM-SM.
2. The statically configured RP only supports global SZ or provides support even if global SZ has not yet created.

**Example**

The following example shows how to designate 198.92.37.33 to be the static RP address.

```
Router_config#router pim-sm
Router_config_ps#static-rp 198.92.37.33
```

**Related command**

c-rp intf\_type intf\_name

**66.1.31 c-rp intf\_type intf\_name**

To set a port to be C-RP and to send the unicast notification periodically to a designated BSR router in the PIM-SM domain, run the first one of the following two commands. To resume the default settings, run the other command.

```
c-rp intf-type intf-name [group-list std-acl] [bidir][intvl seconds][pri pri-value]
no c-rp intf-type intf-name
```

**Parameter**

Name	Prompt	Remarks
------	--------	---------

<i>c-rp</i>	<b>c-rp - To be a PIMv2 RP candidate</b>	<b>PIM-SM must be enabled on C-RP. It is the prefix of the group address. It is not supported currently. The smaller the value is, the higher the priority is. The default value is 192.</b>
<i>intf-type intf-name</i>	<b>Designating the interface type and the interface's name</b>	
<i>group-list</i>	<b>group-list – ip access list for group-list</b>	
<i>std-acl</i>	<b>WORD – ip stand access list</b>	
<i>bidir</i>	<b>bidir - Group range treated in bidirectional shared-tree mode</b>	
<i>intvl</i>	<b>Interval - RP candidate advertisement interval</b>	
<i>Seconds</i>	<b>&lt;1-32767&gt; - number of seconds</b>	
<i>pri</i>	<b>pri – RP priority</b>	
<i>pri-value</i>	<b>&lt;0-255&gt; - RP priority value</b>	

### Default value

Dynamic RP selection is disabled.

### Command mode

pim-sm global view

### Instruction

This command is used to notify all BSRs on C-RP. The range of the group address is listed in a form of the standard ACL.

#### Note:

1. PIM-SM must be enabled on the port that serves as C-RP.
2. You'd better set C-RP on the main PIM-SM domain to avoid static configuration on similar routers or the on-demand dialup stub routers.
3. If C-RP is not specified with a multicast group range, C-RP will serve all multicast groups.
4. If you want to set a router to be C-RP for multiple group ranges, you need to represent multiple group ranges with multiple rules when configuring STD-AC1 that group-list corresponds to.
5. One port can only be set to one C-RP and the following configuration will replace the previous configuration, including the replacement of STD-AC1.
6. You can set C-RP for multiple ports on the same PIM-SM router.
7. Multiple C-RPs can use the same standard ACL.
8. If this command is run many times on a same interface, the previous configuration will be replaced.



9. If multiple SZs are known on C-RP, unicast C-RP-Adv will be sent to the BSR of each SZ. It is noted that the established group range cannot exceed the group range of the destination SZ.

10. If C-RP itself is the ZBR of an SZ, the Admin Scope Bit in the C-RP-Adv packet must be reset; otherwise, this bit will not be reset. At present, it is used for BSR to record logs but possible to be used for protocol expansion.

### Example

The following example shows how to designate lo172 and lo173 to be C-RP ports, the former limiting to provide RP to the group of prefix 239.1/16.

```
Router_config#router pim-sm
Router_config_ps# c-rp loopback172 group-list grp-range
Router_config# ip access-list standard grp-range
Router_config_std_nacl# permit 239.1.0.0 255.255.0.0
Router_config_ps# c-rp loopback173
```

### Related command

None

### 66.1.32 intvl-time

To enable the periodical transmission of join/prune packets and set the interval of periodically transmitting the Hello, BSM or C-RP-Adv packets, run the first of the following two commands:

```
intvl-time { join-prune jp-intvl | hello hlo-intvl | c-bsr cbsr-intvl | crp-adv crp-intvl | spt-check [spt-intvl] }
```

```
no intvl-time {join-prune [jp-intvl] | hello [hlo-intvl] | c-bsr[cbsr-intvl] | crp-adv [crp-intvl] | spt-check [spt-intvl] }
```

### Parameter

Name	Prompt	Remarks
<i>join-prune</i>	<b>join-prune - pim-sm regular join/prune packet periodic</b>	The default interval of transmitting Join/Prune packets is 60 seconds. Sets the interval of transmitting the Hello packets. The default interval of transmitting Hello packets is 30 seconds. The default interval of self selecting packets is 60 seconds.
<i>jp-intvl</i>	<1-65535> - value for JP timer	
<i>Hello</i>	<b>hello – pim-sm hello advertisement interval</b>	
<i>hlo-intvl</i>	<1-65535> - value for JP timer	
<i>c-bsr</i>	<b>c-bsr –Candidate bootstrap router (candidate BSR)</b>	
<i>cbsr-intvl</i>	<1-65535> - value for c-bsr timer	
<i>crp-adv</i>	<b>crp-adv – pim-sm C-RP-ADV interval</b>	
<i>crp-intvl</i>	<1-65535> - value for CRP timer	

<i>spt-check</i>	<b>Spt-check – spt switch timer</b>	<b>Sets the interval of transmitting the C-RP-Adv packets. The default interval of transmitting Report packets is 60 seconds.</b>
<i>spt-intvl</i>	<b>&lt;1-65535&gt; - value for spt switch query timer</b>	

### Default value

See the above-mentioned table.

### Command mode

pim-sm global view

### Instruction

If the holdtime of Join-prune packet is not set and the Join packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast entry will be shifted to the prune state. The default holdtime is 3 minutes. The interval in port configuration mode is prior to the join/prune interval in global mode.

### Example

The following example sets the join/prune advertisement interval value to 30 for global pimsm configuration:

```
Router_config#Router pim-sm
Router_config_ps#timer join-prune 30
```

### Related command

holdtime

### 66.1.33 holdtime

To set the interval of the timeout timer of PIM-SM, run the first one of the following two commands. To resume the default settings, run the other command.

```
holdtime {join-prune jp-hold | assert asrt-hold | c-bsr cbsr-hold | crp-adv crp-hold | sz sz-hold}
```

```
no holdtime {join-prune [jp-hold] | assert [asrt-hold] | c-bsr [cbsr-hold] | crp-adv [crp-hold] | sz [sz-hold]}
```

### Parameter

Name	Prompt	Remarks
<i>holdtime</i>	<b>holdtime – hold timer for keep the status</b>	<b>The default value is 210 seconds.</b>
<i>join-prune</i>	<b>Join-prune –join-prune status hold timer</b>	<b>The default value is 180 seconds.</b>

<i>jp-hold</i>	<1-65535> - time value (second)	<p>By default, it is as follows: holdtime timeout time= holdtime's interval*2+10</p> <p>By default, the holdtime's interval is 60 seconds and the holdtime's timeout time is therefore 130 seconds.</p> <p>The default value is 150 seconds.</p> <p>Because non-BSR updates its timeout time through the BSR's holdtime packets, the timeout time of C-RP must not be less than the interval of holdtime packet transmission. It is best when the former is 2.5 intervals or beyond.</p> <p>The default value is 1300 seconds.</p>
<i>assert</i>	assert – assert status hold timer	
<i>asrt-hold</i>	<7-65535> - time value (second)	
<i>c-bsr</i>	c-bsr –Candidate bootstrap router (candidate BSR)	
<i>cbsr-hold</i>	<1-65535> - time value (second)	
<i>c-rp</i>	c-bsr –Candidate bootstrap router (candidate BSR)	
<i>crp-hold</i>	<1-65535> - time value (second)	
<i>sz</i>	sz –scope zone timer	
<i>sz-hold</i>	<10-4294967295> - time value (second)	

### Default value

See the above-mentioned table.

### Command mode

pim-sm global view

### Instruction

If the holdtime is set on a port, first comes the configuration of this port and then the global configuration; finally, if neither configuration is done, the default configuration will be chosen.

### Note:

- When configuring the holdtime of C-RP, you should set the timeout time of C-RP to 2.5 holdtime transmission intervals or beyond to prevent the C-RP loss in the BSR holdtime packet.
- The timeout time of SZ must be longer than the BSR timeout time and you'd better set it to be 10 BSR timeout times.

### Example

The following example shows how to set the holdtime of C-RP to 150 seconds, among which C-RP and C-BSR are not set on Ra.

```
Ra_config# router pim-sm
```

```
Ra_config_ps# holdtime c-rp 200
```

**Related command**

intvl-time

**66.1.34 log**

To enable the log switch to record DR's change, neighbor's up or down, address conflict and abnormal packets, run the first one of the following two commands:

```
log { nbr-change | ipaddr-conflict | pkt-conflict }
```

```
no log { nbr-change | ipaddr-conflict | pkt-conflict }
```

**Parameter**

Name	Prompt	Remarks
<i>Log</i>	<b>log - To log conflict</b>	
<i>nbr-change</i>	<b>nbr-change – neighbor up/down or DR changes</b>	
<i>ipaddr-conflict</i>	<b>ipaddr-conflict –secondary ip address is conflict with the another neighbor</b>	
<i>pkt-conflict</i>	<b>pkt-conflict – pim-sm mroute items conflict in the pimsm pkt</b>	

**Default value**

The log function is disabled.

**Command mode**

pim-sm global view

**Instruction**

If there is the log server, the corresponding logs will be recorded to the log server.

**Example**

The following example configures the router to log the conflict when the exist secondary ip address is also contained in hello packet when received from another neighbor.

```
Router_config_ps# log nbr-change
```

**Related command**

None

**66.1.35 show running-configure**

To display the global PIM-SM information and the main configuration information about a port, run the following command:

```
show running-configure
```

**Parameter**

None

#### Default value

None

#### Command mode

EXEC

#### Instruction

According to the output information, you can check the configuration information about the current PIM-SM.

#### Example

*66.1.36 show ip pim-sm bsr-router*

#### Syntas

```
show ip pim-sm bsr
```

#### Parameter

None

#### Default

None

#### Command mode

Management mode

#### Explanation

Display PIM-SM router BSR message .

#### Example

```
R142#show ip pim-sm bsr-router
```

```
PIMv2 BSR information:
```

```
I am BSR!
```

```
Address of BSR: 192.166.100.142
```

```
BSR Priority: 201 Hash Mask Length: 30 Uptime: 00:10:56
```

```
Next BSM will be sent in 00:00:04
```

```
Candidate-RP: 192.166.100.142(Loopback0)
```

```
Interval of Advertisements: 60 seconds
```

```
Next Advertisement will be sent in 00:00:04
```

#### Relevant command

None

### 66.1.37 show ip pim-sm interface

Syntas

**show ip pim-sm interface** [*type number*]

Parameter

Parameter	Description
<i>type</i>	Port type
<i>number</i>	Port number

Default

None

Command mode

Management mode

Explanation

Display PIM-SM router port information.

Example

```
R142#show ip pim-sm interface
```

```

Address      Interface  Ver/  Nbr  Query  DR DR
Mode Count Intvl  Prior
192.168.21.142 Serial2/0  v2/S  1    30    1    192.168.21.144
192.168.100.142 Ethernet1/1 v2/S  1    30    100  192.168.100.142
192.166.100.142 Loopback0  v2/S  0    30    1    192.166.100.142

```

Relevant command

None

### 66.1.38 show ip pim-sm neighbor

Syntas

**show ip pim-sm neighbor** [*type number*]

Parameter

Parameter	Description
<i>type</i>	Port type
<i>number</i>	Port number

Default

None

Command mode

Management mode

Explanation

Display PIM-SM router neighbor information.

Example

```
R142#show ip pim-sm neighbor
```

PIM Neighbor Table

Neighbor Address	Interface	Uptime/Expires	Ver	DR	Prio
192.168.21.144	Serial2/0	00:03:53/00:01:22	v2		1
192.168.100.143	Ethernet1/1	00:03:34/00:01:41	v2		1

Relevant command

None

*66.1.39 show ip pim-sm rp*

Syntas

**show ip pim-sm rp [mapping|metric]**

Parameter

Parameter	Description
<i>mapping</i>	Displays RP—GROUP mapping relation.
<i>metric</i>	Displays each RP simple-cast route metric.

Default

None

Command mode

Management

Explanation

Display PIM-SM router RP mapping information .

Example

```
R144#show ip pim-sm rp
```

```
GROUP: 225.1.1.10, RP: 9.1.1.1, Version2 Uptime: 1d01h07m, Expires in 00:02:16
```

## Relevant command

None

**66.1.40 show ip pim-sm rp-hash**

## Syntas

**show ip pim-sm rp-hash** [*group-address*]

## Parameter

Parameter	Description
<i>group-address</i>	<b>Group address.</b>

## Default

None

## Command mode

Management mode

## Explanation

Display specify multicast address hash accout value.

## Example

R142#show ip pim-sm rp-hash 225.1.1.10

RP: 192.166.100.142

Info Source: 192.166.100.142, via BSR

Uptime: 00:00:08, Expires: 00:02:22

## Relevant command

None

**66.1.41 show ip mroute pim-sm**

## Syntas

**show ip mroute pim-sm** [*group-address*/*source-address*] [**type number**] [**summary|count**] [*active kbps*]

## Parameter

Parameter	Description
<i>group-address</i>	<b>Group address.</b>
<i>source-address</i>	<b>source-address</b>
<i>type</i>	<b>Port type</b>
<i>number</i>	<b>Port number</b>



<i>summary</i>	<b>Display table PIM-SM entry</b>
<i>count</i>	<b>Display (S,G) stat information</b>
<i>active</i>	<b>Activity sending data speed</b>

**Default**

None

**Command mode**

Management mode

**Explanation**

Display PIM-SM multicast route information.

**Example**

R142#show ip mroute pim-sm

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir group, s - SSM group,  
 I - IGMP report, R - RP-bit set, F - Register flag, T - SPT-bit set,  
 J - Join Needed, P - Pruned,

Timers: Uptime/Expires

(\*, 225.1.1.10), 00:15:14/00:02:37, RP 9.1.1.1, flags: SRJ

Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143

Outgoing interface list:

Serial2/0, Forward/Sparse, 00:13:23/00:02:37

(192.166.1.253, 225.1.1.10), 00:15:14/00:02:46, flags: STJ

Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143

Outgoing interface list:

Serial2/0, Forward/Sparse, 00:15:14/00:02:46

(192.168.20.141, 225.1.1.10), 00:15:14/00:02:46, flags: STJ

Incoming interface: Ethernet1/1, RPF nbr 192.168.100.143

Outgoing interface list:

Serial2/0, Forward/Sparse, 00:15:14/00:02:46

**Relevant command**

None

### 66.1.42 *show ip rpf pim-sm*

Syntas

**show ip rpf pim-sm** {*source-address*} **metric**

Parameter

Parameter	Description
<i>source-address</i>	Source address.
<i>metric</i>	Simple-cast route Metric

Default

None

Command mode

Management mode

Explanation

Display specify source address converse forwarding information.

Example

```
R142#show ip rpf pim-sm 192.166.1.143
```

```
RPF information for 192.166.1.143
```

```
RPF interface: Ethernet1/1
```

```
RPF neighbor: 192.168.100.143
```

```
RPF route/mask: 192.166.1.0/24
```

```
RPF type: unicast (rip)
```

```
RPF recursion count: 0
```

```
Doing distance-preferred lookups across tables
```

Relevant command

None

### 66.1.43 *debug ip pim-sm alert*

To display the alert information from mrouting or IP, run the first one of the following two commands.

**debug ip pim-sm alert**

**no debug ip pim-sm alert**

Parameter

None

**Default value**

None

**Command mode**

EXEC

**Instruction**

VTY will be exported if the alert information from mrouting or aged (s,g).

**Example**

The following example shows that the route event of RIP is monitored.

```
router# debug ip rip database
```

```
RIP-DB: Adding summary route 192.1.1.0/24 <metric 0> to RIP database
```

The fields in the previous example are explained in the following table:

Domain	Description
<i>summary</i>	<b>Route type which is added to the routing table</b>
<i>192.1.1.0/24</i>	<b>Route which is added to the routing table</b>
<i>&lt;metric 0&gt;</i>	<b>Value of the route's metric</b>

**66.1.44 debug ip pim-sm assert**

To monitor the Assert event of PIM-SM, run the first one of the following two commands:

```
debug ip pim-sm assert [packet | state- machine | A.B.C.D ]
```

```
no debug ip pim-sm assert [packet | state- machine | A.B.C.D ]
```

**Parameter**

Name	Prompt	Remarks
<i>state- machine</i>	<b>Show state machine activity debug information</b>	
<i>packet</i>	<b>Trace information about packet</b>	
<i>A.B.C.D</i>	<b>Group address for stm and packet output</b>	

**Default value**

None

**Command mode**

EXEC

**Instruction**

According to the output information, you can check the current assert event of PIM-SM.

## Result

- Show (S,G) Assert State-machine Actions
- Show (\*,G) Assert Message State Machine actions
- Show activity after timer timeout
- Show packet activity

### 66.1.45 debug ip pim-sm bsr

To monitor the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine, run the first one of the following two commands:

```
debug ip pim-sm assert [packet | state- machine]
```

```
no debug ip pim-sm assert [packet | state- machine]
```

## Parameter

Name	Prompt	Remarks
<i>state- machine</i>	<b>Show state machine activity debug information</b>	
<i>packet</i>	<b>Trace information about packet</b>	

## Default value

None

## Command mode

EXEC

## Instruction

According to the output information, you can check the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine.

## Example

### 66.1.46 debug ip pim-sm rp

To monitor the related events and packets about PIM-SM-RP-SET change, run the first one of the following two commands:

```
debug ip pim-sm rp
```

```
no debug ip pim-sm rp
```

## Parameter

None

## Default value

None

**Command mode**

EXEC

**Instruction**

This command is used to export the reception and transmission of C-RP-ADV and the RP-SET change. As to the change of static RP, no debugging information will be exported at present.

**Example****66.1.47 debug ip pim-sm entry**

To export the creation and update of (\*,\*,rp), (\*,g), (s,g,rpt) and (s,g,spt) and their simultaneous change of them at the time of RP change, run the first one of the following two commands.

**debug ip pim-sm entry****no debug ip pim-sm entry****Parameter**

None

**Default value**

None

**Command mode**

EXEC

**Instruction**

According to the output information, you can browse the information about PIMSM creation and update of multicast routing entries.

**Example****4.1.48 debug ip pim-sm event**

To export all events that PIMSM main task receives, run the first one of the following two commands.

**debug ip pim-sm event****no debug ip pim-sm event****Parameter**

None

**Default value**

None

**Command mode**

EXEC

**Instruction**

According to the output information, you can browse all events of current PIMSM.

## Example

### 66.1.49 debug ip pim-sm hello

To display the Hello packet received or transmitted by PIM-SM for debugging the neighbor's information, run the first one of the following two commands.

**debug ip pim-sm hello**

**no debug ip pim-sm hello**

#### Parameter

Name	Prompt	Remarks
<i>pim-sm</i>	Show state machine activity debug information	
<i>hello</i>	Show information about packet sending and receiving	

#### Default value

None

#### Command mode

EXEC

#### Instruction

According to the output information, you can browse the Hello packets, including those received or transmitted by PIM-SM, to know what's going on the local machine or the neighbors.

#### Results

- The ports, source addresses and genid of the currently received or transmitted Hello packets can be displayed.

## Example

### 66.1.50 debug ip pim-sm jp

To trace the Join/Prune event of (\*,g) or (s,g), run the first one of the following two commands.

**debug ip pim-sm jp** [packet | state- machine | A.B.C.D ]

**no debug ip pim-sm jp** [packet | state- machine | A.B.C.D ]

#### Parameter

Name	Prompt	Remarks
<i>state- machine</i>	Show state machine activity debug information	
<i>packet</i>	Trace information about packet	
<i>A.B.C.D</i>	Group address for stm and packet output	

**Default value**

None

**Command mode**

EXEC

**Instruction****Example*****66.1.51 debug ip pim-sm nbr***

To trace the related events of a neighbor, such as the addition of neighbor, aging deletion or DR selection, run the first one of the following two commands.

**debug ip pim-sm nbr****no debug ip pim-sm nbr****Parameter**

None

**Default value**

None

**Command mode**

EXEC

**Instruction**

According to the output information of this command, you can browse neighbor change, neighbor refreshment, GENID change and DR selection.

**Example*****66.1.52 debug ip pim-sm packet***

To trace the protocol control packets received or transmitted by PIM-SM, run the following command.

**debug ip pim-sm packet****Parameter**

None

**Default value**

None

**Command mode**

EXEC

**Instruction**

After this command is run, the PIM-SM packet's type will be displayed.

### Example

#### 66.1.53 *debug ip pim-sm register*

To display the registration packet and register state event of PIM-SM, run the first one of the following two commands.

**debug ip pim-sm register** [packet | state- machine | A.B.C.D ]

**no debug ip pim-sm register** [packet | state- machine | A.B.C.D ]

### Parameter

Name	Prompt	Remarks
<i>state- machine</i>	Show state machine activity debug information	
<i>packet</i>	Trace information about packet	
<i>A.B.C.D</i>	Group address for stm and packet output	

### Default value

None

### Command mode

EXEC

### Instruction

According to the output information, you can check the register event of PIM-SM.

### Example

#### 66.1.54 *debug ip pim-sm timer*

To display the change of all PIM-SM timers, including creation, deletion, stop and timeout, run the first one of the following two commands.

**debug ip pim-sm timer**

**no debug ip pim-sm timer**

### Parameter

None

### Default value

None

### Command mode

EXEC

### Instruction

The PIM-SM timers include the Hello timer, the neighbor timeout timer, the Join/Prune timer, the override timer, the prune pending timer, the keepalive timer, the assert timer, the register timer, the register limit timer, the BSM timer, and so on.

### Example



## Chapter 67 Multicast VPN Settings

The MVPN functionality is supported on the routers.

### 67.1.1 *ip multicast-routing vrf vpn-instance-name*

To enable the multicast on VRF, run the following command:

```
ip multicast-routing vrf vpn-instance-name
```

Parameter

Parameter	Description
<i>vpn-instance-name</i>	Enables the VPN instance of multicast.

Default value

None

Command mode

EXEC mode

Instruction

After this command is run, the system enters the MVPN configuration mode.

If you run the “no” form of this command, the related VPN multicast will be disabled.

Example

The following example shows how to enable the multicast on VRF.

```
R4_config#ip multicast-r vrf RED
```

```
R4_config_mvpn_(RED)#
```

Related command

```
ip vrf vpn-instance
```

Before enabling the VPN multicast, you have to configure related VPN.

### 67.1.2 *mdt share-group group-address binding mtunnel number*

To designate the share group address of this VPN multicast and the bound Mtunnel ID, run the following command:

```
mdt share-group 232.1.1.1 binding mtunnel 0
```

Parameter

Parameter	Description
<i>Number</i>	Stands for the Mtunnel ID, which is an indispensable parameter and disabled by default. One Mtunnel is bound to only one MVPN.
<i>group-address</i>	Stands for the share group's address, which is an indispensable parameter and disabled by default.

**Default value**

None

**Command mode**

MVPN configuration mode

**Instruction**

This command can be regarded as the switch of global MVPN.

If you want to cancel the share-group settings and the Mtunnel binding, you shall run **no mdt share-group**.

Before you want to modify the share group's address or bind other Mtunnel, you have to cancel the previous binding through the **no mdt share-group** command.

**Example**

The following example shows how to set the share group and bind Mtunnel.

```
R4_config_mvpn_(RED)#mdt share-group 232.1.1.1 binding mtunnel 0
```

**Related command****67.1.3 mdt connect-src interface**

To designate the connect-source address of VPN multicast, run the following command:

```
mdt connect-src interface
```

**Parameter**

Parameter	Description
<i>Interface</i>	<b>Stands for the currently existent port, such as loopback0.</b>

**Default value**

None

**Command mode**

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

**Instruction**

This command can be used to bind the address of the Mtunnel port. When the Mtunnel obtains its binding address, the Mtunnel is up and then receives or transmits the packets.

It is recommended that the Mtunnel address should be the same as the connect-src address of BGP and that the loopback port should be used as the binding port of Mtunnel.

**Example**

以下示例将 loopback0 指定为该 mvpn 的绑定地址

```
R4_config_mvpn_(RED)#mdt connect-src loopback0
```

## Related command

### 67.1.4 mdt switch-group-pool group-address group-mask threshold

To designate the range of the switch pool, run the following command:

```
mdt switch-group-pool 238.1.1.1 255.255.255.0 threshold number
```

## Parameter

Parameter	Description
<i>number</i>	Designates the value of threshold, whose unit is packet/second. The default threshold is 10 packets/second.
<i>Group-address group-mask</i>	Designates a switch pool on the condition that the group mask must be between 225.225.225.0 and 225.255.255.255.

## Default value

None

## Command mode

MVPN configuration mode, which can be entered through the ip multicast-routing vrf vpn-instance command

## Instruction

This command is used to designate the range of the switch pool and then the switch pool is used for data MDT switchover.

## Example

The following example shows how to designate 238.1.1.1/24 as the switch pool and how to set the switchover threshold to 10 packets/second.

```
R4_config_mvpn_(RED)#-group-pool 238.1.1.1 255.255.255.0 threshold 10
```

## Related command

### 67.1.5 mdt mdt switch-delay

To set how long the system switches over to data MDT after the switchover conditions are ready and the JointLV packet is transmitted, run the following command:

```
mdt mdt switch-delay number
```

## Parameter

Parameter	Description
<i>Number</i>	INTEGER<3-60> Value of multicast-domain switch-delay(second)

**Default value**

5 seconds

**Command mode**

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

**Instruction**

This command is used to designate the switchover time of data MDT.

**Example**

The following example shows how to set the switchover time to 4 seconds.

```
R4_config_mvpn_(RED)#mdt switch-delay 4
```

**Related command****67.1.6 mdt hold-down**

To designate the hold-down timer of data MDT, run the following command.

```
mdt hold-down number
```

**Parameter**

Parameter	Description
<i>Number</i>	<b>INTEGER&lt;0-180&gt; Value of multicast-domain holddown-time(second)</b>

**Default value**

60 seconds

**Command mode**

MVPN configuration mode, which can be entered through the ip **multicast-routing vrf vpn-instance** command

**Instruction**

This command is used to designate the hold-down time of data MDT to prevent the twitter. Before the hold-down time times out, the data MTD mapping cannot be deleted.

**Example**

The following example shows how to set the hold-down time to 70 seconds.

```
R4_config_mvpn_(RED)#mdt holddown-time 70
```

**Related command****67.1.7 mdt rd-list**

To set the RD of the peer VRF, run the following command:

**mdt rd-list rd**

## Parameter

Parameter	Description
<i>rd</i>	ASN:nn or IP-address:nn -- VPN Route Distinguisher

## Default value

None

## Command mode

MVPN configuration mode, which can be entered through the `ip multicast-routing vrf vpn-instance` command

## Instruction

## Example

The following example shows how to make settings to enable VRF RED to accept the multicast flow of VRF BLUE.

```
ip vrf RED
```

```
rd 100:1
```

```
ip vrf BLUE
```

```
rd 200:1
```

```
R4_config_mvpn_(RED)#mdt rd-list 200:1
```

## Related command

*67.1.8 show ip mroute vrf vpn-instance pim-s jointlv*

To browse the Join Tlv options of VPN, run this command.

## Parameter

Parameter	Description
<i>Vpn-instance</i>	Browses the name of VPN instance.

## Default value

None

## Command mode

## Instruction

## Example

```
R4#show ip mroute vrf RED pim-s joint
```

```
(1.1.1.160 239.1.1.1) p sg:(10.0.1.1 232.2.1.1) couter:0 flag:R
```

```
mi:00:00:00 dd:00:00:00 hd:00:00:00 dt:00:02:51
```

In this example, psg stands for the sg address peer encapsulated by the public network, flag stands for the local distribution when it is a, or the remote distribution if it is r.

The second line shows 4 related timers.

## Related command

### 67.1.9 debug ip pim-s mvpn

To trace the events related to MVPN and PIM-SM, run `debug ip pim-s mvpn`. To resume this default settings, run `no debug ip pim-s mvpn`.

## Parameter

Parameter	Description
None	

## Default value

None

## Command mode

## Instruction

## Example

```
R4#show ip mroute vrf RED pim-s joinatb
```

```
(20.0.4.4 232.1.1.1) assigner:0.0.0.0 proxy:172.16.34.4
```

```
atb_t:00:00:00 rd: 100:1
```

In this example, the assigner address is the address of the JINATB releaser. If the assigner address is 0.0.0.0, it means the local distribution.

The proxy address stands for the agent address for this flow to send the Join packet. If it is the remote distribution, atb\_t will time out.

## Related command

### 67.1.10 debug ip multicast mvpn

To trace and observe the MVPN-related events, run this command.

## Parameter

Parameter	Description
None	

## Chapter 68 BVSS Configuration Commands affects ONLY PXT-S2790G/2795G or Higher

Virtualization technology is a centralized management port extension technology. Users can connect virtualization-enabled switches to virtual devices using virtualized ports and cables. Virtualization has the following advantages:

- 1) The port density can be extended by virtualization, because the number of ports of the virtualized device are obtained by adding the ports of all member devices in the virtual domain, and all ports can be regarded as the ports of one device.
- 2) Convenient user management operations. By virtualizing users, a group of switches can be managed as a logical object through an IP, reducing the occupation of IP addresses and facilitating management.
- 3) Expand the uplink bandwidth. Virtualization management is used to manage the virtualization function configuration and operational status. The user needs to enable the virtualization function of the virtualization enabled switch. After the virtualization configuration is complete, you need to restart the device for the virtualization function to take effect.

### 68.1.1 BVSS mode NORMAL

ONLY two nodes in one stack



**Configuration example for PXT-S2790G:**

**#member-1:**

```

bvss enable
bvss domain 1
bvss member 1
bvss mode normal
bvss priority 200
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2

```

**#member-2:**

```

bvss enable

```

```
bvss domain 1
bvss member 2
bvss mode normal
bvss priority 100
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
```

#### **Configuration example for PXT-S2795G:**

##### **#member-1:**

```
bvss enable
bvss domain 1
bvss member 1
bvss mode normal
bvss priority 200
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
write bvss-config
reboot
```

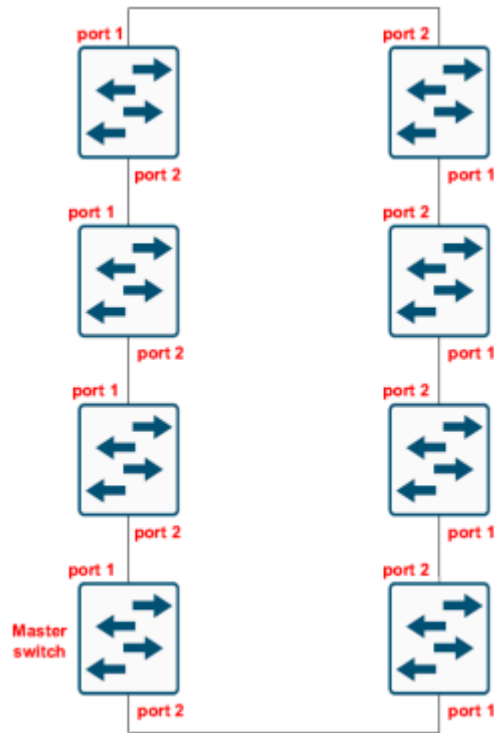
##### **#member-2:**

```
bvss enable
bvss domain 1
bvss member 2
bvss mode normal
bvss priority 100
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
write bvss-config
reboot
```

#### **68.1.1 BVSS mode ENHANCED**

**MAXIMUM eight nodes in one stack**





**Configuration example for PXT-S2790G:**

**#member-1:**

```
bvss enable
bvss domain 1
bvss member 1
bvss mode enhanced
bvss priority 200
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

**#member-2:**

```
bvss enable
bvss domain 1
bvss member 2
bvss mode enhanced
bvss priority 199
bvss interface 1 slot 0 port 1 group 1
```

```
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

**#member-3:**

```
bvss enable
bvss domain 1
bvss member 3
bvss mode enhanced
bvss priority 198
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

**#member-4:**

```
bvss enable
bvss domain 1
bvss member 4
bvss mode enhanced
bvss priority 197
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

**#member-5:**

```
bvss enable
bvss domain 1
bvss member 5
bvss mode enhanced
bvss priority 196
```

```
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

**#member-6:**

```
bvss enable
bvss domain 1
bvss member 6
bvss mode enhanced
bvss priority 195
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

**#member-7:**

```
bvss enable
bvss domain 1
bvss member 7
bvss mode enhanced
bvss priority 194
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

**#member-8:**

```
bvss enable
bvss domain 1
bvss member 8
bvss mode enhanced
```

```
bvss priority 193
bvss interface 1 slot 0 port 1 group 1
bvss interface 2 slot 0 port 2 group 2
write bvss-config
reboot
```

### **Configuration example for PXT-S2795G**

**bvss configuration is the same except interfaces:**

**#member-1:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

**#member-2:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

**#member-3:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

**#member-4:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

**#member-5:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

**#member-6:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

**#member-7:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

**#member-8:**

```
bvss interface 1 type TGigaEthernet port 1 group 1
bvss interface 2 type TGigaEthernet port 2 group 2
```

### **67.1.6 BVSS stack operation commands**

#### **BVSS stack reboot**

To reboot the whole BVSS stack, execute the following command:

**redundancy reload shelf**

#### **Example**

This example shows how to reboot the whole stack.

```
switch_A_config#redundancy reload shelf
```

To reboot peer in stack, execute the following command:

**redundancy reload peer**

#### **Example**

This example shows how to reboot the whole stack.

```
switch_A_config#redundancy reload peer
```

#### **BVSS stack switchover**

To initialize a switchover, execute the following command:

```
redundancy switchover
```

#### **Example**

This example shows how to switchover:

```
switch_A_config#redundancy switchover
```

#### **BVSS stack upgrade**

To initialize a upgrade of the whole stack, the procedure is the following:

- 1) Update the firmware of master node first , with the command "**copy tftp:XXX.bin flash:switch.bin**"
- 2) Update the firmware of slave devices, with the command "**update switch switch.bin**"
- 3) reboot the whole vss system by command "**redundancy reload shelf**"

### 68.1.8 show BVSS stack

Description

**show bvss**

Parameter

Parameter	Description
<i>current-config</i>	Current bvss configuration
<i>running-config</i>	Running bvss configuration
<i>management</i>	Current bvss running information
<i>mcpath</i>	Nounicast running information
<i>rnp</i>	Show rnp info
<i>sgnp</i>	Show sgnp info
<i>statistics</i>	Statistics information
<i>tmp</i>	Show tmp info

Example

This example shows the current configuration of BVSS stack:

```
switch_A#show bvss current-config
```

bvss configuration information:

bvss enable: TRUE

bvss domain-id: 1

bvss member-id : 1

bvss mode: enhanced

bvss priority: 200

bvss vlan: 4094

bvss mac-address mode: use-active-member

This example shows the running configuration of BVSS stack:

```
switch_A#show bvss running-config
```

bvss configuration information:

bvss enable: TRUE

bvss domain-id: 1

bvss member-id : 1

```
bvss mode: enhanced
bvss priority: 200
bvss vlan: 4094
bvss mac-address mode: use-active-member
```

**This example shows the current BVSS running information:**

**switch\_A#show bvss management**

```
bvss member 1 management information:
active member: 1, standby member: 2
lgroup: 1, rgroup: 2
internal topology:0 , global topology: LOOP-TOPO
```

**This example shows the BVSS Nonunicast running information:**

**switch\_A#show bvss mcpath**

```
nonunicast information:
mcpath_set[l]: ,mcpath_set[r]:
mcpath_cur[l]:0 ,mcpath_cur[r]:0
mc internal topo:0
HTmc:0
NLNS path type:0, magic:1
```

**This example shows the BVSS rnp information:**

**switch\_A##show bvss rnp**

```
RNP is running. CfgPri 200, SwitchType 0x115a, Slot 0
System started, ignoreTimeoutCnt 0
DomainId 111, MemberId 1, LoopTopology 0, Merge 0, Master State
MasterMemId 1, BackupMemId 2, MasterGlbMacAddr
5894.8000.cd8b
OldMasterMemberId 0, OldMasterWhile 0, txAdvPduCnt 766146
lacpMad: OldActiveId 0, OldActiveWhile 0, ActiveWhile 0
bvss link group 1 is usable, bvss link group 2 is usable.
```

Pri info for member 1 (SwitchType 115a, slot 0):

Priority 200, RunningTime 1915469, MAC 5894.8000.cd8b

Pri info for member 2 (SwitchType 1171, slot 0):

Priority 199, RunningTime 1915299, MAC 5894.8001.3e62

Pri info for member 3 (SwitchType 115a, slot 0):

Priority 198, RunningTime 1915462, MAC 5894.8000.cd51

Pri info for member 4 (SwitchType 115a, slot 0):

Priority 197, RunningTime 1915461, MAC 5894.8000.cbd8

Pri info for member 5 (SwitchType 1171, slot 0):

Priority 196, RunningTime 1915461, MAC 5894.8001.3e9c

Pri info for member 6 (SwitchType 115a, slot 0):

Priority 195, RunningTime 1915461, MAC 5894.8000.cbf5

Pri info for member 7 (SwitchType 115a, slot 0):

Priority 194, RunningTime 1915461, MAC 5894.8000.cc69

Pri info for member 8 (SwitchType 1171, slot 0):

Priority 193, RunningTime 1915462, MAC 5894.8001.3e7f

**This example shows the BVSS sgnp information:**

**switch\_A#show bvss sgnp**

SGNP is running, Running Time 1915544, NeighbourTimeout 3, Started TMP

bvss Role notified, System started, ignoreTimeoutCnt 3830886

DomainId 111, MemberId 1, bvss Mode 3, LoopTopology 0

MAC Addr:5894.8000.cd8b, portMap:1-2

bvss link group info for group 1:



cfgMemberPt: 1; validMemberPt: 1

peerMemberId 2, peerGroupId 2

bvss link group info for group 2:

cfgMemberPt: 2; validMemberPt: 2

peerMemberId 8, peerGroupId 1

bvss port info for port 1:

tg2/0/2 slotId 0, groupId 1, peerPortId 2, peerSlotId 0, peerGroupId 2

bvss port info for port 2:

tg8/0/1 slotId 0, groupId 2, peerPortId 1, peerSlotId 0, peerGroupId 1

**This example shows the BVSS statistics:**

**switch\_A#show bvss statistics**

bvss statistics information:

topo change:5, errParam:0

messageSendFailed:0, cfgUncompleted:0

notifyGroupChange:4, GroupChangeErrParam:0

notifyMCPPath:0, MCPPathErrParam:0

phyServiceErr:3

**This example shows the BVSS tmp informmation:**

**switch\_A#show bvss tmp**

TMP is running. Started RNP

DomainId 111, MemberId 1, StackingMode 3, LoopTopology 1, Stable State

SL group 1 is usable, SL group 2 is usable.

SIGroup MemberId Distance

-----

1      2      1

1      3      2

1      4      3

1	5	4
1	6	5
1	7	6
1	8	7
2	2	7
2	3	6
2	4	5
2	5	4
2	6	3
2	7	2
2	8	1