



CLI Reference

ZEQUO 5410DL

Model Number: PN88162C

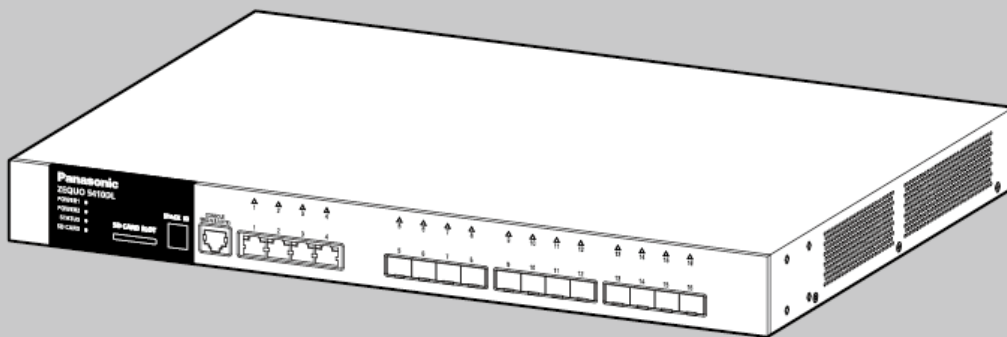


Table of Contents

1	Introduction	1
1.1	Overview.....	2
1.2	User (Privilege) Levels.....	2
1.3	CLI Command Modes	4
1.4	Accessing the CLI.....	7
1.5	CLI Command Conventions.....	8
1.6	Editing Features	8
1.7	Interface Naming Conventions.....	12
1.8	IPv6z Address Conventions.....	14
2	ACL Commands.....	15
2.1	ip access-list (IP extended)	15
2.2	permit (IP).....	16
2.3	deny (IP)	19
2.4	ipv6 access-list (IPv6 extended).....	22
2.5	permit (IPv6)	23
2.6	deny (IPv6)	26
2.7	mac access-list.....	29
2.8	permit (MAC)	30
2.9	deny (MAC)	32
2.10	access-group in.....	34
2.11	access-group out.....	36
2.12	time-range	37
2.13	absolute	39
2.14	periodic	40
2.15	show time-range.....	42
2.16	show access-list	43
2.17	clear access-list counters.....	44
2.18	show interfaces access-list trapped packets	45
2.19	ip access-list (IP standard).....	46
2.20	ipv6 access-list (IP standard).....	48
3	Address Table Commands	50
3.1	bridge multicast filtering	50
3.2	bridge multicast mode.....	51
3.3	bridge multicast address.....	53
3.4	bridge multicast forbidden address	55
3.5	bridge multicast ip-address	57
3.6	bridge multicast forbidden ip-address	59
3.7	bridge multicast source group	60
3.8	bridge multicast forbidden source group	62
3.9	bridge multicast ipv6 mode.....	64

3.10	bridge multicast ipv6 ip-address	66
3.11	bridge multicast ipv6 forbidden ip-address	68
3.12	bridge multicast ipv6 source group.....	70
3.13	bridge multicast ipv6 forbidden source group	71
3.14	bridge multicast unregistered.....	73
3.15	bridge multicast forward-all	74
3.16	bridge multicast forbidden forward-all.....	75
3.17	bridge unicast unknown.....	76
3.18	show bridge unicast unknown	77
3.19	mac address-table static	78
3.20	clear mac address-table	80
3.21	mac address-table aging-time.....	81
3.22	port security	82
3.23	port security mode.....	84
3.24	port security max	86
3.25	show mac address-table	87
3.26	show mac address-table count	89
3.27	show bridge multicast mode	90
3.28	show bridge multicast address-table	91
3.29	show bridge multicast address-table static	94
3.30	show bridge multicast filtering.....	96
3.31	show bridge multicast unregistered	97
3.32	show ports security	98
3.33	show ports security addresses	99
3.34	bridge multicast reserved-address.....	100
3.35	show bridge multicast reserved-addresses.....	102
4	Authentication, Authorization and Accounting.....	103
4.1	password.....	103
4.2	enable password.....	104
4.3	service password-recovery	106
4.4	username.....	107
4.5	show users accounts.....	109
4.6	passwords complexity enable.....	110
4.7	passwords complexity	112
4.8	passwords aging	114
4.9	show passwords configuration	115
5	Auto-Update and Auto-Configuration.....	116
5.1	boot host auto-config	116
5.2	boot host auto-update.....	118
5.3	show boot.....	120
5.4	ip dhcp tftp-server ip address	121
5.5	ip dhcp tftp-server file.....	122

5.6	ip dhcp tftp-server image file	123
5.7	show ip dhcp tftp-server.....	124
6	Clock Commands	125
6.1	absolute	125
6.2	clock dhcp timezone	126
6.3	clock set	126
6.4	clock source	128
6.5	clock summer-time	129
6.6	clock timezone	131
6.7	periodic	132
6.8	sntp anycast client enable.....	134
6.9	sntp authenticate	135
6.10	sntp authentication-key	136
6.11	sntp broadcast client enable	137
6.12	sntp client enable	138
6.13	sntp client enable (interface)	139
6.14	sntp server.....	140
6.15	sntp source-interface.....	141
6.16	sntp source-interface-ipv6.....	142
6.17	sntp trusted-key	143
6.18	sntp unicast client enable	144
6.19	sntp unicast client poll.....	145
6.20	show clock.....	146
6.21	show sntp configuration.....	147
6.22	show sntp status	149
6.23	show time-range.....	151
6.24	time-range	152
7	DHCP Relay Commands	153
7.1	ip dhcp relay enable (Global)	153
7.2	ip dhcp relay enable (Interface)	154
7.3	ip dhcp relay address (Global)	155
7.4	show ip dhcp relay.....	156
7.5	ip dhcp information option.....	158
7.6	show ip dhcp information option	159
8	DHCP Server Commands	160
8.1	address (DHCP Host).....	160
8.2	address (DHCP Network)	162
8.3	clear ip dhcp binding.....	163
8.4	client-name.....	164
8.5	default-router	165
8.6	dns-server.....	166
8.7	domain-name.....	167

8.8	ip dhcp excluded-address	168
8.9	ip dhcp pool host.....	169
8.10	ip dhcp pool network	170
8.11	ip dhcp server	171
8.12	lease.....	172
8.13	netbios-name-server.....	174
8.14	netbios-node-type	175
8.15	next-server	176
8.16	next-server-name	177
8.17	option.....	178
8.18	show ip dhcp	180
8.19	show ip dhcp allocated	181
8.20	show ip dhcp binding	183
8.21	show ip dhcp declined	185
8.22	show ip dhcp excluded-addresses	186
8.23	show ip dhcp expired.....	187
8.24	show ip dhcp pool host	188
8.25	show ip dhcp pool network.....	190
8.26	show ip dhcp pre-allocated.....	192
8.27	show ip dhcp server statistics	193
8.28	time-server	194
9	DHCP Snooping Commands.....	195
9.1	ip dhcp snooping.....	195
9.2	ip dhcp snooping vlan.....	196
9.3	ip dhcp snooping trust.....	197
9.4	ip dhcp snooping information option allowed-untrusted	198
9.5	ip dhcp snooping verify	199
9.6	ip dhcp snooping database	200
9.7	ip dhcp snooping binding	201
9.8	clear ip dhcp snooping database	203
9.9	show ip dhcp snooping	204
9.10	show ip dhcp snooping binding	205
9.11	ip source-guard.....	206
9.12	ip source-guard binding	207
9.13	ip source-guard tcam retries-freq	208
9.14	ip source-guard tcam locate	209
9.15	show ip source-guard configuration.....	210
9.16	show ip source-guard status	211
9.17	show ip source-guard inactive	212
9.18	show ip source-guard statistics.....	213
9.19	ip arp inspection.....	214
9.20	ip arp inspection vlan.....	215

9.21	ip arp inspection trust.....	216
9.22	ip arp inspection validate	217
9.23	ip arp inspection list create.....	218
9.24	ip mac	219
9.25	ip arp inspection list assign	220
9.26	ip arp inspection logging interval	221
9.27	show ip arp inspection	222
9.28	show ip arp inspection list	223
9.29	show ip arp inspection statistics.....	224
9.30	clear ip arp inspection statistics	225
10	DHCPv6 Commands	226
10.1	clear ipv6 dhcp client	226
10.2	ipv6 dhcp client information refresh	227
10.3	ipv6 dhcp client information refresh minimum	228
10.4	ipv6 dhcp duid-en.....	229
10.5	ipv6 dhcp relay destination (Global).....	230
10.6	ipv6 dhcp relay destination (Interface).....	232
10.7	show ipv6 dhcp	235
10.8	show ipv6 dhcp interface.....	237
11	DNS Client Commands	239
11.1	clear host	239
11.2	ip domain lookup.....	240
11.3	ip domain name.....	241
11.4	ip domain polling-interval	242
11.5	ip domain retry.....	243
11.6	ip domain timeout	244
11.7	ip host.....	245
11.8	ip name-server	246
11.9	show hosts	247
12	Ethernet Configuration Commands.....	249
12.1	interface.....	249
12.2	interface range	250
12.3	shutdown	251
12.4	operation time	253
12.5	description.....	254
12.6	speed.....	255
12.7	duplex	256
12.8	negotiation.....	257
12.9	flowcontrol.....	258
12.10	mdix.....	259
12.11	back-pressure	260
12.12	port jumbo-frame.....	261

12.13	clear counters	262
12.14	set interface active	263
12.15	errdisable recovery cause.....	264
12.16	errdisable recovery interval.....	265
12.17	errdisable recovery reset.....	266
12.18	show interfaces configuration	267
12.19	show interfaces status.....	269
12.20	show interfaces advertise.....	270
12.21	show interfaces description.....	272
12.22	show interfaces counters	273
12.23	show ports jumbo-frame.....	276
12.24	show errdisable recovery.....	277
12.25	show errdisable interfaces	278
12.26	clear switchport monitor	279
12.27	show switchport monitor.....	280
13	File System Commands	284
13.1	File Specification.....	284
13.2	System Flash Files.....	288
13.3	Flash File System on Stack	290
13.4	boot config	291
13.5	boot localization	293
13.6	boot system.....	295
13.7	cd	297
13.8	copy.....	298
13.9	delete	300
13.10	dir	301
13.11	mkdir	302
13.12	more.....	303
13.13	pwd	304
13.14	reboot.....	305
13.15	rename.....	307
13.16	rmdir.....	310
13.17	show bootvar / show version	311
13.18	show reboot.....	314
13.19	show running-config.....	315
13.20	show startup-config.....	317
13.21	write.....	319
14	GARP VLAN Registration Protocol (GVRP) Commands	320
14.1	clear gvrp statistics	320
14.2	gvrp enable (Global)	321
14.3	gvrp enable (Interface).....	322
14.4	gvrp registration-forbid.....	323

14.5	gvrp vlan-creation-forbid	324
14.6	show gvrp configuration.....	325
14.7	show gvrp error-statistics	326
14.8	show gvrp statistics.....	327
15	IGMP Commands.....	328
15.1	clear ip igmp snooping counters	328
15.2	ip igmp last-member-query-count	329
15.3	ip igmp snooping last-member-query-interval	330
15.4	ip igmp snooping query-interval.....	331
15.5	ip igmp snooping query-max-response-time.....	332
15.6	ip igmp snooping robustness-variable	333
15.7	ip igmp version.....	334
15.8	show ip igmp snooping counters	335
15.9	show ip igmp groups	336
15.10	show ip igmp groups summary	338
15.11	show ip igmp interface	339
16	IGMP Proxy Commands	340
16.1	ip igmp-proxy	340
16.2	ip igmp-proxy downstream protected	341
16.3	ip igmp-proxy downstream protected interface.....	342
16.4	ip igmp-proxy ssm	343
16.5	show ip igmpproxy interface.....	344
17	IGMP Snooping Commands	346
17.1	ip igmp snooping (Global)	346
17.2	ip igmp snooping vlan	347
17.3	ip igmp snooping vlan mrouter.....	348
17.4	ip igmp snooping vlan mrouter interface	349
17.5	ip igmp snooping vlan forbidden mrouter	350
17.6	ip igmp snooping vlan static	351
17.7	ip igmp snooping querier	352
17.8	ip igmp snooping vlan querier	353
17.9	ip igmp snooping vlan querier address.....	354
17.10	ip igmp snooping vlan querier election.....	355
17.11	ip igmp snooping vlan querier version.....	357
17.12	ip igmp snooping vlan immediate-leave	358
17.13	show ip igmp snooping groups	359
17.14	show ip igmp snooping interface.....	360
17.15	show ip igmp snooping mrouter.....	361
18	IP Addressing Commands	362
18.1	ip address	362
18.2	ip address dhcp.....	365
18.3	renew dhcp	366

18.4	ip default-gateway.....	367
18.5	show ip interface	368
18.6	arp	369
18.7	arp timeout (Global).....	370
18.8	Ip arp proxy disable	371
18.9	ip proxy-arp.....	372
18.10	clear arp-cache	373
18.11	show arp	374
18.12	show arp configuration.....	375
18.13	interface ip.....	376
18.14	ip helper-address.....	377
18.15	show ip helper-address.....	379
18.16	show ip dhcp client interface	380
19	IP Routing Protocol-Independent Commands	381
19.1	directed-broadcast.....	381
19.2	ip redirects.....	382
19.3	ip route	383
19.4	ip routing.....	385
19.5	show ip route	386
19.6	show ip route summary.....	388
20	IP Setup Interface Commands	389
20.1	ip setup interface.....	389
20.2	show ip setup interface	390
21	IP System Management Commands.....	391
21.1	ping.....	391
21.2	ssh.....	394
21.3	telnet	396
21.4	traceroute	399
22	IPv6 Commands.....	402
22.1	clear ipv6 neighbors	402
22.2	ipv6 address	403
22.3	ipv6 address anycast	404
22.4	ipv6 address autoconfig.....	406
22.5	ipv6 address eui-64	408
22.6	ipv6 address link-local	410
22.7	ipv6 default-gateway.....	411
22.8	ipv6 enable	412
22.9	ipv6 hop-limit	413
22.10	ipv6 icmp error-interval.....	414
22.11	ipv6 link-local default zone	416
22.12	ipv6 nd advertisement-interval	417
22.13	ipv6 nd dad attempts	418

22.14	ipv6 nd hop-limit	420
22.15	ipv6 nd managed-config-flag	421
22.16	ipv6 nd ns-interval	422
22.17	ipv6 nd other-config-flag	423
22.18	ipv6 nd prefix	424
22.19	ipv6 nd ra interval	428
22.20	ipv6 nd ra lifetime	430
22.21	ipv6 nd suppress-ra	431
22.22	ipv6 nd reachable-time	432
22.23	ipv6 nd router-preference	433
22.24	ipv6 neighbor	434
22.25	ipv6 redirects	436
22.26	ipv6 route	437
22.27	ipv6 unicast-routing	439
22.28	ipv6 unreachable	440
22.29	show ipv6 interface	441
22.30	show ipv6 link-local default zone	445
22.31	show ipv6 nd prefix	446
22.32	show ipv6 neighbors	448
22.33	show ipv6 route	450
22.34	show ipv6 route summary	452
22.35	show ipv6 static	453
23	IPv6 Prefix List Commands	455
23.1	clear ipv6 prefix-list	455
23.2	ipv6 prefix-list	456
23.3	show ipv6 prefix-list	461
24	Line Commands	463
24.1	exec-timeout	463
24.2	line	464
24.3	speed	465
24.4	show line	466
25	Link Aggregation Control Protocol (LACP) Commands	467
25.1	lacp port-priority	467
25.2	lacp system-priority	468
25.3	lacp timeout	469
25.4	show lacp	470
25.5	show lacp port-channel	472
26	Loopback Detection Protocol Commands	473
26.1	line loopback enable (Global)	473
26.2	line loopback enable (Interface)	474
26.3	line loopback mode	475
26.4	line loopback recovery	476

26.5	show line loopback configuration.....	477
26.6	show line loopback history.....	478
26.7	clear line loopback history.....	479
27	Management ACL Commands	480
27.1	deny (Management)	480
27.2	permit (Management)	482
27.3	management access-list	483
27.4	management access-class.....	485
27.5	show management access-list.....	486
27.6	show management access-class	487
28	MLD Commands	488
28.1	clear ipv6 mld counters.....	488
28.2	ipv6 mld last-member-query-count.....	489
28.3	ipv6 mld snooping last-member-queryinterval	490
28.4	ipv6 mld snooping query-interval.....	491
28.5	ipv6 mld snooping query-max-response-time.....	492
28.6	ipv6 mld robustness-variable.....	493
28.7	ipv6 mld version.....	494
28.8	show ipv6 mld snooping counters	495
28.9	show ipv6 mld groups	496
28.10	show ipv6 mld groups summary	498
28.11	show ipv6 mld interface	499
29	MLD Proxy Commands	500
29.1	ipv6 mld-proxy	500
29.2	ipv6 mld proxy downstream protected	502
29.3	ipv6 mld-proxy downstream protected interface.....	503
29.4	ipv6 mld-proxy ssm	504
29.5	show ipv6 mldproxy interface.....	505
30	MLD Snooping Commands.....	507
30.1	ipv6 mld snooping (Global)	507
30.2	ipv6 mld snooping vlan	508
30.3	ipv6 mld snooping querier	509
30.4	ipv6 mld snooping vlan querier	510
30.5	ipv6 mld snooping vlan querier election.....	511
30.6	ipv6 mld snooping vlan querier version	512
30.7	ipv6 mld snooping vlan mrouter.....	513
30.8	ipv6 mld snooping vlan mrouter interface	514
30.9	ipv6 mld snooping vlan forbidden mrouter	515
30.10	ipv6 mld snooping vlan static	516
30.11	ipv6 mld snooping vlan immediate-leave	517
30.12	show ipv6 mld snooping groups	518
30.13	show ipv6 mld snooping interface.....	520

30.14	show ipv6 mld snooping mrouter	521
31	Network Management Protocol (SNMP) Commands	522
31.1	snmp-server community	522
31.2	snmp-server community-group	524
31.3	snmp-server server	526
31.4	snmp-server source-interface	527
31.5	snmp-server source-interface-ipv6	529
31.6	snmp-server view	531
31.7	snmp-server group	533
31.8	show snmp views	535
31.9	show snmp groups	536
31.10	snmp-server user	537
31.11	show snmp users	539
31.12	snmp-server filter	541
31.13	show snmp filters	542
31.14	snmp-server host	543
31.15	snmp-server engineID local	545
31.16	snmp-server engineID remote	547
31.17	show snmp engineID	548
31.18	snmp-server enable traps	549
31.19	snmp-server trap authentication	550
31.20	snmp-server contact	551
31.21	snmp-server location	552
31.22	snmp-server set	553
31.23	snmp trap link-status	554
31.24	show snmp	555
32	PHY Diagnostics Commands	557
32.1	test cable-diagnostics tdr	557
32.2	show cable-diagnostics tdr	558
32.3	show cable-diagnostics cable-length	559
33	Port Channel Commands	560
33.1	channel-group	560
33.2	port-channel load-balance	561
33.3	show channel-group	562
34	Quality of Service (QoS) Commands	563
34.1	mls qos	563
34.2	mls qos advanced-mode trust	564
34.3	show mls qos	565
34.4	class-map	566
34.5	show class-map	568
34.6	match	569
34.7	policy-map	570

34.8	class	571
34.9	show policy-map	572
34.10	trust	573
34.11	set	575
34.12	redirect	576
34.13	mirror	577
34.14	police.....	578
34.15	service-policy	580
34.16	mls qos aggregate-policer	582
34.17	show mls qos aggregate-policer.....	584
34.18	police aggregate.....	585
34.19	wrr-queue cos-map	586
34.20	wrr-queue bandwidth.....	587
34.21	priority-queue out num-of-queues	588
34.22	traffic-shape	589
34.23	traffic-shape queue.....	590
34.24	mls qos wrr-queue wrtd.....	591
34.25	show mls qos wrr-queue wrtd	592
34.26	show mls qos interface	593
34.27	mls qos map policed-dscp	597
34.28	mls qos map dscp-queue.....	598
34.29	mls qos trust (Global)	599
34.30	mls qos trust (Interface)	600
34.31	mls qos cos	601
34.32	mls qos dscp-mutation.....	602
34.33	mls qos map dscp-mutation.....	603
34.34	show mls qos map.....	604
34.35	clear mls qos statistics	606
34.36	mls qos statistics policer.....	607
34.37	mls qos statistics aggregate-policer	608
34.38	clear queue statistics.....	609
34.39	show queue statistics	610
34.40	show mls qos statistics	611
35	RADIUS Commands	612
35.1	radius-server host	612
35.2	radius-server key	614
35.3	radius-server retransmit.....	615
35.4	radius-server host source-interface	616
35.5	radius-server host source-interface-ipv6	617
35.6	radius-server timeout.....	618
35.7	radius-server deadtime	619
35.8	show radius-servers	620

35.9	show radius-servers key.....	621
36	Rate Limit and Storm Control Commands	622
36.1	clear storm-control counters	622
36.2	rate-limit (Ethernet)	624
36.3	rate-limit vlan	625
36.4	storm-control.....	626
36.5	show mls qos rate-limit interface	628
36.6	show mls qos rate-limit vlan.....	629
36.7	show storm-control interface	630
37	Remote Network Monitoring (RMON) Commands	632
37.1	rmon alarm.....	632
37.2	show rmon alarm-table	634
37.3	show rmon alarm	635
37.4	rmon event	637
37.5	show rmon events.....	638
37.6	show rmon log	639
37.7	mon table-size	640
37.8	show rmon statistics	641
37.9	rmon collection stats	643
37.10	show rmon collection stats.....	644
37.11	show rmon history.....	645
38	RIP Commands	648
38.1	clear rip statistics.....	648
38.2	default-information originate	649
38.3	default-metric.....	650
38.4	ip rip authentication key-chain	651
38.5	ip rip authentication mode.....	652
38.6	ip rip authentication-key	653
38.7	ip rip default-information originate.....	654
38.8	ip rip distribute-list in	655
38.9	ip rip distribute-list out	656
38.10	ip rip offset	657
38.11	ip rip passive-interface.....	658
38.12	ip rip shutdown	659
38.13	network.....	660
38.14	passive-interface (RIP).....	662
38.15	redistribute (RIP)	663
38.16	router rip	666
38.17	show ip rip database	666
38.18	show ip rip peers	671
38.19	show ip rip statistics	672
38.20	shutdown	673

39	Router Resources Commands.....	674
39.1	system router resources	674
39.2	show system router resources.....	678
40	RSA and Certificate Commands	679
40.1	crypto key generate dsa	681
40.2	crypto key generate rsa.....	682
40.3	crypto key import	683
40.4	show crypto key	685
40.5	crypto certificate generate	685
40.6	crypto certificate request	688
40.7	crypto certificate import.....	690
40.8	show crypto certificate	693
41	Spanning-Tree Commands	694
41.1	spanning-tree	694
41.2	spanning-tree mode.....	695
41.3	spanning-tree forward-time.....	696
41.4	spanning-tree hello-time.....	697
41.5	spanning-tree max-age	698
41.6	spanning-tree priority	699
41.7	spanning-tree state	700
41.8	spanning-tree cost	701
41.9	spanning-tree port-priority	702
41.10	spanning-tree portfast.....	703
41.11	spanning-tree link-type.....	704
41.12	spanning-tree pathcost method	705
41.13	spanning-tree bpdu (Global)	706
41.14	spanning-tree forward-bpdu (Interface)	707
41.15	spanning-tree guard root	708
41.16	clear spanning-tree detected-protocols	709
41.17	spanning-tree mst priority.....	710
41.18	spanning-tree mst max-hops.....	711
41.19	spanning-tree mst port-priority	712
41.20	spanning-tree mst cost.....	713
41.21	spanning-tree mst configuration.....	715
41.22	instance (MST)	716
41.23	name (MST).....	717
41.24	revision (MST).....	718
41.25	show (MST).....	719
41.26	exit (MST).....	720
41.27	abort (MST)	721
41.28	show spanning-tree	722
42	SPAN and RSPAN Commands.....	724

42.1	monitor session destination	724
42.2	monitor session source	728
42.3	remote-span.....	731
42.4	show monitor session	733
42.5	show vlan remote-span	736
43	SSH Client Commands	737
43.1	ip ssh-client authentication	737
43.2	ip ssh-client change server password	738
43.3	ip ssh-client key	739
43.4	ip ssh-client password.....	743
43.5	ip ssh-client server authentication	744
43.6	ip ssh-client server fingerprint	745
43.7	ip ssh-client source-interface	747
43.8	ipv6 ssh-client source-interface	748
43.9	ip ssh-client username	749
43.10	show ip ssh-client	750
43.11	show ip ssh-client server	752
44	Stack Commands	754
44.1	stack unit.....	754
44.2	stack	755
44.3	show stack configuration	757
44.4	show stack	758
44.5	show stack links	759
44.6	snmp-server enable traps stack.....	760
45	SYSLOG Commands.....	761
45.1	clear logging	761
45.2	clear logging file	762
45.3	file-system logging	763
45.4	logging buffered.....	764
45.5	logging console	765
45.6	logging file	766
45.7	logging server	767
45.8	logging on	769
45.9	logging source-interface	770
45.10	logging source-interface-ipv6	771
45.11	logging aggregation on	772
45.12	logging aggregation aging-time	773
45.13	logging origin-id	774
45.14	show logging	775
45.15	show logging file	776
45.16	show syslog-servers	777
46	System Management Commands.....	778

46.1	disable ports leds.....	778
46.2	hostname.....	779
46.3	resume.....	780
46.4	service cpu-utilization.....	781
46.5	show cpu input rate.....	782
46.6	show cpu utilization.....	783
46.7	show environment.....	784
46.8	show inventory.....	786
46.9	show reboot.....	787
46.10	show sessions.....	788
46.11	show system.....	789
46.12	show system languages.....	790
46.13	show system tcam utilization.....	791
46.14	how services tcp-udp.....	792
46.15	debug show tech-support.....	793
46.16	show system fans.....	795
46.17	show system sensors.....	796
46.18	show system power-supply.....	797
46.19	show system id.....	798
46.20	show ports leds configuration.....	799
46.21	show users.....	800
46.22	show hardware version.....	801
46.23	system recovery.....	802
47	TACACS+Commands.....	803
47.1	tacacs-server host.....	803
47.2	tacacs-server host source-interface.....	805
47.3	tacacs-server host source-interface-ipv6.....	806
47.4	tacacs-server key.....	807
47.5	tacacs-server timeout.....	808
47.6	show tacacs.....	809
47.7	show tacacs key.....	810
48	Telnet, Secure Shell (SSH) and Secure Login(Slogin) Commands.....	811
48.1	ip telnet server.....	811
48.2	ip ssh server.....	812
48.3	ip ssh port.....	813
48.4	ip ssh password-auth.....	814
48.5	ip ssh pubkey-auth.....	815
48.6	crypto key pubkey-chain ssh.....	817
48.7	user-key.....	818
48.8	key-string.....	819
48.9	show ip ssh.....	821
48.10	show crypto key pubkey-chain ssh.....	822

49	User Interface Commands.....	823
49.1	banner exec	823
49.2	banner login	825
49.3	configure.....	827
49.4	disable	828
49.5	do	829
49.6	enable	830
49.7	end.....	831
49.8	exit (Configuration).....	832
49.9	exit (EXEC)	833
49.10	help	834
49.11	history.....	835
49.12	history size	836
49.13	logout.....	837
49.14	terminal datadump	838
49.15	terminal history	839
49.16	terminal history size	840
49.17	terminal prompt.....	841
49.18	terminal width.....	842
49.19	show banner	843
49.20	show history	844
49.21	show privilege.....	845
50	Virtual Local Area Network (VLAN) Commands.....	846
50.1	vlan database	846
50.2	vlan.....	847
50.3	show vlan.....	848
50.4	interface vlan	849
50.5	interface range vlan	850
50.6	name	851
50.7	switchport protected-port.....	852
50.8	show interfaces protected-ports	853
50.9	switchport.....	854
50.10	switchport mode	855
50.11	switchport access vlan.....	857
50.12	switchport trunk allowed vlan.....	858
50.13	switchport trunk native vlan	860
50.14	switchport hybrid allowed vlan.....	861
50.15	switchport hybrid native vlan.....	863
50.16	no ingress-checking.....	864
50.17	acceptable-frame-type	865
50.18	switchport hybrid forbidden vlan	866
50.19	map protocol protocols-group.....	867

50.20	show vlan protocols-groups	869
50.21	map mac macs-group	870
50.22	switchport hybrid map macs-group vlan	872
50.23	show vlan macs-groups	874
50.24	map subnet subnets-group.....	875
50.25	switchport hybrid map subnets-group vlan.....	876
50.26	show vlan subnets-groups	877
50.27	show interfaces switchport	878
50.28	private-vlan	880
50.29	private-vlan association	881
50.30	switchport private-vlan mapping.....	883
50.31	switchport private-vlan host-association.....	884
50.32	show vlan private-vlan.....	886
50.33	vlan prohibit-internal-usage	888
50.34	show vlan internal usage	890
51	VRRP Commands	891
51.1	clear vrrp counters	891
51.2	show vrrp.....	892
51.3	show vrrp counters.....	895
51.4	vrrp description.....	896
51.5	vrrp ip.....	897
51.6	vrrp preempt	899
51.7	vrrp priority.....	900
51.8	vrrp shutdown.....	901
51.9	vrrp source-ip	902
51.10	vrrp timers advertise	903
51.11	vrrp version	904
51.12	vrrp non-owner-ping response	905

1 Introduction

This section describes how to use the Command Line Interface (CLI). It contains the following topics:

- Overview
- User (Privilege) Levels
- CLI Command Modes
- Accessing the CLI
- CLI Command Conventions
- Editing Features
- Interface Naming Conventions
- IPv6z Address Conventions

1.1 Overview

The CLI is divided into various command modes. Each mode includes a group of commands. These modes are described in CLI Command Modes.

Users are assigned privilege levels. Each user privilege level can access specific CLI modes. User levels are described in the section below.

The Switch's serial port's default settings are as follows:

- 9600 baud
- no parity
- 8 data bits
- 1 stop bit

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above is then connected to the Switch's serial port via an RJ-45 to RS-232 DB-9 convertor cable.

With the serial port properly connected to a management computer, the following screen should be visible.

Input the UserName and Password (default value each “manager”).

Login success, display the ZEQUOxxxxDL>.

This is the command line where all commands are input.

1.2 User (Privilege) Levels

Users can be created with one of the following user levels:

- Level 1—Users with this level can only run User EXEC mode commands. Users at this level cannot access the web GUI or commands in the Privileged EXEC mode.
- Level 7—Users with this level can run commands in the User EXEC mode and a subset of commands in the Privileged EXEC mode. Users at this level cannot access the web GUI.
- Level 15—Users with this level can run all commands. Only users at this level can access the web GUI.

A system administrator (user with level 15) can create passwords that allow a lower level user to temporarily become a higher level user. For example, the user may go from level 1 to level 7, level 1 to 15, or level 7 to level 15.

The passwords for each level are set (by an administrator) using the following command:

```
enable password [level privilege-level]{password|encrypted encrypted-password}
```

Using these passwords, you can raise your user level by entering the command: enable and the password for level 7 or 15. You can go from level 1 to level 7 or directly to level 15. The higher level holds only for the current session.

The disable command returns the user to a lower level.

To create a user and assign it a user level, use the username command. Only users with command level 15, can create users at this level.

Example—Create passwords for level 7 and 15 (by the administrator):

```
ZEQU0xxxxDL#configure
ZEQU0xxxxDL<conf># enable passwd level 7 level7@abc
ZEQU0xxxxDL<conf># enable password level 15 level15@abc
ZEQU0xxxxDL<conf>#
```

Create a user with user level 1:

```
ZEQU0xxxxDL#configure
ZEQU0xxxxDL<conf> username john password john1234 privilege 1
ZEQU0xxxxDL<conf>
```

Example 2— Switch between Level 1 to Level 15. The user must know the password:

```
ZEQU0xxxxDL#
ZEQU0xxxxDL# enable
Enter Password: ***** (this is the password for level 15-level15@abc)
ZEQU0xxxxDL#
```

NOTE If authentication of passwords is performed on RADIUS or TACACS+ servers, the passwords assigned to user level 7 and user level 15 must be configured on the external server and associated with the \$enable7\$ and \$enable15\$ user names, respectively. See the Authentication, Authorization and Accounting (AAA) Commands chapter for details.

1.3 CLI Command Modes

The CLI is divided into four command modes. The command modes are (in the order in which they are accessed):

- User EXEC mode
- Privileged EXEC mode
- Global Configuration mode
- Interface Configuration mode

Each command mode has its own unique console prompt and set of CLI commands. Entering a question mark at the console prompt displays a list of available commands for the current mode and for the level of the user. Specific commands are used to switch from one mode to another.

Users are assigned privilege levels that determine the modes and commands available to them. User levels are described in User (Privilege) Levels.

User EXEC Mode

Users with level 1 initially log into User EXEC mode. User EXEC mode is used for tasks that do not change the configuration, such as performing basic tests and listing system information.

The user-level prompt consists of the switch host name followed by a #. The default host name is **ZEQUOxxxxDL** where xxxxxx is the last six digits of the device's MAC address, as shown below

ZEQUOxxxxDL#

The default host name can be changed via the hostname command in Global Configuration mode.

Privileged EXEC Mode

A user with level 7 or 15 automatically logs into Privileged EXEC mode.

Users with level 1 can enter Privileged Exec mode by entering the enable command, and when prompted, the password for level 15.

To return from the Privileged EXEC mode to the User EXEC mode, use the disable command.

Global Configuration Mode

The Global Configuration mode is used to run commands that configure features at the system level, as opposed to the interface level.

Only users with command level of 7 or 15 can access this mode.

To access Global Configuration mode from Privileged EXEC mode, enter the **configure** command at the Privileged EXEC mode prompt and press **Enter**. The Global Configuration mode prompt, consisting of the device host name followed by **(config)#**, is displayed:

ZEQUOxxxxDL(config)#

Use any of the following commands to return from Global Configuration mode to the Privileged EXEC mode:

- exit
- end
- Ctrl+Z

The following example shows how to access Global Configuration mode and return to Privileged EXEC mode:

```
ZEQUOxxxxDL#  
ZEQUOxxxxDL#configure  
ZEQUOxxxxDL(config)#exit  
ZEQUOxxxxDL#
```

Interface or Line Configuration Modes

The following is a sample of some of the available submodes:

- Interface—Contains commands that configure a specific interface (port, VLAN, port channel, or tunnel) or range of interfaces. The Global Configuration mode command **interface** is used to enter the Interface Configuration mode. The interface Global Configuration command is used to enter this mode.
- Line Interface—Contains commands used to configure the management connections for the console, Telnet and SSH. These include commands such as line timeout settings, etc. The **line** Global Configuration command is used to enter the Line Configuration command mode.
- VLAN Database—Contains commands used to configure a VLAN as a whole. The **vlan database** Global Configuration mode command is used to enter the VLAN Database Interface Configuration mode.
- Management Access List—Contains commands used to define management access-lists. The **management access-list** Global Configuration mode command is used to enter the Management Access List Configuration mode.

- MAC Access-List, IPv6 Access List, IP Access List—Configures conditions required to allow traffic based on MAC addresses, IPv6 address and IPv4 address, respectively. The **mac access-list**, **ipv6 access-list** and **ip access-list** Global Configuration mode commands are used to enter the these configuration mode.

To return from any Interface Configuration mode to the Global Configuration mode, use the **exit** command.

1.4 Accessing the CLI

The CLI can be accessed from a terminal or computer by performing one of the following tasks:

- Running a terminal application, on a computer's com port that is directly connected to the switch's console port,
—or—
- Running a Telnet session from a command prompt on a computer with a network connection to the switch.
- Using SSH from an application that supports SSH client running on a computer with a network connection to the switch.

NOTE Telnet and SSH are disabled by default on the switch.

If access is via a Telnet or SSH connection, ensure that the following conditions are met before using CLI commands:

- The switch has a defined IP address.
- Corresponding management access is enabled.
- There is an IP path such that the computer and the switch can reach each other.

1.5 CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

Convention	Description
[]	In a command line, square brackets indicate an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated the character. One option must be selected. For example, flowcontrol {auto on off} means that for the flowcontrol command, either auto, on, or off must be selected.
"" (inverted commas)	When the input string contains space and/or reserved words (i.e. VLAN), put the string in inverted commas.
parameter	Italic text indicates a parameter.
press key	Names of keys to be pressed are shown in bold .
Ctrl+F4	Keys separated by the + character are to be pressed simultaneously on the keyboard
Screen Display	Fixed-width font indicates CLI prompts, CLI commands entered by the user, and system messages displayed on the console.
all	When a parameter is required to define a range of ports or parameters and all is an option, the default for the command is all when no parameters are defined. For example, the command interface range port-channel has the option of either entering a range of channels, or selecting all. When the command is entered without a parameter, it automatically defaults to all.
text	When free text can be entered as a parameter for a command (for example in command: snmp-server contact) if the text consists of multiple words separated by blanks, the entire string must appear in double quotes. For example: snmp-server contact "QA on floor 8"

1.6 Editing Features

Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command **show interfaces status Gigabitethernet 1**, *show*, *interfaces* and *status* are keywords, Gigabitethernet is an argument that specifies the interface type, and 1 specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

ZEQUOxxxxDL(config)#username manager password manager

When working with the CLI, the command options are not displayed. The standard command to request help is ?.

There are two instances where help information can be displayed:

- Keyword lookup—The character ? is entered in place of a command. A list of all valid commands and corresponding help messages are is displayed.
- Partial keyword lookup—If a command is incomplete and or the character ? is entered in place of a parameter, the matched keyword or parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- Terminal Command Buffer
- Command Completion
- Interface Naming Conventions
- Keyboard Shortcuts

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

Keyword	Description
Up-Arrow key Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-Arrow key	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For more information on enabling or disabling the history buffer, refer to the **history** command.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system. For more information on configuring the command history buffer, refer to the **history size** command.

To display the history buffer, refer to the **show history** command.

Negating the Effect of Commands

For many configuration commands, the prefix keyword **no** can be entered to cancel the effect of a command or reset the configuration to the default value. This Reference Guide provides a description of the negation effect for each CLI command.

Command Completion

If the command entered is incomplete, invalid or has missing or invalid parameters, then the appropriate error message is displayed. This assists in entering the correct command. By pressing **Tab** after an incomplete command is entered, the system will attempt to identify and complete the command. If the characters already entered are not enough for the system to identify a single matching command, press **?** to display the available commands matching the characters already entered.

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Keyboard Key	Description
Up-arrow	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older
Down-arrow	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any configuration mode.
Backspace	Deletes one character left to the cursor position.

Copying and Pasting Text

Up to 1000 lines of text (or commands) can be copied and pasted into the device.

NOTE It is the user's responsibility to ensure that the text copied into the device consists of legal commands only.

When copying and pasting commands from a configuration file, make sure that the following conditions exist:

- A device Configuration mode has been accessed.

The commands contain no encrypted data, like encrypted passwords or keys. Encrypted data cannot be copied and pasted into the device except for encrypted passwords where the keyword encrypted is used before the encrypted data (for instance in the enable password command).

1.7 Interface Naming Conventions

Interfaces on the device can be one of the following types:

- Fast Ethernet (10/100 kbits) ports—This can be written as FastEthernet, **fa** or fe.
- Gigabit Ethernet (10/100/1000 kbits) ports—These can be written as either GigabitEthernet or gi or GE.
- Ten Gigabit Ethernet (10,000 kbits) ports—This can be written as either TenGigabitEthernet or te or XG.
- LAG (Port Channel)—Written as either Port-Channel or po.
- VLAN—Written as VLAN

Within the CLI, interfaces are denoted by concatenating the following elements:

- Type of Interface—As described above
- Unit Number—Unit in stack.
- Slot Number—The slot number is always 0.
- The syntax for interface names in stacking mode is:

```
{<ethernet-type>[ ][<unit-number>]/<slot-number>/<port-number> } |  
{port-channel | po | ch }[ ]<port-channel-number> |  
vlan[ ]<vlan-id>
```

- Interface Number—Port, LAG, tunnel or VLAN numbers

Samples of these various options are shown in the example below:

```
ZEQU0xxxxDL(config)# interface GigabitEthernet 1/0/1  
ZEQU0xxxxDL(config)# interface GE 1/0/1  
ZEQU0xxxxDL(config)# interface gi1/0/1  
ZEQU0xxxxDL(config)# interface TenGigabitEthernet 1/0/25  
ZEQU0xxxxDL(config)# interface XG 1/0/25  
ZEQU0xxxxDL(config)# interface gi1/0/25  
ZEQU0xxxxDL(config)# interface Port-Channel 1  
ZEQU0xxxxDL(config)# interface vlan 1
```

Interface Range

Interfaces may be described on an individual basis or within a range. The interface range command has the following syntax:

<interface-range> ::=

**{<port-type>[]<unit-number>/<slot-number>/<first-port-number>[-
<last-port-number>]} |**

**port-channel[]<first-port-channel-number>[- <last-port-channel-number>] |
vlan[]<first-vlan-id>[- <last-vlan-id>]**

A sample of this command is shown in the example below:

```
ZEQU0xxxxDL#configure
ZEQU0xxxxDL(config-if)#interface range gi1/0/1-5
```

List of Multiple Interface Types

A combination of interface types can be specified in the interface range command in the following format:

<range-list> ::= <interface-range> | <range-list>, <interface-range>

Up to five ranges can be included.

NOTE Range lists can contain either ports and port-channels or VLANs. Combinations of port/port-channels and VLANs are not allowed

The space after the comma is optional.

When a range list is defined, a space after the first entry and before the comma (,) must be entered.

A sample of this command is shown in the example below:

```
ZEQU0xxxxDL#configure
ZEQU0xxxxDL(config)#interface range gi1-5, vlan 1-2
```


1.8 IPv6z Address Conventions

The following describes how to write an IPv6z address, which is a link-local IPv6 address.

The format is: <ipv6-link-local-address>%<egress-interface>

where:

egress-interface (also known as zone) = **vlan**<vlan-id> | **po**<number> | **tunnel**<number> | **port**<number> | 0

If the egress interface is not specified, the default interface is selected. Specifying egress interface = 0 is equal to not defining an egress interface.

The following combinations are possible:

- **ipv6_address%egress-interface**—Refers to the IPv6 address on the interface specified.
- **ipv6_address%0**—Refers to the IPv6 address on the single interface on which an IPv6 address is defined.
- **ipv6_address**—Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

2 ACL Commands

2.1 ip access-list (IP extended)

Use the ip access-list extended Global Configuration mode command to name an IPv4 access list (ACL) and to place the device in IPv4 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the permit (IP) and deny (IP) commands. The service-acl input command is used to attach this ACL to an interface.

Use the no form of this command to remove the access list.

Syntax

ip access-list extended acl-name

no ip access-list extended acl-name

Parameters

- acl-name—Name of the IPv4 access list. (Range 1-32 characters)

Default Configuration

No IPv4 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

An IPv4 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Example

```
ZEQU0xxxxDL(config)# ip access-list extended server
ZEQU0xxxxDL(config-ip-acl)#
```

2.2 permit (IP)

Use the permit IP Access-list Configuration mode command to set permit conditions for an IPv4 access list (ACL). Permit conditions are also known as access control entries (ACEs). Use the no form of the command to remove the access control entry.

Syntax

- [sequence priority] permit protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name] [log-input]
- [sequence priority] permit icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code] [dscp number | precedence number] [time-range time-range-name] [log-input]
- [sequence priority] permit igmp {any | source source-wildcard} {any | destination destination-wildcard} [igmp-type] [dscp number | precedence number] [time-range time-range-name] [log-input]
- [sequence priority] permit tcp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]
- [sequence priority] permit udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [log-input]
- no [sequence priority] permit icmp {any | source source-wildcard} {any | destination destination-wildcard} {any | icmp-type} {any | icmp-code} [dscp number | precedence number] [time-range time-range-name] [log-input]
- no [sequence priority] permit igmp {any | source source-wildcard} {any | destination destination-wildcard} [igmp-type] [dscp number | precedence number] [time-range time-range-name] [log-input]
- no [sequence priority] permit tcp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]
- no [sequence priority] permit udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [log-input]

Parameters

- protocol—The name or the number of an IP protocol. Available protocol names are: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the ip keyword.(Range: 0–255)
- source—Source IP address of the packet.
- source-wildcard—Wildcard bits to be applied to the source IP address. Use ones in the bit position that you want to be ignored.
- destination—Destination IP address of the packet.
- destination-wildcard—Wildcard bits to be applied to the destination IP address. Use ones in the bit position that you want to be ignored.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- dscp number—Specifies the DSCP value.
- precedence number—Specifies the IP precedence value.
- icmp-type—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- icmp-code—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- igmp-type—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- destination-port—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).(Range: 0–65535).
- source-port—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set, it is prefixed by “+”. If a flag should be unset, it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **log-input**—Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

If a range of ports is used for source port in an ACE, it is not counted again, if it is also used for a source port in another ACE. If a range of ports is used for the destination port in an ACE, it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL. If the user types already existed priority, then the command is rejected.

Example

```
ZEQU0xxxxDL(config)# ip access-list extended server
ZEQU0xxxxDL(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
```

2.3 deny (IP)

Use the deny IP Access-list Configuration mode command to set deny conditions for IPv4 access list. Deny conditions are also known as access control entries (ACEs). Use the no form of the command to remove the access control entry.

Syntax

- [sequence priority] deny protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number][time-range time-range-name] [disable-port |log-input]
- [sequence priority] deny icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code] [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- [sequence priority] deny igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type] [dscp number | precedencenumber] [time-range time-range-name] [disable-port |log-input]
- [sequence priority] denytcp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags][time-range time-range-name] [disable-port |log-input]
- [sequence priority] deny udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no [sequence priority] deny protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no [sequence priority] deny icmp {any | source source-wildcard} {any |destination destination-wildcard} {any | icmp-type} {any | icmp-code}[dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no [sequence priority] deny igmp {any | source source-wildcard} {any |destination destination-wildcard}[igmp-type] [dscp number |precedence number] [time-range time-range-name] [disable-port |loginput]
- no [sequence priority] deny tcp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port|log-input]
- no [sequence priority] deny udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]

Parameters

- protocol—The name or the number of an IP protocol. Available protocol names: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the Ip keyword. (Range: 0–255)
- source—Source IP address of the packet.
- source-wildcard—Wildcard bits to be applied to the source IP address. Use 1s in the bit position that you want to be ignored.
- destination—Destination IP address of the packet.
- destination-wildcard—Wildcard bits to be applied to the destination IP address. Use 1s in the bit position that you want to be ignored.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- dscp number—Specifies the DSCP value.
- precedence number—Specifies the IP precedence value.
- icmp-type—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- icmp-code—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- igmp-type—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- destination-port—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp 161, snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).

(Range: 0–65535)

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”. If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.
- **log-input**—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for a source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port, it is counted again if it is also used for destination port.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL. If the user types already existed priority, then the command is rejected.

Example

```
ZEQU0xxxxDL (config)# ip access-list extended server
ZEQU0xxxxDL (config-ip-af)# deny ip 176.212.0.0 00.255.255 any
```

2.4 ipv6 access-list (IPv6 extended)

Use the `ipv6 access-list` Global Configuration mode command to define an IPv6 access list (ACL) and to place the device in IPv6 Access-list Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the `permit ( IPv6 )` and `deny ( IPv6 )` commands. The `service-acl` input command is used to attach this ACL to an interface.

Use the `no` form of this command to remove the access list.

Syntax

```
ipv6 access-list [acl-name]
```

```
no ipv6 access-list [acl-name]
```

Parameters

`acl-name`—Name of the IPv6 access list. Range 1-32 characters.

Default Configuration

No IPv6 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

IPv6 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Every IPv6 ACL has an implicit `permit icmp any any nd-ns any`, `permit icmp any any nd-na any`, and `deny ipv6 any any` statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.)

The IPv6 neighbor discovery process uses the IPv6 network layer service, therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Example

```
ZEQU0xxxxDL(config)# ipv6 access-list acl1  
ZEQU0xxxxDL(config-ip-acl)# permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

2.5 permit (IPv6)

Use the permit command in Ipv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

Syntax

- [sequence priority] permit protocol {any | {source-prefix/length} {any | destination-prefix/length} [dscp number | precedence number] [timerange time-range-name] [log-input]
- [sequence priority] permit icmp {any | {source-prefix/length} {any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [loginput]
- [sequence priority] permit tcp {any | {source-prefix/length} {any | source-port/port-range}} {any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]
- [sequence priority] permit udp {any | {source-prefix/length}} {any | source-port/port-range}} {any | destination-prefix/length} {any | destination-port/port-range} [dscp number | precedence number] [timerange time-range-name] [log-input]
- no [sequence priority] permit protocol {any | {source-prefix/ length} {any | destination-prefix/length} [dscp number | precedence number] [time-range time-range-name] [log-input]
- no [sequence priority] permit icmp {any | {source-prefix/length} {any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [loginput]
- no [sequence priority] permit tcp {any | {source-prefix/length} {any | source-port/port-range}} {any | destination- prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [log-input]
- no [sequence priority] permit udp {any | {source-prefix/length}} {any | source-port/port-range}} {any | destination-prefix /length} {any| destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [log-input]

Parameters

- protocol—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- source-prefix/length—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.

- destination-prefix/length—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- dscp number—Specifies the DSCP value. (Range: 0–63)
- precedence number—Specifies the IP precedence value.
- icmp-type—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- icmp-code—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- destination-port—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- source-port—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- match-all list-of-flag—List of TCP flags that should occur. If a flag should be set it is prefixed by "+". If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- time-range-name—Name of the time range that applies to this permit statement. (Range: 1–32)

- **log-input**—Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv6 access list is defined.

Command Mode

IPv6 Access-list Configuration mode

User Guidelines

If a range of ports is used for the destination port in an ACE, it is not counted again if it is also used for destination port in another ACE.

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for a source port in ACE, it is not counted again if it is also used for a source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

If **ace-priority** is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL. If the user types already existed priority, then the command is rejected.

Example: This example defines an ACL by the name of server and enters a rule (ACE) for tcp packets.

```
ZEQU0xxxxDL(config)# ipv6 access-list server
ZEQU0xxxxDL(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

2.6 deny (IPv6)

Use the deny command in Ipv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

Syntax

- [sequence priority] deny protocol {any | {source-prefix/length} {any | destination-prefix/length} [dscp number | precedence number] [timerange time-range-name] [disable-port |log-input]
- [sequence priority] deny icmp {any | {source-prefix/length} {any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [disableport |log-input]
- [sequence priority] deny tcp {any | {source-prefix/length} {any | source-port/port-range}} {any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port |log-input]
- [sequence priority] deny udp {any | {source-prefix/length}} {any | source-port/port-range}} {any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]
- no [sequence priority] deny protocol {any | {source-prefix/length} {any | destination-prefix/length} [dscp number | precedence number] [timerange time-range-name] [disable-port |log-input]
- no [sequence priority] deny icmp {any | {source-prefix/length} {any | destination-prefix/length} {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [disableport |log-input]
- no [sequence priority] deny tcp {any | {source-prefix/length} {any | source-port/port-range}} {any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port |log-input]
- no [sequence priority] deny udp {any | {source-prefix/length}} {any | source-port/port-range}} {any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port |log-input]

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **priority** - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- **dscp number**—Specifies the DSCP value. (Range: 0–63)
- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)

- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”. If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.
- **log-input**—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv6 access list is defined.

Command Mode

IPv6 Access-list Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. If a range of ports is used for source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for a destination port in ACE it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

If **ace-priority** is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL. If the user types already existed priority, then the command is rejected.

Example

```
ZEQU0xxxxDL(config)# ipv6 access-list server
ZEQU0xxxxDL(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

2.7 mac access-list

Use the mac access-list Global Configuration mode command to define a Layer 2 access list (ACL) based on source MAC address filtering and to place the device in MAC Access-list Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the permit (MAC) and deny (MAC) commands. The service-acl input command is used to attach this ACL to an interface.

Use the no form of this command to remove the access list.

Syntax

mac access-list extended acl-name

no mac access-list extended acl-name

Parameters

acl-name—Specifies the name of the MAC ACL (Range: 1–32 characters).

Default Configuration

No MAC access list is defined.

Command Mode

Global Configuration mode

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
ZEQU0xxxxDL(config)# mac access-list extended server1
ZEQU0xxxxDL(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

2.8 permit (MAC)

Use the permit command in MAC Access-list Configuration mode to set permit conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.

Syntax

- [sequence priority] permit {any | source source-wildcard} {any | destination destination-wildcard} [eth-type 0 | aarp | amber | decspanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [log-input]
- no [sequence priority] permit {any | source source-wildcard} {any | destination destination-wildcard} [eth-type 0 | aarp | amber | decspanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [log-input]

Parameters

- source—Source MAC address of the packet.
- source-wildcard—Wildcard bits to be applied to the source MAC address. Use 1s in the bit position that you want to be ignored.
- destination—Destination MAC address of the packet.
- destination-wildcard—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- priority - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- eth-type—The Ethernet type in hexadecimal format of the packet.
- vlan-id—The VLAN ID of the packet. (Range: 1–4094)
- cos—The Class of Service of the packet. (Range: 0–7)
- cos-wildcard—Wildcard bits to be applied to the CoS.
- time-range-name—Name of the time range that applies to this permit statement. (Range: 1–32)
- log-input—Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL. If the user types already existed priority, then the command is rejected.

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

Example

```
ZEQU0xxxxDL(config)# mac access-list extended server1
ZEQU0xxxxDL(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

2.9 deny (MAC)

Use the deny command in MAC Access-list Configuration mode to set deny conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.

Syntax

- [sequence priority] deny {any | source source-wildcard} {any | destination destination-wildcard} [{eth-type 0} | aarp | amber | decspanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [disable-port | loginput]
- no [sequence priority] deny {any | source source-wildcard} {any | destination destination-wildcard} [{eth-type 0} | aarp | amber | decspanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name] [disable-port | loginput]

Parameters

- source—Source MAC address of the packet.
- source-wildcard—Wildcard bits to be applied to the source MAC address. Use ones in the bit position that you want to be ignored.
- destination—Destination MAC address of the packet.
- destination-wildcard—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- SEQUENCE-NUMBER - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- eth-type—The Ethernet type in hexadecimal format of the packet.
- vlan-id—The VLAN ID of the packet. (Range: 1–4094).
- cos—The Class of Service of the packet.(Range: 0–7).
- cos-wildcard—Wildcard bits to be applied to the CoS.
- time-range-name—Name of the time range that applies to this permit statement. (Range: 1–32)
- disable-port—The Ethernet interface is disabled if the condition is matched.
- log-input—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL. If the user types already existed priority, then the command is rejected.

Example

```
ZEQU0xxxxDL (config)# mac access-list extended server1
ZEQU0xxxxDL (config-mac-al)# deny 00:00:00:00:00:01 00:00:00:00:00:ff any
```

2.10 access-group in

Use the access-group in command in Interface Configuration mode to bind an access list(s) (ACL) to an interface.

Use the no form of this command to remove all ACLs from the interface.

Syntax

- {mac | ip | ipv6} access-group NAME in [default-action {deny-any | permit-any}]
- no {mac | ip | ipv6} access-group in

Parameters

- NAME—Specifies an ACL to apply to the interface. See the user guidelines. (Range: 1–32 characters).
- deny-any—Deny all packets (that were ingress at the port) that do not meet the rules in this ACL.
- permit-any—Forward all packets (that were ingress at the port) that do not meet the rules in this ACL.

Default Configuration

No ACL is assigned.

Command Mode

Interface Configuration mode (Ethernet, Port-Channel,,VLAN)

User Guidelines

The following rules govern when ACLs can be bound or unbound from an interface:

- IPv4 ACLs and IPv6 ACLs can be bound together to an interface.
- A MAC ACL cannot be bound on an interface which already has an IPv4 ACL or IPv6 ACL bound to it.
- Two ACLs of the same type cannot be bound to a port.
- An ACL cannot be bound to a port that is already bound to an ACL, without first removing the current ACL. Both ACLs must be mentioned at the same time in this command.
- MAC ACLs that include a VLAN as match criteria cannot be bound to a VLAN.
- ACLs with time-based configuration on one of its ACEs cannot be bound to a VLAN.

- ACLs with the action Shutdown cannot be bound to a VLAN.
- When the user binds ACL to an interface, TCAM resources will be consumed. One TCAM rule for each MAC or IP ACE and two TCAM rules for each IPv6 ACE. The TCAM consumption is always even number, so in case of odd number of rules the consumption will be increased by 1.
- An ACL cannot be bound as input if it has been bound as output.

Example

```
ZEQU0xxxxDL(config)# mac access-list extended server-acl
ZEQU0xxxxDL(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
ZEQU0xxxxDL(config-mac-acl)# exit
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# mac access-group server-acl in default-action deny-any
```

2.11 access-group out

Use the access-group out command in Interface Configuration mode to control access to an interface on the egress (transmit path).

Use the no form of this command to remove the access control.

Syntax

- {mac | ip | ipv6} access-group NAME out
- no {mac | ip | ipv6} access-group out

Parameters

NAME-Specifies an ACL to apply to the interface. See the usage guidelines. (Range: NAME is from 0-32 characters. Use "" for empty string)

Default

No ACL is assigned.

Command Mode

Interface Configuration mode(Ethernet, Port-Channel).

User Guidelines

The rule actions: log-input is not supported. Trying to use it will result in an error. The deny rule action disable-port is not supported. Trying to use it will result in an error.

IPv4 and IPv6 ACLs can be bound together on an interface.

A MAC ACL cannot be bound on an interface together with an IPv4 ACL or IPv6 ACL.

Two ACLs of the same type cannot be added to a port.

An ACL cannot be added to a port that is already bounded to an ACL, without first removing the current ACL and binding the two ACLs together.

An ACL cannot be bound as output if it has been bound as input.

Example

This example binds an egress ACL to a port:

```
ZEQU0xxxxDL(config)# mac access-list extended server
ZEQU0xxxxDL(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
ZEQU0xxxxDL(config-mac-al)# exit
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# mac access-group server out
```

2.12 time-range

Use the time-range Global Configuration mode command to define time ranges for different functions. In addition, this command enters the Time-range Configuration mode. All commands after this one refer to the time-range being defined.

This command sets a time-range name. Use the absolute and periodic commands to actually configure the time-range.

Use the no form of this command to remove the time range from the device.

Syntax

- time-range
time-range-name
- no time-range time-range-name

Parameters

time-range-name—Specifies the name for the time range. (Range: 1–32 characters)

Default Configuration

No time range is defined

Command Mode

Global Configuration mode

User Guidelines

After adding the name of a time range with this command, use the absolute and periodic commands to actually configure the time-range. Multiple periodic commands are allowed in a time range. Only one absolute command is allowed.

If a time-range command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not evaluated again after the absolute end time is reached.

All time specifications are interpreted as local time.

To ensure that the time range entries take effect at the desired times, the software clock should be set by the user or by SNTP. If the software clock is not set by the user or by SNTP, the time range ACEs are not activated.

The user cannot delete a time-range that is bound to any features.

When a time range is defined, it can be used in the following commands:

- dot1x port-control
- power inline
- operation time
- permit (IP)
- deny (IP)
- permit (IPv6)
- deny (IPv6)
- permit (MAC)
- deny (MAC)

Example

```
ZEQU0xxxxDL(config)# time-range http-allowed  
ZEQU0xxxxDL(config-time-range)#periodic mon 12:00 to wed 12:00
```

2.13 absolute

Use the absolute Time-range Configuration mode command to specify an absolute time when a time range is in effect. Use the no form of this command to remove the time limitation.

Syntax

- absolute start hh:mm day month year
- no absolute start
- absolute end hh:mm day month year
- no absolute end

Parameters

- start—Absolute time and date that the permit or deny statement of the associated function going into effect. If no start time and date are specified, the function is in effect immediately.
- end—Absolute time and date that the permit or deny statement of the associated function is no longer in effect. If no end time and date are specified, the function is in effect indefinitely.
- hh:mm—Time in hours (military format) and minutes (Range: 0–23, mm: 0–5)
- day—Day (by date) in the month. (Range: 1–31)
- month—Month (first three letters by name). (Range: Jan...Dec)
- year—Year (no abbreviation) (Range: 2000–2097)

Default Configuration

There is no absolute time when the time range is in effect.

Command Mode

Time-range Configuration mode

Example

```
ZEQU0xxxxDL(config)# time-range http-allowed
ZEQU0xxxxDL(config-time-range)# absolute start 12:00 1 jan 2019
ZEQU0xxxxDL(config-time-range)# absolute end 12:00 31 dec 2019
```

2.14 periodic

Use the periodic Time-range Configuration mode command to specify a recurring (weekly) time range for functions that support the time-range feature. Use the no form of this command to remove the time limitation.

Syntax

- periodic day-of-the-week hh:mm to day-of-the-week hh:mm
- no periodic day-of-the-week hh:mm to day-of-the-week hh:mm
- periodic list hh:mm to hh:mm day-of-the-week1
[day-of-the-week2...day-of-the-week7]
- no periodic list hh:mm to hh:mm day-of-the-week1
[day-of-the-week2...day-of-the-week7]
- periodic list hh:mm to hh:mm all
- no periodic list hh:mm to hh:mm all

Parameters

- day-of-the-week—The starting day that the associated time range is in effect. The second occurrence is the ending day the associated statement is in effect. The second occurrence can be the following week (see description in the User Guidelines). Possible values are: mon, tue, wed, thu, fri, sat, and sun.
- hh:mm—The first occurrence of this argument is the starting hours:minutes (military format) that the associated time range is in effect. The second occurrence is the ending hours:minutes (military format) the associated statement is in effect. The second occurrence can be at the following day (see description in the User Guidelines). (Range: 0–23, mm: 0–59)
- list day-of-the-week1—Specifies a list of days that the time range is in effect.

Default Configuration

There is no periodic time when the time range is in effect.

Command Mode

Time-range Configuration mode

User Guidelines

The second occurrence of the day can be at the following week, e.g. Thursday– Monday means that the time range is effective on Thursday, Friday, Saturday, Sunday, and Monday.

The second occurrence of the time can be on the following day, e.g. “22:00–2:00”.

Example

```
ZEQU0xxxxDL (config)# time-range http-allowed  
ZEQU0xxxxDL (config-time-range)# periodic mon 12:00 to wed 12:00
```

2.15 show time-range

Use the show time-range User EXEC mode command to display the time range configuration.

Syntax

show time-range time-range-name

Parameters

time-range-name—Specifies the name of an existing time range.

Command Mode

User EXEC mode

Example

```
ZEQU0xxxxDL> show time-range
time-range http-allowed
absolute start 12:00 1 Jan 2019 end 12:00 31 Dec 2019
periodic Monday 12:00 to Wednesday 12:00
```

2.16 show access-list

Use the show access-lists Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.

Syntax

- show access-list [name]
- show access-list time-range-active [name]

Parameters

- name—Specifies the name of the ACL.(Range: 1-160 characters).
- time-range-active—Shows only the Access Control Entries (ACEs) whose time-range is currently active (including those that are not associated with time-range).

Command Mode

Privileged EXEC mode

Example

```
ZEQU0xxxxDL# show access-list
Standard IP access list 1
Extended IP access list ACL2
sequence 20 permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
sequence 40 permit 234 172.30.23.8 0.0.0.255 any time-range weekdays
ZEQU0xxxxDL# show access-list time-range-active
Extended IP access list ACL1
sequence 20 permit 234 172.30.40.1 0.0.0.0 any
sequence 40 permit 234 172.30.8.8 0.0.0.0 any
Extended IP access list ACL2
sequence 20 permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
ZEQU0xxxxDL# show access-list ACL1
Extended IP access list ACL1
sequence 20 permit 234 172.30.40.1 0.0.0.0 any
sequence 40 permit 234 172.30.8.8 0.0.0.0 any
```

2.17 clear access-list counters

Use the clear access-lists counters Privileged EXEC mode command to clear access-lists (ACLs) counters.

Syntax

clear access-list counters [interface-id]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Example

```
ZEQU0xxxxDL# clear access-list counters gi1/0/1
```

2.18 show interfaces access-list trapped packets

Use the show interfaces access-lists trapped packets Privileged EXEC mode command to display Access List (ACLs) trapped packets.

Syntax

```
show interfaces access-list trapped packets [interface-id | port-channel-number | VLAN  
vlan-id]
```

Parameters

- interface-id—Specifies an interface ID, the interface ID is an Ethernet port port-channel.
- port-channel—Specifies a port-channel.
- vlan-id—Specifies a VLAN

Command Mode

Privileged EXEC mode

User Guidelines

This command shows whether packets were trapped from ACE hits with logging enable on an interface.

Examples

Example 1:

```
ZEQU0xxxxDL# show interfaces access-list trapped packets  
Ports/LAGs: gi1/0/1-gi1/0/3, ch1-ch3, ch4  
VLANs: VLAN1, VLAN12-VLAN15  
Packets were trapped globally due to lack of resources
```

Example 2:

```
ZEQU0xxxxDL# show interfaces access-list trapped packets gi1/0/1  
Packets were trapped on interface gi1/0/1
```

2.19 ip access-list (IP standard)

Use the ip access-list Global Configuration mode command to define an IP standard list. The no format of the command removes the list.

Syntax

- ip access-list access-list-name {deny|permit} {src-addr[/src-len] | any}
- no ip access-list access-list-name

Parameters

- access-list-name—The name of the Standard IP access list. The name may contain maximum 32 characters.
- deny/permit—Denies/permits access if the conditions are matched.
 - src-addr[/src-len] | any— IP prefix defined as an IP address and length or any. The any value matches all IP addresses. If src-len is not defined, a value of 32 is applied. A value of src-len must be in the interval 1-32.

Default Configuration

No access list is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the ip access-list command to configure IP address filtering. Access lists are configured with permit or deny keywords to either permit or deny an IP address based on a matching condition. An implicit deny is applied to address that does not match any access-list entry.

An access-list entry consists of an IP address and a bit mask. The bit mask is a number from 1 to 32.

Evaluation of an IP address by an access list starts with the first entry of the list and continues down the list until a match is found. When the IP address match is found, the permit or deny statement is applied to that address and the remainder of the list is not evaluated.

Use the no ip access-list command to delete the access list.

In addition to filtering IP traffic on a per port base, a basic IP access control list can be used by RIP (Routing Information Protocol) to filter route updates.

Examples

Example 1 - The following example of a standard access list allows only the three specified networks. Any IP address that does not match the access list statements will be rejected.

```
ZEQU0xxxxDL(config)# ip access-list 1 permit 192.168.34.0/24
ZEQU0xxxxDL(config)# ip access-list 1 permit 10.88.0.0/16
ZEQU0xxxxDL(config)# ip access-list 1 permit 10.0.0.0/8
```

Note: all other access is implicitly denied.

Example 2 - The following example of a standard access list allows access for IP addresses in the range from 10.29.2.64 to 10.29.2.127. All IP addresses not in this range will be rejected.

```
ZEQU0xxxxDL(config)# ip access-list apo permit 10.29.2.64/26
```

Note: all other access is implicitly denied.

Example 3 - To specify a large number of individual addresses more easily, you can omit the mask length if it is 32. Thus, the following two configuration commands are identical in effect:

```
ZEQU0xxxxDL(config)# ip access-list 2aa permit 10.48.0.3
ZEQU0xxxxDL(config)# ip access-list 2aa permit 10.48.0.3/32
```

2.20 ipv6 access-list (IP standard)

The ipv6 access-list Global Configuration mode command defines an IPv6 standard list. The no format of the command removes the list.

Syntax

- `ipv6 access-list access-list-name {deny|permit} {src-addr[/src-len] | any}`
- `no ipv6 access-list access-list-name`

Parameters

- `access-list-name`—The name of the Standard IPv6 access list. The name may contain maximum 32 characters.
- `deny`—Denies access if the conditions are matched.
- `permit`—Permits access if the conditions are matched.
- `src-addr[/src-len] | any`— IPv6 prefix defined as an IPv6 address and length or any. The any value matches to all IPv6 addresses. If the src-len is not defined a value of 128 is applied. A value of src-len must be in interval 1-128.

Default Configuration

`no access list`

Command Mode

Global Configuration mode

User Guidelines

Use the `ipv6 access-list` command to configure IPv6 address filtering. Access lists are configured with `permit` or `deny` keywords to either permit or deny an IPv6 address based on a matching condition. An implicit deny is applied to address that does not match any access-list entry.

An access-list entry consists of an IP address and a bit mask. The bit mask is a number from 1 to 128.

Evaluation of an IPv6 address by an access list starts with the first entry of the list and continues down the list until a match is found. When the IPv6 address match is found, the `permit` or `deny` statement is applied to that address and the remainder of the list is not evaluated.

Use the `no ipv6 access-list` command to delete the access list.

The IPv6 standard access list is used to filter received and sent IPv6 routing information.

Example

The following example of an access list allows only the one specified prefix: Any IPv6 address that does not match the access list statements will be rejected.

```
ZEQU0xxxxDL(config)# ipv6 access-list 1 permit 3001::2/64
```

Note: all other access implicitly denied.

3 Address Table Commands

3.1 bridge multicast filtering

To enable the filtering of Multicast addresses, use the bridge multicast filtering Global Configuration mode command. To disable Multicast address filtering, use the no form of this command.

Syntax

- bridge multicast filtering
- no bridge multicast filtering

Parameters

This command has no arguments or keywords.

Default Configuration

Multicast address filtering is disabled. All Multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

When this feature is enabled, unregistered Multicast traffic (as opposed to registered) will still be flooded.

All registered Multicast addresses will be forwarded to the Multicast groups. There are two ways to manage Multicast groups, one is the IGMP Snooping feature, and the other is the bridge multicast forward-all command.

Example

The following example enables bridge Multicast filtering.

```
ZEQU0xxxxDL (config)# bridge multicast filtering
```

3.2 bridge multicast mode

To configure the Multicast bridging mode, use the bridge multicast mode Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast mode {mac-group | ipv4-group | ipv4-src-group}
- no bridge multicast mode

Parameters

- mac-group—Specifies that Multicast bridging is based on the packet's VLAN and MAC address.
- ipv4-group—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN and IPv4 destination address for IPv4 packets.
- ipv4-src-group—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN, IPv4 destination address and IPv4 source address for IPv4 packets.

Default Configuration

The default mode is mac-group.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the mac-group option when using a network management system that uses a MIB based on the Multicast MAC address. Otherwise, it is recommended to use

the ipv4 mode, because there is no overlapping of IPv4 Multicast addresses in these modes.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries in the FDB, as described in the following table:

FDB Mode	CLI Commands	
mac-group	bridge multicast address	bridge multicast forbidden address
ipv4-group	bridge multicast ip-address	bridge multicast forbidden ip-address
ipv4-src-group	bridge multicast source group	bridge multicast forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the IGMP version that is used in the network:

FDB Mode	IGMP version 2	IGMP version 3
mac-group	MAC group address	MAC group address
ipv4-group	IP group address	IP group address
ipv4-src-group	(*)	IP source and group addresses

(*) Note that (*,G) cannot be written to the FDB if the mode is ipv4-src-group. In that case, no new FDB entry is created, but the port is added to the static (S,G) entries (if they exist) that belong to the requested group. It is recommended to set the FDB mode to ipv4-group or mac-group for IGMP version 2.

If an application on the device requests (*,G), the operating FDB mode is changed to ipv4-group.

Example

The following example configures the Multicast bridging mode as an mac-group on VLAN 2.

```

ZEQU0xxxxDL (config)# interface vlan 2
ZEQU0xxxxDL (config-if)# bridge multicast mode mac-group

```

3.3 bridge multicast address

To register a MAC-layer Multicast address in the bridge table and statically add or remove ports to or from the group, use the bridge multicast address Interface (VLAN) Configuration mode command. To unregister the MAC address, use the no form of this command.

Syntax

- bridge multicast address {mac-multicast-address | ipv4-multicast-address} [{add | remove} {interface-list | port-channel port-channel-list}]
- no bridge multicast address mac-multicast-address

Parameters

- mac-multicast-address—Specifies the MAC group Multicast address.
- ipv4-multicast-address—Specifies the IP group Multicast address.
- add—(Optional) Adds ports to the group.
- remove—(Optional) Removes ports from the group.
- interface-list—(Optional) Specifies a list of Ethernet ports.
Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels.
Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

If ethernet interface-list or port-channel port-channel-list is specified without specifying add or remove, the default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the `mac-multicast-address` parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Examples

Example 1 - The following example registers the MAC address to the bridge table:

```
ZEQU0xxxxDL (config)# interface vlan 8  
ZEQU0xxxxDL (config-if)# bridge multicast address 01:00:5e:02:02:03
```

Example 2 - The following example registers the MAC address and adds ports statically.

```
ZEQU0xxxxDL (config)# interface vlan 8  
ZEQU0xxxxDL (config-if)# bridge multicast address 01:00:5e:02:02:03 add gi1/0/1-2
```

3.4 bridge multicast forbidden address

To forbid adding or removing a specific Multicast address to or from specific ports, use the bridge multicast forbidden address IInterface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast forbidden address {mac-multicast-address | ipv4-multicast-address} {add | remove} {interface-list | port-channel port-channel-list}
- no bridge multicast forbidden address mac-multicast-address

Parameters

- mac-multicast-address—Specifies the MAC group Multicast address.
- ipv4-multicast-address—Specifies the IP group Multicast address.
- add—Forbids adding ports to the group.
- remove—Forbids removing ports from the group.
- interface-list—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered, using bridge multicast address.

You can execute the command before the VLAN is created.

Example

The following example forbids MAC address 0100.5e02.0203 on port gi1/0/2 within VLAN 8.

```
ZEQU0xxxxDL (config)# interface vlan 8  
ZEQU0xxxxDL (config-if)# bridge multicast address 0100.5e02.0203  
ZEQU0xxxxDL (config-if)# bridge multicast forbidden address 0100.5e02.0203 add gi1/0/2
```

3.5 bridge multicast ip-address

To register IP-layer Multicast addresses to the bridge table, and statically add or remove ports to or from the group, use the bridge multicast ip-address Interface (VLAN) Configuration mode command. To unregister the IP address, use the no form of this command.

Syntax

- bridge multicast ip-address ip-multicast-address [[add | remove] {interface-list | port-channel port-channel-list}]
- no bridge multicast ip-address ip-multicast-address

Parameters

- ip-multicast-address—Specifies the group IP Multicast address.
- add—(Optional) Adds ports to the group.
- remove—(Optional) Removes ports from the group.
- interface-list—(Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

Default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the `ip-multicast-address` parameter only.

Static Multicast addresses can be defined on static VLANs only. You can execute the command before the VLAN is created.

Example

The following example registers the specified IP address to the bridge table:

```
ZEQU0xxxxDL (config) # interface vlan 8  
ZEQU0xxxxDL (config-if) # bridge multicast ip-address 239.2.2.2
```

The following example registers the IP address and adds ports statically.

```
ZEQU0xxxxDL (config) # interface vlan 8  
ZEQU0xxxxDL (config-if) # bridge multicast ip-address 239.2.2.2 add gi1/0/4
```

3.6 bridge multicast forbidden ip-address

To forbid adding or removing a specific IP Multicast address to or from specific ports, use the bridge multicast forbidden ip-address Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast forbidden ip-address {ip-multicast-address} {add | remove} { interface-list | port-channel port-channel-list}
- no bridge multicast forbidden ip-address ip-multicast-address

Parameters

- ip-multicast-address—Specifies the group IP Multicast address.
- add—(Optional) Forbids adding ports to the group.
- remove—(Optional) Forbids removing ports from the group.
- interface-list—(Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered. You can execute the command before the VLAN is created.

Example

The following example registers IP address 239.2.2.2, and forbids the IP address on port gi1/0/4 within VLAN 8.

```
ZEQU0xxxxDL (config) # interface vlan 8
ZEQU0xxxxDL (config-if) # bridge multicast ip-address 239.2.2.2
ZEQU0xxxxDL (config-if) # bridge multicast forbidden ip-address 239.2.2.2 add gi1/0/4
```

3.7 bridge multicast source group

To register a source IP address - Multicast IP address pair to the bridge table, and statically add or remove ports to or from the source-group, use the bridge multicast source group Interface (VLAN) Configuration mode command. To unregister the source-group-pair, use the no form of this command.

Syntax

- bridge multicast source ip-address group ip-multicast-address [[add | remove] {interface-list | port-channel port-channel-list}]
- no bridge multicast source ip-address group ip-multicast-address

Parameters

- ip-address—Specifies the source IP address.
- ip-multicast-address—Specifies the group IP Multicast address.
- add—(Optional) Adds ports to the group for the specific source IP address.
- remove—(Optional) Removes ports from the group for the specific source IP address.
- interface-list—(Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined. The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

The following example registers a source IP address - Multicast IP address pair to the bridge table:

```
ZEQU0xxxxDL(config)# interface vlan 8  
ZEQU0xxxxDL(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
```

3.8 bridge multicast forbidden source group

To forbid adding or removing a specific IP source address - Multicast address pair to or from specific ports, use the bridge multicast forbidden source group Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast forbidden source ip-address group ip-multicast-address {add | remove} {interface-list | port-channel port-channel-list}
- no bridge multicast forbidden source ip-address group ip-multicast-address

Parameters

- ip-address—Specifies the source IP address.
- ip-multicast-address—Specifies the group IP Multicast address.
- add—(Optional) Forbids adding ports to the group for the specific source IP address.
- remove—(Optional) Forbids removing ports from the group for the specific source IP address.
- interface-list—(Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered. You can execute the command before the VLAN is created.

Example

The following example registers a source IP address - Multicast IP address pair to the bridge table, and forbids adding the pair to port gi1/0/4 on VLAN 8:

```
ZEQU0xxxxDL(config)# interface vlan 8  
ZEQU0xxxxDL(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2  
ZEQU0xxxxDL(config-if)# bridge multicast forbidden source 13.16.1.1 group 239.2.2.2 add gi1/0/4
```

3.9 bridge multicast ipv6 mode

To configure the Multicast bridging mode for IPv6 Multicast packets, use the bridge multicast ipv6 mode Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast ipv6 mode {mac-group | ip-group | ip-src-group}
- no bridge multicast ipv6 mode

Parameters

- mac-group—Specifies that Multicast bridging is based on the packet's VLAN and MAC destination address.
- ip-group—Specifies that Multicast bridging is based on the packet's VLAN and IPv6 destination address for IPv6 packets.
- ip-src-group—Specifies that Multicast bridging is based on the packet's VLAN, IPv6 destination address and IPv6 source address for IPv6 packets.

Default Configuration

The default mode is mac-group.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the mac-group mode when using a network management system that uses a MIB based on the Multicast MAC address.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries for IPv6 Multicast addresses in the FDB, as described in the following table::

FDB Mode	CLI Commands	
mac-group	bridge multicast address	bridge multicast forbidden address
Ipv6-group	bridge multicast ipv6 ip-address	bridge multicast ipv6 forbidden ip-address
Ipv6-src-group	bridge multicast ipv6 source group	bridge multicast ipv6 forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the MLD version that is used in the network:

FDB Mode	MLD version 1	MLD version 2
mac-group	MAC group address	MAC group address
ipv6-group	Ipv6 group address	Ipv6 group address
ipv6-src-group	(*)	Ipv6 source and group addresses

(*) In ip-src-group mode a match is performed on 4 bytes of the multicast address and 4 bytes of the source address. In the group address the last 4 bytes of the address are checked for match. In the source address the last 3 bytes and 5th from last bytes of the interface ID are examined.

(*) Note that (*,G) cannot be written to the FDB if the mode is ip-src-group. In that case, no new FDB entry is created, but the port is added to the (S,G) entries (if they exist) that belong to the requested group.

If an application on the device requests (*,G), the operating FDB mode is changed to ip-group.

You can execute the command before the VLAN is created.

Example

The following example configures the Multicast bridging mode as an ip-group on VLAN 2.

```
ZEQU0xxxxDL (config)# interface vlan 2
ZEQU0xxxxDL (config-if)# bridge multicast ipv6 mode ip-group
```

3.10 bridge multicast ipv6 ip-address

To register an IPv6 Multicast address to the bridge table, and statically add or remove ports to or from the group, use the bridge multicast ipv6 ip-address Interface (VLAN) Configuration mode command. To unregister the IPv6 address, use the no form of this command.

Syntax

- bridge multicast ipv6 ip-address ipv6-multicast-address [[add | remove] {interface-list | port-channel port-channel-list}]
- no bridge multicast ipv6 ip-address ip-multicast-address

Parameters

- ipv6-multicast-address—Specifies the group IPv6 multicast address.
- add—(Optional) Adds ports to the group.
- remove—(Optional) Removes ports from the group.
- interface-list—(Optional) Specifies a list of Ethernet ports.
Separate nonconsecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels.
Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined. The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the `ipv6-multicast-address` parameter only.

Static Multicast addresses can be defined on static VLANs only. You can execute the command before the VLAN is created.

Examples

Example 1 - The following example registers the IPv6 address to the bridge table:

```
ZEQU0xxxxDL (config)# interface vlan 8  
ZEQU0xxxxDL (config-if)#bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
```

Example 2 - The following example registers the IPv6 address and adds ports statically.

```
ZEQU0xxxxDL (config)# interface vlan 8  
ZEQU0xxxxDL (config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1 add gi1/0/1-2
```

3.11 bridge multicast ipv6 forbidden ip-address

To forbid adding or removing a specific IPv6 Multicast address to or from specific ports, use the bridge multicast ipv6 forbidden ip-address Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast ipv6 forbidden ip-address {ipv6-multicast-address} {add | remove} {interface-list | port-channel port-channel-list}
- no bridge multicast ipv6 forbidden ip-address ipv6-multicast-address

Parameters

- ipv6-multicast-address—Specifies the group IPv6 Multicast address.
- add—(Optional) Forbids adding ports to the group.
- remove—(Optional) Forbids removing ports from the group.
- interface-list—(Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined. The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered. You can execute the command before the VLAN is created.

Example

The following example registers an IPv6 Multicast address, and forbids the IPv6 address on port gi1/0/2 within VLAN 8.

```
ZEQU0xxxxDL(config)# interface vlan 8
ZEQU0xxxxDL(config-if)# bridge multicast ipv6 ip-address FF00:0:0:0:4:4:1
ZEQU0xxxxDL(config-if)# bridge multicast ipv6 forbidden ip-address FF00:0:0:0:4:4:1 add gi1/0/2
```

3.12 bridge multicast ipv6 source group

To register a source IPv6 address - Multicast IPv6 address pair to the bridge table, and statically add or remove ports to or from the source-group, use the bridge.

multicast ipv6 source group Interface (VLAN) Configuration mode command. To unregister the source-group-pair, use the no form of this command.

Syntax

- bridge multicast ipv6 source ipv6-source-address group ipv6-multicast-address [[add | remove] {interface-list | port-channel port-channel-list}]
- no bridge multicast ipv6 source ipv6-address group ipv6-multicast-address

Parameters

- ipv6-source-address—Specifies the source IPv6 address.
- ipv6-multicast-address—Specifies the group IPv6 Multicast address.
- add—(Optional) Adds ports to the group for the specific source IPv6 address.
- remove—(Optional) Removes ports from the group for the specific source IPv6 address.
- interface-list—(Optional) Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—(Optional) Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined. The default option is add.

Command Mode

Interface (VLAN) Configuration mode

Example

The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table:

```
ZEQU0xxxxDL (config)# interface vlan 8
ZEQU0xxxxDL (config-if)# bridge multicast source 2001:0:0:0:4:4:4 group FF00:0:0:0:4:4:4:1
```

3.13 bridge multicast ipv6 forbidden source group

To forbid adding or removing a specific IPv6 source address - Multicast address pair to or from specific ports, use the bridge multicast ipv6 forbidden source group Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

Syntax

- bridge multicast ipv6 forbidden source ipv6-source-address group
ipv6-multicast-address {add | remove} {interface-list | port-channel port-channel-list}
- no bridge multicast ipv6 forbidden source ipv6-address group ipv6-multicast-address

Parameters

- ipv6-source-address—Specifies the source IPv6 address.
- ipv6-multicast-address—Specifies the group IPv6 Multicast address.
- add—Forbids adding ports to the group for the specific source IPv6 address.
- remove—Forbids removing ports from the group for the specific source IPv6 address.
- interface-list—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered. You can execute the command before the VLAN is created.

Example

The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table, and forbids adding the pair to gi1/0/2 on VLAN 8:

```
ZEQU0xxxxDL(config)# interface vlan 8
ZEQU0xxxxDL(config-if)# bridge multicast source 2001:0:0:0:4:4:4 group FF00:0:0:0:4:4:4:1
ZEQU0xxxxDL(config-if)# bridge multicast forbidden source 2001:0:0:0:4:4:4:1 group
FF00:0:0:0:4:4:4:1 add gi1/0/2
```

3.14 bridge multicast unregistered

To configure forwarding unregistered Multicast addresses, use the bridge multicast unregistered Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast unregistered {forwarding | filtering}
- no bridge multicast unregistered

Parameters

- forwarding—Forwards unregistered Multicast packets.
- filtering—Filters unregistered Multicast packets.

Default Configuration

Unregistered Multicast addresses are forwarded.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Do not enable unregistered Multicast filtering on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Note that routers do not necessarily send IGMP reports for the 224.0.0.x range.

You can execute the command before the VLAN is created.

Example

The following example specifies that unregistered Multicast packets are filtered on gi1/0/1:

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# bridge multicast unregistered filtering
```

3.15 bridge multicast forward-all

To enable forwarding all multicast packets for a range of ports or port channels, use the bridge multicast forward-all Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- bridge multicast forward-all {add | remove} {interface-list | port-channel port-channel-list}
- no bridge multicast forward-all

Parameters

- add—Forces forwarding of all Multicast packets.
- remove—Does not force forwarding of all Multicast packets.
- interface-list—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- port-channel port-channel-list—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

Forwarding of all Multicast packets is disabled.

Command Mode

Interface (VLAN) Configuration mode

Example

The following example enables all Multicast packets on port gi1/0/2 to be forwarded.

```
ZEQU0xxxxDL (config)# interface vlan 2
ZEQU0xxxxDL (config-if)# bridge multicast forward-all add gi1/0/2
```

3.16 bridge multicast forbidden forward-all

To forbid a port to dynamically join Multicast groups, use the bridge multicast forbidden forward-all Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- `bridge multicast forbidden forward-all {add | remove} {interface-list | port-channel port-channel-list}`
- `no bridge multicast forbidden forward-all`

Parameters

- `add`—Forbids forwarding of all Multicast packets.
- `remove`—Does not forbid forwarding of all Multicast packets.
- `interface-list` —Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- `port-channel port-channel-list`—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

Ports are not forbidden to dynamically join Multicast groups. The default option is add.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to forbid a port to dynamically join (by IGMP, for example) a Multicast group.

The port can still be a Multicast router port.

Example

The following example forbids forwarding of all Multicast packets to gi1/0/1 within VLAN 2.

```
ZEQU0xxxxDL (config)# interface vlan 2  
ZEQU0xxxxDL (config-if)# bridge multicast forbidden forward-all add ethernet gi1/0/1
```

3.17 bridge unicast unknown

To enable egress filtering of Unicast packets where the destination MAC address is unknown to the device, use the bridge unicast unknown Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- `bridge unicast unknown {filtering | forwarding}`
- `no bridge unicast unknown`

Parameters

- `filtering`—Filter unregistered Unicast packets.
- `forwarding`—Forward unregistered Unicast packets.

Default Configuration

Forwarding.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode.

Example

The following example drops Unicast packets on gi1/0/1 when the destination is unknown.

```
ZEQU0xxxxDL (config)# interface gi1/0/1  
ZEQU0xxxxDL (config-if)# bridge unicast unknown filtering
```

3.18 show bridge unicast unknown

To display the unknown Unicast filtering configuration, use the show bridge unicast unknown Privileged EXEC mode command.

Syntax

show bridge unicast unknown [interface-id]

Parameters

interface-id—(Optional) Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel

Command Mode

Privileged EXEC mode

Example

ZEUQ0xxxxDL (config) # show bridge unicast unknown	
Port	Unregistered
-----	-----
gi1/0/1	Forward
gi1/0/2	Filter
gi1/0/3	Filter

3.19 mac address-table static

To add a MAC-layer station source address to the MAC address table, use the `mac address-table static` Global Configuration mode command. To delete the MAC address, use the `no` form of this command.

Syntax

- `mac address-table static mac-address vlan vlan-id interface interface-id [permanent | delete-on-reset | delete-on-timeout | secure]`
- `no mac address-table static [mac-address] vlan vlan-id`

Parameters

- `mac-address`—MAC address (Range: Valid MAC address)
- `vlan-id`— Specify the VLAN
- `interface-id`—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel (Range: valid ethernet port, valid port-channel)
- `permanent`—(Optional) The permanent static MAC address. The keyword is applied by the default.
- `delete-on-reset`—(Optional)The delete-on-reset static MAC address.
- `delete-on-timeout`—(Optional)The delete-on-timeout static MAC address.
- `secure`—(Optional)The secure MAC address. May be used only in a secure mode.

Default Configuration

No static addresses are defined. The default mode for an added address is permanent.

Command Mode

Global Configuration mode

User Guidelines

Use the command to add a static MAC address with given time-to-live in any mode or to add a secure MAC address in a secure mode.

Each MAC address in the MAC address table is assigned two attributes: type and time-to-live.

The following value of time-of-live is supported:

- `permanent`—MAC address is saved until it is removed manually.
- `delete-on-reset`—MAC address is saved until the next reboot.

- delete-on-timeout—MAC address that may be removed by the aging timer.

The following types are supported:

- static— MAC address manually added by the command with the following keywords specifying its time-of-live:
 - permanent
 - delete-on-reset
 - delete-on-timeout

A static MAC address may be added in any port mode.

- secure— A MAC address added manually or learned in a secure mode. Use the mac address-table static command with the secure keyword to add a secure MAC address. The MAC address cannot be relearned.

A secure MAC address may be added only in a secure port mode.

- dynamic— a MAC address learned by the switch in non-secure mode. A value of its time-to-live attribute is delete-on-timeout.

Examples

Example 1 - The following example adds two permanent static MAC address:

```
ZEQU0xxxxDL (config) # mac address-table static 00:3f:bd:45:5a:b1 vlan 1 interface gi1/0/1
ZEQU0xxxxDL (config) # mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
permanent
```

Example 2 - The following example adds a deleted-on-reset static MAC address:

```
ZEQU0xxxxDL (config) # mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
delete-on-reset
```

Example 3 - The following example adds a deleted-on-timeout static MAC address:

```
ZEQU0xxxxDL (config) # mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
delete-on-timeout
```

Example 4 - The following example adds a secure MAC address:

```
ZEQU0xxxxDL (config) # mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
secure
```

3.20 clear mac address-table

To remove learned or secure entries from the forwarding database (FDB), use the clear mac address-table Privileged EXEC mode command.

Syntax

- clear mac address-table dynamic interface interface-id
- clear mac address-table secure interface interface-id

Parameters

- dynamic interface interface-id—Delete all dynamic (learned) addresses on the specified interface. The interface ID can be one of the following types: Ethernet port or port-channel. If interface ID is not supplied, all dynamic addresses are deleted.
- secure interface interface-id—Delete all the secure addresses learned on the specific interface. A secure address on a MAC address learned on ports on which port security is defined.

Default Configuration

For dynamic addresses, if interface-id is not supplied, all dynamic entries are deleted.

Command Mode

Privileged EXEC mode

Examples

Example 1 - Delete all dynamic entries from the FDB.

```
ZEQU0xxxxDL# clear mac address-table dynamic
```

Example 2 - Delete all secure entries from the FDB learned on secure port gi1/0/1.

```
ZEQU0xxxxDL# clear mac address-table secure interface gi1/0/1
```

3.21 mac address-table aging-time

To set the aging time of the address table, use the mac address-table aging-time Global configuration command. To restore the default, use the no form of this command.

Syntax

- mac address-table aging-time seconds
- no mac address-table aging-time

Parameters

seconds—Time is number of seconds. (Range:10-630)

Default Configuration

300

Command Mode

Global Configuration mode

Example

```
ZEQU0xxxxDL (config) # mac address-table aging-time 600
```

3.22 port security

To enable port security learning mode on an interface, use the port security Interface (Ethernet, Port Channel) Configuration mode command. To disable port security learning mode on an interface, use the no form of this command.

Syntax

- port security [forward | discard | discard-shutdown] [trap seconds]
- no port security

Parameters

- forward—(Optional) Forwards packets with unlearned source addresses, but does not learn the address.
- discard—(Optional) Discards packets with unlearned source addresses.
- discard-shutdown—(Optional) Discards packets with unlearned source addresses and shuts down the port.
- trap seconds—(Optional) Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1–1000000)

Default Configuration

The feature is disabled by default. The default mode is discard.

The default number of seconds is zero, but if traps is entered, a number of seconds must also be entered.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The command may be used only when the interface is in the regular (non-secure with unlimited MAC learning) mode.

See the `mac address-table static` command for information about MAC address attributes (type and time-to-live) definitions.

When the port security command enables the lock mode on a port all dynamic addresses learned on the port are changed to permanent secure addresses.

When the port security command enables a mode on a port differing from the lock mode all dynamic addresses learned on the port are deleted.

When the `no port security` command cancels a secure mode on a port all secure addresses defined on the port are changed to dynamic addresses.

Additionally to set a mode, use the port security command to set an action that the switch should perform on a frame which source MAC address cannot be learned.

Example

The following example forwards all packets to port `gi1/0/1` without learning addresses of packets from unknown sources and sends traps every 100 seconds, if a packet with an unknown source address is received.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# port security mode lock
ZEQU0xxxxDL(config-if)# port security forward trap 100
ZEQU0xxxxDL(config-if)# exit
```

3.23 port security mode

To configure the port security learning mode, use the port security mode Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- port security mode {max-addresses | lock | secure permanent | secure delete-on-reset}
- no port security mode

Parameters

- max-addresses—Non-secure mode with limited learning dynamic MAC addresses. The static MAC addresses may be added on the port manually by the mac address-table static command.
- lock—Secure mode without MAC learning. The static and secure MAC addresses may be added on the port manually by the mac address-table static command.
- secure permanent—Secure mode with limited learning permanent secure MAC addresses with the permanent time-of-live. The static and secure MAC addresses may be added on the port manually by the mac address-table static command.
- secure delete-on-reset—Secure mode with limited learning secure MAC addresses with the delete-on-reset time-of-live. The static and secure MAC addresses may be added on the port manually by the mac address-table static command.

Default Configuration

The default port security mode is lock.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The default port mode is called regular. In this mode, the port allows unlimited learning of dynamic addresses.

The static MAC addresses may be added on the port manually by the mac address-table static command.

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use the port security mode command to change the default mode before the port security command.

Example

The following example sets the port security mode to

Lock for gi1/0/4.

```
ZEQU0xxxxDL (config)# interface gi1/0/4  
ZEQU0xxxxDL (config-if)# port security mode lock  
ZEQU0xxxxDL (config-if)# port security  
ZEQU0xxxxDL (config-if)# exit
```

3.24 port security max

To configure the maximum number of addresses that can be learned on the port while the port is in port, max-addresses or secure mode, use the port security max Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

- port security max max-addr
- no port security max

Parameters

max-addr—Specifies the maximum number of addresses that can be learned on the port. (Range: 0–256)

Default Configuration

This default maximum number of addresses is 1.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The command may be used only when the interface is in the regular (non-secure with unlimited MAC learning) mode.

Use this command to change the default value before the port security command.

Example

The following example sets the port to limited learning mode:

```
ZEQU0xxxxDL (config)# interface gi1/0/4
ZEQU0xxxxDL (config-if)# port security mode max
ZEQU0xxxxDL (config-if)# port security max 20
ZEQU0xxxxDL (config-if)# port security
ZEQU0xxxxDL (config-if)# exit
```

3.25 show mac address-table

To display entries in the MAC address table, use the show mac address-table Privileged EXEC mode command.

Syntax

- show mac address-table [dynamic | static | secure] [vlan vlan] [interface interface-id] [address mac-address]

Parameters

- dynamic—(Optional) Displays only dynamic MAC address table entries.
- static—(Optional) Displays only static MAC address table entries.
- secure—(Optional) Displays only secure MAC address table entries.
- vlan—(Optional) Displays entries for a specific VLAN.
- interface interface-id—(Optional) Displays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- address mac-address—(Optional) Displays entries for a specific MAC address.

Default Configuration

If no parameters are entered, the entire table is displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Internal usage VLANs (VLANs that are automatically allocated on routed ports) are presented in the VLAN column by a port number and not by a VLAN ID.

Examples

Example 1 - Displays entire address table.

```
ZEQU0xxxxDL# show mac address-table  
Aging time is 300 sec
```

VLAN	MAC Address	Port	Type
1	00:00:26:08:13:23	0	self
1	00:3f:bd:45:5a:b1	gi1/0/1	static
1	00:a1:b0:69:63:f3	gi1/0/2	dynamic
2	00:a1:b0:69:63:f3	gi1/0/3	dynamic
gi1/0/4	00:a1:b0:69:61:12	gi1/0/4	dynamic

Example 2 - Displays address table entries containing the specified MAC address.

```
ZEQU0xxxxDL# show mac address-table address 00:3f:bd:45:5a:b1  
Aging time is 300 sec
```

VLAN	MAC Address	Port	Type
1	00:3f:bd:45:5a:b1	static	gi1/0/4

3.26 show mac address-table count

To display the number of addresses present in the Forwarding Database, use the show mac address-table count Privileged EXEC mode command.

Syntax

```
show mac address-table count [vlan vlan | interface interface-id]
```

Parameters

- vlan vlan—(Optional) Specifies VLAN.
- interface-id interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Example

```
ZEQU0xxxxDL# show mac address-table count
Capacity : 16384
Free     : 16379
Used     : 5
Secure   : 0
Dynamic  : 2
Stataic  : 2
Internal : 1
```

3.27 show bridge multicast mode

To display the Multicast bridging mode for all VLANs or for a specific VLAN, use the show bridge multicast mode Privileged EXEC mode command.

Syntax

show bridge multicast mode [vlan vlan-id]

Parameters

vlan vlan-id—(Optional) Specifies the VLAN ID.

Command Mode

Privileged EXEC mode

Example

The following example displays the Multicast bridging mode for all VLANs

ZEQU0xxxxDL# show bridge multicast mode				
VLAN	IPv4 Multicast Mode		IPv6 Multicast Mode	
	Admin	Oper	Admin	Oper
----	-----	-----	-----	-----
1	MAC-GROUP	MAC-GROUP	MAC-GROUP	MAC-GROUP
11	IPv4-GROUP	IPv4-GROUP	IPv6-GROUP	IPv6-GROUP
12	IPv4-SRC-	IPv4-SRC-	IPv6-SRC-	IPv6-SRC-
	GROUP	GROUP	GROUP	GROUP

3.28 show bridge multicast address-table

To display Multicast MAC addresses or IP Multicast address table information, use the show bridge multicast address-table Privileged EXEC mode command.

Syntax

- show bridge multicast address-table [vlan vlan-id]
- show bridge multicast address-table [vlan vlan-id] [address mac-multicast-address] [format {ip | mac}]
- show bridge multicast address-table [vlan vlan-id] [address ipv4-multicast-address] [source ipv4-source-address]
- show bridge multicast address-table [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-source-address]

Parameters

- vlan-id vlan-id—(Optional) Display entries for specified VLAN ID.
- address—(Optional) Display entries for specified Multicast address. The possible values are:
 - mac-multicast-address—(Optional) Specifies the MAC Multicast address.
 - ipv4-multicast-address—(Optional) Specifies the IPv4 Multicast address.
 - ipv6-multicast-address—(Optional) Specifies the IPv6 Multicast address.
- format—(Optional) Applies if mac-multicast-address was selected. In this case either MAC or IP format can be displayed. Display entries for specified Multicast address format. The possible values are:
 - ip—Specifies that the Multicast address is an IP address.
 - mac—Specifies that the Multicast address is a MAC address.
- source —(Optional) Specifies the source address. The possible values are:
 - ipv4-address—(Optional) Specifies the source IPv4 address.
 - ipv6-address—(Optional) Specifies the source IPv6 address.

Default Configuration

If the format is not specified, it defaults to mac (only if mac-multicast-address was entered).

If VLAN ID is not entered, entries for all VLANs are displayed.

If MAC or IP address is not supplied, entries for all addresses are displayed.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000 through 0100.5e7f.ffff.

Multicast router ports (defined statically or discovered dynamically) are members in all MAC groups.

Ports that were defined via the bridge multicast forbidden forward-all command are displayed in all forbidden MAC entries.

Changing the Multicast mode can move static Multicast addresses that are written in the device FDB to a shadow configuration because of FDB hash collisions.

Example

The following example displays bridge Multicast address information.

```
ZEQU0xxxxDL# show bridge multicast address-table
```

Multicast address table for VLANs in MAC-GROUP bridging mode:

Vlan	MAC Address	Type	Ports
8	01:00:5e:02:02:03	Static	1-2

Forbidden ports for Multicast addresses:

Vlan	MAC Address	Ports
8	01:00:5e:02:02:03	gi1/0/4

Multicast address table for VLANs in IPv4-GROUP bridging mode:

Vlan	MAC Address	Type	Ports
1	224.0.0.251	Dynamic	gi1/0/2

Forbidden ports for Multicast addresses:

Vlan	MAC Address	Ports
1	232.5.6.5	
1	233.22.2.6	

Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:

Vlan	Group Address	Source address	Type	Ports
1	224.2.2.251	11.2.2.3	Dynamic	gi1/0/1

Forbidden ports for Multicast addresses:

Vlan	Group Address	Source Address	Ports
8	239.2.2.2	*	gi1/0/4
8	239.2.2.2	1.1.1.11	gi1/0/4

Multicast address table for VLANs in IPv6-GROUP bridging mode:

VLAN	IP/MAC Address	Type	Ports
8	ff02::4:4:4	Static	gi1/0/1-2, gi1/0/3, Po1

Forbidden ports for Multicast addresses:

VLAN	IP/MAC Address	Ports
8	ff02::4:4:4	gi1/0/4

Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:

Vlan	Group Address	Source address	Type	Ports
8	ff02::4:4:4	*	Static	gi1/0/1-2, gi1/0/3, Po1
8	ff02::4:4:4	fe80::200:7ff:f e00:200	Static	

Forbidden ports for Multicast addresses:

Vlan	Group Address	Source address	Ports
8	ff02::4:4:4 *		gi1/0/4
8	ff02::4:4:4	fe80::200:7ff:f e00:200	gi1/0/4

3.29 show bridge multicast address-table static

To display the statically-configured Multicast addresses, use the show bridge multicast address-table static Privileged EXEC mode command.

Syntax

- show bridge multicast address-table static [vlan vlan-id] [all]
- show bridge multicast address-table static [vlan vlan-id] [address mac-multicast-address] [ip | mac]
- show bridge multicast address-table static [vlan vlan-id] [address ipv4-multicast-address] [source ipv4-source-address]
- show bridge multicast address-table static [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-source-address]

Parameters

- vlan vlan-id—(Optional) Specifies the VLAN ID.
- address—(Optional) Specifies the Multicast address. The possible values are:
 - mac-multicast-address—(Optional) Specifies the MAC Multicast address.
 - ipv4-multicast-address—(Optional) Specifies the IPv4 Multicast address.
 - ipv6-multicast-address—(Optional) Specifies the IPv6 Multicast address.
- source—(Optional) Specifies the source address. The possible values are:
 - ipv4-address—(Optional) Specifies the source IPv4 address.
 - ipv6-address—(Optional) Specifies the source IPv6 address.

Default Configuration

When all/mac/ip is not specified, all entries (MAC and IP) will be displayed.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000— 0100.5e7f.ffff.

Example

The following example displays the statically-configured Multicast addresses.

```
ZEQU0xxxxDL# show bridge multicast address-table static
MAC-GROUP table
Vlan      MAC Address      Ports
-----
```

1 0100.9923.8787 gi1/0/1, gi1/0/2

Forbidden ports for multicast addresses:

Vlan	MAC Address	Ports

IPv4-GROUP Table

Vlan	IP Address	Ports

1	231.2.2.3	gi1/0/1, gi1/0/2

19	231.2.2.8	gi1/0/2-3

Forbidden ports for multicast addresses:

Vlan	IP Address	Ports

1	231.2.2.3	gi1/0/4

19	231.2.2.8	gi1/0/3

IPv4-SRC-GROUP Table:

Vlan	Group Address	Source address	Ports

Forbidden ports for multicast addresses:

Vlan	Group Address	Source address	Ports

IPv6-GROUP Table

Vlan	IP Address	Ports

191	FF12::8	gi1/0/1-4

Forbidden ports for multicast addresses:

Vlan	IP Address	Ports

11	FF12::3	gi1/0/4

191	FF12::8	gi1/0/4

IPv6-SRC-GROUP Table:

Vlan	Group Address	Source address	Ports

192	FF12::8	FE80::201:C9A9:FE40	gi1/0/1-4

:8988

Forbidden ports for multicast addresses:

Vlan	Group Address	Source address	Ports

192	FF12::3	FE80::201:C9A9:FE40	gi1/0/2

:8988

3.30 show bridge multicast filtering

To display the Multicast filtering configuration, use the show bridge multicast filtering Privileged EXEC mode command.

Syntax

show bridge multicast filtering vlan-id

Parameters

vlan-id—Specifies the VLAN ID. (Range: Valid VLAN)

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the Multicast configuration for VLAN 1.

```
ZEQU0xxxxDL# show bridge multicast filtering 1
```

```
Filtering: Enabled
```

```
VLAN: 1
```

```
Forward-All
```

Port	Static	Status
gi1/0/1	Forbidden	Filter
gi1/0/2	Forward	Forward(s)
gi1/0/3	-	Forward(d)

3.31 show bridge multicast unregistered

To display the unregistered Multicast filtering configuration, use the show bridge multicast unregistered Privileged EXEC mode command.

Syntax

```
show bridge multicast unregistered [interface-id]
```

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Display for all interfaces.

Command Mode

Privileged EXEC mode

Example

The following example displays the unregistered Multicast configuration.

```
ZEQU0xxxxDL# show bridge multicast unregistered
```

Port	Unregistered
-----	-----
gi1/0/1	Forward
gi1/0/2	Filter
gi1/0/3	Filter

3.32 show ports security

To display the port-lock status, use the show ports security Privileged EXEC mode command.

Syntax

```
show ports security [interface-id | detailed]
```

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the port-lock status of all ports.

```
ZEQU0xxxxDL# show ports security
```

Port	Status	Learning	Action	Maximum	Trap	Frequency
gi1/0/1	Enabled	Max-Addresses	Discard	3	Enabled	100
gi1/0/2	Disabled	Max-Addresses	-	28	-	-
gi1/0/3	Enabled	Lock	Discard	8	Disabled	-

The following table describes the fields shown above.

Field	Description
Port	The port number.
Status	The port security status. The possible values are: Enabled or Disabled.
Action	The action taken on violation.
Maximum	The maximum number of addresses that can be associated on this port in the Max-Addresses mode.
Trap	The status of SNMP traps. The possible values are: Enable or Disable.
Freque	The minimum time interval between consecutive traps.

3.33 show ports security addresses

To display the current dynamic addresses in locked ports, use the show ports security addresses Privileged EXEC mode command.

Syntax

```
show ports security addresses [interface-id | detailed]
```

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays dynamic addresses in all currently locked port:

Port	Status	Learning	Current	Maximum
-----	-----	-----	-----	-----
gi1/0/1	Disabled	Lock	0	10
gi1/0/2	Disabled	Lock	0	1
gi1/0/3	Disabled	Lock	0	1
gi1/0/4	Disabled	Lock	0	1
...				

3.34 bridge multicast reserved-address

To define the action on Multicast reserved-address packets, use the bridge multicast reserved-address Global Configuration mode command. To revert to default, use the no form of this command.

Syntax

- bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype | llc sap | llc-snap pid] {discard | bridge}
- no bridge multicast reserved-address mac-multicast-address [ethernet-v2 ethtype | llc sap | llc-snap pid]

Parameters

- mac-multicast-address—MAC Multicast address in the reserved MAC addresses range. (Range: 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-2F)
- ethernet-v2 ethtype—(Optional) Specifies that the packet type is Ethernet v2 and the Ethernet type field (16 bits in hexadecimal format). (Range: 0x0600–0xFFFF)
- llc sap—(Optional) Specifies that the packet type is LLC and the DSAP-SSAP field (16 bits in hexadecimal format). (Range: 0xFFFF)
- llc-snap pid—(Optional) Specifies that the packet type is LLC-SNAP and the PID field (40 bits in hexadecimal format). (Range: 0x000000000000 - 0xFFFFFFFFFFFF)
- discard—Specifies discarding the packets.
- bridge—Specifies bridging (forwarding) the packets

Default Configuration

- If the user-supplied MAC Multicast address, ethertype and encapsulation (LLC) specifies a protocol supported on the device (called Peer), the default action (discard or bridge) is determined by the protocol.
- If not, the default action is as follows:
 - For MAC addresses in the range 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-0F, the default is discard.
 - For MAC addresses in the range 00-80-C2-00-00-10–01-80-C2-00-00-2F, the default is bridge.

Command Mode

Global Configuration mode

User Guidelines

If the packet/service type (ethertype/encapsulation) is not specified, the configuration is relevant to all the packets with the configured MAC address.

Specific configurations (that contain service type) have precedence over less specific configurations (contain only MAC address).

The packets that are bridged are subject to security ACLs.

The actions define by this command has precedence over forwarding rules defined by applications/protocols (STP, LLDP etc.) supported on the device.

Example

```
ZEQU0xxxxDL (config)# bridge multicast reserved-address 00:3f:bd:45:5a:b1
```

3.35 show bridge multicast reserved-addresses

To display the Multicast reserved-address rules, use the show bridge multicast reserved-addresses Privileged EXEC mode command.

Syntax

show bridge multicast reserved-addresses

Command Mode

Privileged EXEC mode

Example

ZEQU0xxxxDL# show bridge multicast reserved-addresses

MAC Address	Frame Type	Protocol	Action
01-80-C2-00-00-00	LLC-SNAP	00-00-0C-01-29	Bridge

4 Authentication, Authorization and Accounting

4.1 password

Use the password Line Configuration mode command to specify a password on a line (also known as an access method, such as a console or Telnet). Use the no form of this command to return to the default password.

Syntax

- password password [encrypted]
- no password

Parameters

- password—Specifies the password for this line. (Length: 0–159 characters)
- encrypted—Specifies that the password is encrypted and copied from another device configuration.

Default Configuration

No password is defined.

Command Mode

Line Configuration Mode

Example

The following example specifies the password ‘secret’ on a console.

```
ZEQU0xxxxDL (config)# line console
ZEQU0xxxxDL (config-line)# password secret
```

4.2 enable password

Use the enable password Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the no form of this command to return to the default password.

Syntax

- enable password [level privilege-level] {unencrypted-password | encrypted encrypted-password}
- no enable password [level level]

Parameters

- level privilege-level—Level for which the password applies. If not specified, the level is 15. (Range: 1–15)
 - unencrypted-password—Password for this level. (Range: 0–159 chars)
- password encrypted encrypted-password—Specifies that the password is encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)

Default Configuration

Default for level is 15.

Passwords are encrypted by default.

Command Mode

Global Configuration mode

User Guidelines

When the administrator configures a new enable password, this password is encrypted automatically and saved to the configuration file. No matter how the password was entered, it appears in the configuration file with the keyword encrypted and the encrypted value.

If the administrator wants to manually copy a password that was configured on one switch (for instance, switch B) to another switch (for instance, switch A), the

administrator must add encrypted in front of this encrypted password when entering the enable command in switch A. In this way, the two switches will have the same password.

Passwords are encrypted by default. You only are required to use the encrypted keyword when you are actually entering an encrypted keyword.

Examples

Example 1 - The command sets a password that has already been encrypted. It will copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
ZEQU0xxxxDL (config) # enable password encrypted
```

Example 2 - The command sets an unencrypted password for level 7 (it will be encrypted in the configuration file).

```
ZEQU0xxxxDL (config) # enable password level 7 let-me-in
```

4.3 service password-recovery

Use the service password-recovery Global Configuration mode command to enable the password-recovery mechanism. This mechanism allows an end user, with physical access to the console port of the device, to enter the boot menu and trigger the password recovery process. Use the no service password-recovery command to disable the password-recovery mechanism. When the password-recovery mechanism is disabled, accessing the boot menu is still allowed and the user can trigger the password recovery process. The difference is, that in this case, all the configuration files and all the user files are removed. The following log message is generated to the terminal: “All the configuration and user files were removed”.

Syntax

- service password-recovery
- no service password-recovery

Parameters

N/A

Default Configuration

The service password recovery is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

- If password recovery is enabled, the user can access the boot menu and trigger the password recovery in the boot menu. All configuration files and user files are kept.
- If password recovery is disabled, the user can access the boot menu and trigger the password recovery in the boot menu. The configuration files and user files are removed.
- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.
- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.

Example

The following command disables password recovery:

```
ZEQU0xxxxDL (config)# no service password recovery
```

Note that choosing to use Password recovery option in the Boot Menu during the boot process will remove the configuration files and the user files. Would you like to continue ? (Y/N) [N]

4.4 username

Use the username Global Configuration mode command to establish a username-based authentication system. Use the no form to remove a user name.

Syntax

- username name {nopassword | {password {unencrypted-password | {encrypted encrypted-password}}} | {privilege privilege-level {unencrypted-password | {encrypted encrypted-password}}}
- no username name

Parameters

- name—The name of the user. (Range: 1–20 characters)
- nopassword—No password is required for this user to log in.
- password—Specifies the password for this username. (Range: 1–64)
- unencrypted-password—The authentication password for the user. (Range: 1–159)
- encrypted encrypted-password—Specifies that the password is MD5 encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)
- privilege privilege-level —Privilege level for which the password applies. If not specified the level is 1. (Range: 1–15).

Default Configuration

No user is defined.

Command Mode

Global Configuration mode

Usage Guidelines

The last level 15 user (regardless of whether it is the default user or any user) cannot be removed and cannot be a remote user.

Examples

Example 1 - Sets an unencrypted password for user tom (level 15). It will be encrypted in the configuration file.

```
ZEQU0xxxxDL (config)# username tom password 1234
```

Example 2 - Sets a password for user jerry (level 15) that has already been encrypted. It will be copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
ZEQU0xxxxDL (config)# username jerry privilege 15 encrypted
```

4.5 show users accounts

The show users accounts Privileged EXEC mode command displays information about the users local database.

Syntax

show users accounts

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays information about the users local database:

ZEQU0xxxxDL# **show users accounts**

Username	Privilege	Password Expiry date	Lockout
-----	-----	-----	-----
Bob	15	Jan 18 2017	-
Robert	15	Jan 19 2017	-
Smith	15	-	-

The following table describes the significant fields shown in the display:

Field	Description
Username	The user name.
Privilege	The user's privilege level.
Password	The user's password expiration date. date

4.6 passwords complexity enable

Use the passwords complexity enable Global Configuration mode command to enforce minimum password complexity. The no form of this command disables enforcing password complexity.

Syntax

- passwords complexity enable
- no passwords complexity enable

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

If password complexity is enabled, the user is forced to enter a password that:

- Has a minimum length of 8 characters.
- Contains characters from at least 3 character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Is different from the current password.
- Contains no character that is repeated more than 3 times consecutively.
- Does not repeat or reverse the user name or any variant reached by changing the case of the characters.
- Does not repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

You can control the above attributes of password complexity with specific commands described in this section.

If you have previously configured other complexity settings, then those settings are used. This command does not wipe out the other settings. It works only as a toggle.

Example

The following example configures requiring complex passwords that fulfill the minimum requirements specified in the User Guidelines above.

```
ZEQU0xxxxDL (config)# passwords complexity enable
ZEQU0xxxxDL# show passwords configuration Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 8 characters
Minimal classes: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
ZEQU0xxxxDL#
```

4.7 passwords complexity

Use the passwords complexity Global Configuration mode commands to control the minimum requirements from a password when password complexity is enabled. Use the no form of these commands to return to default.

Syntax

- passwords complexity {min-length number} | {min-classes number} | not-current | {no-repeat number} | not-username | not-manufacturer-name
- no passwords complexity min-length | min-classes | not-current | no-repeat | not-username | not-manufacturer-name

Parameters

- min-length number—Sets the minimal length of the password. (Range: 0–64)
- min-classes number—Sets the minimal character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 0–4)
- not-current—Specifies that the new password cannot be the same as the current password.
- no-repeat number—Specifies the maximum number of characters in the new password that can be repeated consecutively. Zero specifies that there is no limit on repeated characters. (Range: 0–16)
- not-username—Specifies that the password cannot repeat or reverse the user name or any variant reached by changing the case of the characters.
- not-manufacturer-name—Specifies that the password cannot repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

Default Configuration

The minimal length is 8.

The number of classes is 3. The

default for no-repeat is 3.

All the other controls are enabled by default.

Command Mode

Global Configuration mode

Example

The following example configures the minimal required password length to 8 characters.

```
ZEQU0xxxxDL (config)# passwords complexity min-length 8
```

4.8 passwords aging

Use the passwords aging Global Configuration mode command to enforce password aging. Use the no form of this command to return to default.

Syntax

- passwords aging days
- no passwords aging

Parameters

- days—Specifies the number of days before a password change is forced. You can use 0 to disable aging. (Range: 0–365).

Default Configuration

180

Command Mode

Global Configuration mode

User Guidelines

Aging is relevant only to users of the local database with privilege level 15 and to enable a password of privilege level 15.

To disable password aging, use passwords aging 0.

Using no passwords aging sets the aging time to the default.

Example

The following example configures the aging time to be 24 days.

```
ZEQU0xxxxDL (config)# passwords aging 24
```

4.9 show passwords configuration

The show passwords configuration Privileged EXEC mode command displays information about the password management configuration.

Syntax

show passwords configuration

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
ZEQU0xxxxDL# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is disabled.
Minimal length: 8 characters
Minimal classed: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
```

5 Auto-Update and Auto-Configuration

5.1 boot host auto-config

Use the boot host auto-config Global Configuration mode command to enable auto configuration via DHCP. Use the no form of this command to disable DHCP auto configuration.

Syntax

- boot host auto-config [tftp | scp | auto [extension]]
- no boot host auto-config

Parameters

- tftp—Only the TFTP protocol is used by auto-configuration.
- scp—Only the SCP protocol is used by auto-configuration.
- auto—(Default) Auto-configuration uses the TFTP or SCP protocol depending on the configuration file's extension. If this option is selected, the extension parameter may be specified or, if not, the default extension is used.
- extension—The SCP file extension. When no value is specified, 'scp' is used. (Range: 1-16 characters)

Default Configuration

Enabled by default with the auto option.

Command Mode

Global Configuration mode

User Guidelines

The TFTP or SCP protocol is used to download/upload a configuration file.

Examples

Example 1. The following example specifies the auto mode and specifies "scon" as the SCP extension:

```
ZEQU0xxxxDL(config)# boot host auto-config auto scon
```

Example 2. The following example specifies the auto mode and does not provide an SCP extension.

In this case "scp" is used.

```
ZEQU0xxxxDL(config)# boot host auto-config auto
```

Example 3. The following example specifies that only the SCP protocol will be used:

```
ZEQU0xxxxDL(config)# boot host auto-config scp
```

5.2 boot host auto-update

Use the boot host auto-update Global Configuration mode command to enable the support of auto update via DHCP. Use the no form of this command to disable DHCP auto configuration.

Syntax

- boot host auto-update [tftp | scp | auto [extension]]
- no boot host auto-update

Parameters

- tftp—Only the TFTP protocol is used by auto-update.
- scp—Only the SCP protocol is used by auto-update.
- auto (Default)—Auto-configuration uses the TFTP or SCP protocol depending on the Indirect image file's extension. If this option is selected, the extension parameter may be specified or, if not, the default extension is used.
- extension—The SCP file extension. When no value is specified, 'scp' is used. (Range: 1-16 characters)

Default Configuration

Enabled by default with the auto option.

Command Mode

Global Configuration mode

User Guidelines

The TFTP or SCP protocol is used to download/upload an image file.

Examples

Example 1—The following example specifies the auto mode and specifies "scon" as the SCP extension:

```
ZEQU0xxxxDL (config) # boot host auto-update auto scon
```

Example 2—The following example specifies the auto mode and does not provide an SCP extension. In this case "scp" is used.

```
ZEQU0xxxxDL (config) # boot host auto-update auto
```

Example 3—The following example specifies that only the SCP protocol will be used:

```
ZEQU0xxxxDL (config) # boot host auto-update scp
```

5.3 show boot

Use the show boot Privilege EXEC mode command to show the status of the IP DHCP Auto Config process.

Syntax

show boot

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

ZEQU0xxxxDL# **show boot**

Auto Config

ConfigDownload via DHCP: enabled
Download Protocol: auto
SCP protocol will be used for files with extension: scp
Next Boot Config Download via DHCP: default

Auto Update

Image Download via DHCP: enabled
Download protocol: auto
SCP protocol will be used for files with extension: scp

5.4 ip dhcp tftp-server ip address

Use the `ip dhcp tftp-server ip address` Global Configuration mode command to set the backup server's IP address. This address server as the default address used by a switch when it has not been received from the DHCP server. Use the `no` form of the command to return to default.

Syntax

- `ip dhcp tftp-server ip address ip-addr`
- `no ip dhcp tftp-server ip address`

Parameters

- `ip-addr`—IPv4 Address, or IPv6 Address or DNS name of TFTP or SCP server.

Default Configuration

No IP address

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Examples

Example 1. The example specifies the IPv4 address of TFTP server:

```
ZEQU0xxxxDL(config)# ip dhcp tftp-server ip address 10.5.234.232
```

Example 2. The example specifies the IPv6 address of TFTP server:

```
ZEQU0xxxxDL(config)# ip dhcp tftp-server ip address 3000:1::12
```

Example 3. The example specifies the IPv6 address of TFTP server:

```
ZEQU0xxxxDL(config)# ip dhcp tftp-server ip address tftp-server.company.com
```

5.5 ip dhcp tftp-server file

Use the `ip dhcp tftp-server file` Global Configuration mode command to set the full file name of the configuration file to be downloaded from the backup server when it has not been received from the DHCP server. Use the `no` form of this command to remove the name.

Syntax

- `ip dhcp tftp-server file file-path`
- `no ip dhcp tftp-server file`

Parameters

- `file-path`—Full file path and name of the configuration file on the server.

Default Configuration

No file name

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or an SCP server.

Examples

```
ZEQU0xxxxDL(config)# ip dhcp tftp-server file conf/conf-file
```

5.6 ip dhcp tftp-server image file

Use the `ip dhcp tftp-server image file` Global Configuration mode command to set the indirect file name of the image file to be downloaded from the backup server when it has not been received from the DHCP server. Use the `no` form of this command to remove the file name.

Syntax

- `ip dhcp tftp-server image file file-path`
- `no ip dhcp tftp-server image file`

Parameters

- `file-path`—Full indirect file path and name of the configuration file on the server.

Default Configuration

No file name

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Examples

```
ZEQU0xxxxDL(config)# ip dhcp tftp-server image file imag/imag-file
```

5.7 show ip dhcp tftp-server

Use the show ip dhcp tftp-server EXEC mode command to display information about the backup server.

Syntax

show ip dhcp tftp-server

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Example

```
show ip dhcp tftp-server
server address
active    1.1.1.1 from sname
manual    2.2.2.2
file path on server
active    conf/conf-file from option 67
manual    conf/conf-file1
image indirect file path on server
manual    imag/imag-file
```

6 Clock Commands

6.1 absolute

To specify an absolute time when a time range is in effect, use the absolute command in Time-range Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- absolute start hh:mm day month year
- no absolute start
- absolute end hh:mm day month year

no absolute end

Parameters

- start—Absolute time and date that the permit or deny statement of the associated function going into effect. If no start time and date are specified, the function is in effect immediately.
- end—Absolute time and date that the permit or deny statement of the associated function is no longer in effect. If no end time and date are specified, the function is in effect indefinitely.
- hh:mm—Time in hours (military format) and minutes (Range: 0–23, mm: 0–5)
- day—Day (by date) in the month. (Range: 1–31)
- month—Month (first three letters by name). (Range: Jan...Dec)
- year—Year (no abbreviation) (Range: 2000–2097)

Default Configuration

There is no absolute time when the time range is in effect.

Command Mode

Time-range Configuration mode

Example

```
ZEQU0xxxxDL (config) # time-range http-allowed
ZEQU0xxxxDL (config-time-range) # absolute start 12:00 1 jan 2019
ZEQU0xxxxDL (config-time-range) # absolute end 12:00 31 dec 2019
```

6.2 clock dhcp timezone

To specify that the timezone and the Summer Time (Daylight Saving Time) of the system can be taken from the DHCP Timezone option, use the `clock dhcp timezone` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `clock dhcp timezone`
- `no clock dhcp timezone`

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The TimeZone taken from the DHCP server has precedence over the static TimeZone.

The Summer Time taken from the DHCP server has precedence over static SummerTime.

The TimeZone and SummerTime remain effective after the IP address lease time has expired.

The TimeZone and SummerTime that are taken from the DHCP server are cleared after reboot.

The `no` form of the command clears the dynamic Time Zone and Summer Time from the DHCP server are cleared.

In case of multiple DHCP-enabled interfaces, the following precedence is applied:

- information received from DHCPv6 precedes information received from DHCPv4
- information received from DHCP client running on lower interface precedes information received from DHCP client running on higher interface

Disabling the DHCP client from where the DHCP-TimeZone option was taken, clears the dynamic Time Zone and Summer Time configuration.

Example

```
ZEQU0xxxxDL(config)# clock dhcp timezone
```

6.3 clock set

To set the system clock manually, use the clock set command in Privileged EXEC mode.

Syntax

clock set hh:mm:ss {[day month] | [month day]} year

Parameters

- *hh:mm:ss*—Specifies the current time in hours (military format), minutes, and seconds. (Range: hh: 0-23, mm: 0-59, ss: 0-59)
- *day*—Specifies the current day of the month. (Range: 1-31)
- *month*—Specifies the current month using the first three letters of the month name. (Range: Jan–Dec)
- *year*—Specifies the current year. (Range: 2000–2037)

Default Configuration

The time of the image creation.

Command Mode

Privileged EXEC mode

User Guidelines

After boot the system clock is set to the time of the image creation.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
ZEQU0xxxxDL# clock set 13:32:00 7 Mar 2019
```

6.4 clock source

To configure an external time source for the system clock, use the clock source command in Global Configuration mode. To disable the external time source, use the no form of this command.

Syntax

- clock source {sntp}
- no clock source {sntp}

Parameters

- sntp—(Optional) Specifies that an SNTP server is the external clock source.

Default Configuration

SNTP

Command Mode

Global Configuration mode

User Guidelines

After boot the system clock is set to the time of the image creation.

If no parameter is specified, SNTP will be configured as the time source.

if the command is executed twice, each time with a different clock source, both sources will be operational, SNTP has higher priority than time from browser.

Example

The following example configures an SNTP server as an external time source for the system clock.

```
ZEQU0xxxxDL (config)# clock source sntp
ZEQU0xxxxDL (config)# exit
ZEQU0xxxxDL# show clock
*10:46:48 UTC May 28 2019
Time source is sntp
```

6.5 clock summer-time

To configure the system to automatically switch to summer time (Daylight Saving Time), use the clock summer-time command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- clock summer-time zone recurring {usa | eu | {week day month hh:mm week day month hh:mm}} [offset]
- clock summer-time zone date day month year hh:mm date month year hh:mm [offset]
- clock summer-time zone date month day year hh:mm month day year hh:mm [offset]
- no clock summer-time

Parameters

- zone—The acronym of the time zone to be displayed when summer time is in effect. (Range: up to 4 characters)
- recurring—Indicates that summer time starts and ends on the corresponding specified days every year.
- date—Indicates that summer time starts on the first date listed in the command and ends on the second date in the command.
- usa—The summer time rules are the United States rules.
- eu—The summer time rules are the European Union rules.
- week—Week of the month. Can be 1–5, first to last.
- day—Day of the week (first three characters by name, such as Sun).
- date—Date of the month. (Range: 1–31)
- month—Month (first three characters by name, such as Feb).
- year—year (no abbreviation). (Range: 2000–2097)
- hh:mm—Time (military format) in hours and minutes. (Range: hh:mmhh: 0-23, mm: 0-59)
- offset—(Optional) Number of minutes to add during summer time (default is 60). (Range: 1440)

Default Configuration

Summer time is disabled.

Command Mode

Global Configuration mode

User Guidelines

In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rules for Daylight Saving Time:

- From 2007:
 - Start: Second Sunday in March
 - End: First Sunday in November
 - Time: 2 AM local time
- Before 2007:
 - Start: First Sunday in April
 - End: Last Sunday in October
 - Time: 2 AM local time

EU rules for Daylight Saving Time:

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00) Greenwich Mean Time (GMT)

Example

```
ZEQU0xxxxDL(config)# clock summer-time abc date apr 1 2019 09:00 aug 2 2019 09:00
```

6.6 clock timezone

To set the time zone for display purposes, use the clock timezone command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- clock timezone zone hours-offset [minutes-offset]
- no clock timezone

Parameters

- zone—The acronym of the time zone. (Range: Up to 4 characters)
- hours-offset—Hours difference from UTC. (Range: (-12)–(+13))
- minutes-offset—(Optional) Minutes difference from UTC. (Range: 0–59)

Default Configuration

Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same:

- Offsets are 0.
- Acronym is empty.

Command Mode

Global Configuration mode

User Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Example

```
ZEQU0xxxxDL (config)# clock timezone abc +2 minutes 32
```

6.7 periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the periodic command in Time-range Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- periodic day-of-the-week hh:mm to day-of-the-week hh:mm
- no periodic day-of-the-week hh:mm to day-of-the-week hh:mm
- periodic list hh:mm to hh:mm day-of-the-week1
[day-of-the-week2...day-of-the-week7]
- no periodic list hh:mm to hh:mm day-of-the-week1
[day-of-the-week2...day-of-the-week7]
- periodic list hh:mm to hh:mm all
- no periodic list hh:mm to hh:mm all

Parameters

- day-of-the-week—The starting day that the associated time range is in effect. The second occurrence is the ending day the associated statement is in effect. The second occurrence can be the following week (see description in the User Guidelines). Possible values are: mon, tue, wed, thu, fri, sat, and sun.
- hh:mm—The first occurrence of this argument is the starting hours:minutes (military format) that the associated time range is in effect. The second occurrence is the ending hours:minutes (military format) the associated statement is in effect. The second occurrence can be at the following day (see description in the User Guidelines). (Range: 0–23, mm: 0–59)
- list day-of-the-week1—Specifies a list of days that the time range is in effect.

Default Configuration

There is no periodic time when the time range is in effect.

Command Mode

Time-range Configuration mode

User Guidelines

The second occurrence of the day can be at the following week, e.g. Thursday– Monday means that the time range is effective on Thursday, Friday, Saturday, Sunday, and Monday.

The second occurrence of the time can be on the following day, e.g. “22:00–2:00”.

Example

```
ZEQU0xxxxDL (config) # time-range http-allowed  
ZEQU0xxxxDL (config-time-range) # periodic mon 12:00 to wed 12:00
```

6.8 sntp anycast client enable

To enable the SNTP Anycast client, use the `sntp anycast client enable` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

`sntp anycast client enable [both | ipv4 | ipv6]`

Parameters

- `both`—(Optional) Specifies the IPv4 and IPv6 SNTP Anycast clients are enabled. If the parameter is not defined it is the default value.
- `ipv4`—(Optional) Specifies the IPv4 SNTP Anycast clients are enabled.
- `ipv6`—(Optional) Specifies the IPv6 SNTP Anycast clients are enabled.

Default Configuration

The SNTP anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enable the SNTP Anycast client.

Example

The following example enables SNTP Anycast clients.

```
ZEQU0xxxxDL (config) # sntp anycast client enable
```

6.9 sntp authenticate

To enable authentication for received SNTP traffic from servers, use the `sntp authenticate` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp authenticate`
- `no sntp authenticate`

Parameters

N/A

Default Configuration

Authentication is disabled.

Command Mode

Global Configuration mode

Examples

The following example enables authentication for received SNTP traffic and sets the key and encryption key.

```
ZEQU0xxxxDL (config) # sntp authenticate  
ZEQU0xxxxDL (config) # sntp authentication-key 8 md5 ClkKey  
ZEQU0xxxxDL (config) # sntp trusted-key 8
```

6.10 sntp authentication-key

To define an authentication key for Simple Network Time Protocol (SNTP), use the `sntp authentication-key` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp authentication-key key-number md5 key-value`
- `no sntp authentication-key key-number`

Parameters

- `key-number`—Specifies the key number. (Range: 1–4294967295)
- `key-value`—Specifies the key value. (Length: 1–8 characters)

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

Examples

The following example defines the authentication key for SNTP.

```
ZEQU0xxxxDL (config) # sntp authentication-key 8 md5 ClkKey
ZEQU0xxxxDL (config) # sntp authentication-key 8 md5 ClkKey
ZEQU0xxxxDL (config) # sntp trusted-key 8
ZEQU0xxxxDL (config) # sntp authenticate
```

6.11 sntp broadcast client enable

To enable SNTP Broadcast clients, use the `sntp broadcast client enable` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp broadcast client enable [both | ipv4 | ipv6]`
- `no sntp broadcast client enable`

Parameters

- `both`—(Optional) Specifies the IPv4 and IPv6 SNTP Broadcast clients are enabled. If the parameter is not defined it is the default value.
- `ipv4`—(Optional) Specifies the IPv4 SNTP Broadcast clients are enabled.
- `ipv6`—(Optional) Specifies the IPv6 SNTP Broadcast clients are enabled.

Default Configuration

The SNTP Broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp broadcast client enable` Interface Configuration mode command to enable the SNTP Broadcast client on a specific interface.

After entering this command, you must enter the `clock source` command with the `sntp` keyword for the command to be run. If this command is not run, the switch will not synchronize with Broadcast servers.

Example

The following example enables SNTP Broadcast clients.

```
ZEQU0xxxxDL (config)# sntp broadcast client enable
```

6.12 sntp client enable

To enable the SNTP Broadcast and Anycast client, use the `sntp client enable` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp client enable interface-id`
- `no sntp client enable interface-id`

Parameters

- `interface-id`—Specifies an interface ID, which can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration

The SNTP client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp client enable` command to enable SNTP Broadcast and Anycast clients.

Example

The following example enables the SNTP Broadcast and Anycast clients on VLAN 100:

```
ZEQU0xxxxDL (config) # sntp client enable vlan 100
```

6.13 sntp client enable (interface)

To enable the SNTP Broadcast and Anycast client on an interface, use the `sntp client enable` command in Interface Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp client enable`
- `no sntp client enable`

Parameters

N/A

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface Configuration mode

User Guidelines

This command enables the SNTP Broadcast and Anycast client on an interface. Use the `no` form of this command to disable the SNTP client.

Example

The following example enables the SNTP broadcast and anycast client on an interface.

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# sntp client enable
ZEQU0xxxxDL(config-if)# exit
```

6.14 sntp server

To configure the device to use the SNTP to request and accept Network Time Protocol (NTP) traffic from a specified server (meaning to accept system time from an SNTP server), use the `sntp server` command in Global Configuration mode. To remove a server from the list of SNTP servers, use the `no` form of this command.

Syntax

- `sntp server {ip-address | hostname} [poll] [key keyid]}`
- `no sntp server [ip-address | hostname]`

Parameters

- `ip-address`—Specifies the server IP address. This can be an IPv4, IPv6 or IPv6z address.
- `hostname`—Specifies the server hostname. Only translation to IPv4 addresses is supported. (Length: 1–158 characters. Maximum label length for each part of the hostname: 63 characters)
- `poll`—(Optional) Enables polling.
- `key keyid`—(Optional) Specifies the Authentication key to use when sending packets to this peer. (Range:1–4294967295)

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp server {ip-address | hostname} [poll] [key keyid]` command to define a SNTP server. The switch supports up to 8 SNTP servers.

Use the `sntp server default` command to return to the default configuration. Use the `no sntp server ip-address | hostname` command to remove one SNTP server.

Use the `no sntp server` to remove all SNTP servers.

Example

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1 with polling.

```
ZEQU0xxxxDL (config)# sntp server 192.1.1.1 poll
```

6.15 sntp source-interface

To specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SNTP servers, use the `sntp source-interface` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp source-interface interface-id`
- `no sntp source-interface`

Parameters

- `interface-id`—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SNTP server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL (config)# sntp source-interface vlan 10
```

6.16 sntp source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 SNTP servers, use the `sntp source-interface-ipv6` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp source-interface-ipv6 interface-id`
- `no sntp source-interface-ipv6`

Parameters

- `interface-id`—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

The outgoing interface is selected based on the SNTP server's IP address. If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SNTP server.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL (config) # sntp source-interface-ipv6 vlan 10
```

6.17 sntp trusted-key

To define the trusted key, use the `sntp trusted-key` command in Global Configuration mode. To restore the default configuration, use the `no` form of this command.

Syntax

- `sntp trusted-key key-number`
- `no sntp trusted-key key-number`

Parameters

- `key-number`—Specifies the key number of the authentication key to be trusted. (Range: 1–4294967295).

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

The trusted key is used for authentication of all servers not having personal keys assigned by the `sntp server` command.

Examples

The following example authenticates key 8.

```
ZEQU0xxxxDL (config)# sntp trusted-key 8
ZEQU0xxxxDL (config)# sntp authentication-key 8 md5 ClkKey
ZEQU0xxxxDL (config)# sntp trusted-key 8
ZEQU0xxxxDL (config)# sntp authenticate
```

6.18 sntp unicast client enable

To enable the device to use Simple Network Time Protocol (SNTP) Unicast clients, use the `sntp unicast client enable` command in Global Configuration mode. To disable the SNTP Unicast clients, use the `no` form of this command.

Syntax

- `sntp unicast client enable`
- `no sntp unicast client enable`

Parameters

N/A

Default Configuration

The SNTP unicast clients are enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the `sntp server` Global Configuration mode command to define SNTP servers.

Example

The following example enables the device to use SNTP Unicast clients.

```
ZEQU0xxxxDL (config) # sntp unicast client enable
```

6.19 sntp unicast client poll

To enable polling for the SNTP Unicast clients, use the `sntp unicast client poll` command in Global Configuration mode. To disable the polling, use the `no` form of this command.

Syntax

- `sntp unicast client poll`
- `no sntp unicast client poll`

Parameters

N/A

Default Configuration

Polling is enabled.

Command Mode

Global Configuration mode

User Guidelines

The polling interval is 1024 seconds.

Example

The following example enables polling for SNTP unicast clients.

```
ZEQU0xxxxDL (config)# sntp unicast client poll
```

6.20 show clock

To display the time and date from the system clock, use the show clock command in User EXEC mode.

Syntax

show clock [detail]

Parameters

- detail—(Optional) Displays the time zone and summer time configuration.

Command Mode

User EXEC mode

User Guidelines

Before the time, there is displayed either a star (*), period (.), or blank:

- star (*)—The clock is invalid.
- period (.)—The clock was set manually or by Browser.
- blank—The clock was set by SNTP.

Examples

Example 1 - The following example displays the system time and date.

```
ZEQU0xxxxDL# show clock
* 15:29:03 PDT (UTC-7) Jun 17 2019
Time source is SNTP
Time from Browser is disabled
```

Example 2 - The following example displays the system time and date along with the time zone and summer time configuration.

```
ZEQU0xxxxDL# show clock detail
*03:45:23 UTC Apr 23 2019
Time source is sntp
Time from Browser is disabled
ZEQU0xxxxDL# show clock detail
*03:49:52 UTC Apr 1 2019
Time source is sntp
Time from Browser is disabled

Time zone (Static):
Offset is UTC+0

DHCP timezone: Disabled
```

6.21 show sntp configuration

To display the SNTP configuration on the device, use the show sntp configuration command in Privileged EXEC mode.

Syntax

```
show sntp configuration
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following example displays the device's current SNTP configuration.

```
ZEQU0xxxxDL# show sntp configuration
```

```
SNTP destination port : 123 .
```

```
Polling interval: 1024 seconds.
```

```
No MD5 authentication keys.
```

```
Authentication is not required for synchronization.
```

```
No trusted keys.
```

```
Unicast Clients: Enabled
```

```
Unicast Clients Polling: Enabled
```

```
Server          : time-a.timefreq.bldrdoc.gov
```

```
  Polling       : Enabled
```

```
  Encryption Key : Disabled
```

```
Server          : time-b.timefreq.bldrdoc.gov
```

```
  Polling       : Enabled
```

```
  Encryption Key : Disabled
```

```
Server          : time-c.timefreq.bldrdoc.gov
```

```
  Polling       : Enabled
```

```
  Encryption Key : Disabled
```

```
Broadcast Clients: disabled
```

```
Anycast Clients: disabled
```

```
No Broadcast Interfaces.
```

```
Source IPv4 interface:
```

```
Source IPv6 interface:
```

6.22 show sntp status

To display the SNTP servers status, use the show sntp status command in Privileged EXEC mode.

Syntax

```
show sntp status
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the SNTP servers status:

```
ZEQU0xxxxDL# show sntp status
```

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast

Reference time is afe2525e.70597b34 (00:10:22.438 PDT Jul 5 2019)

Unicast servers:

Server: 176.1.1.8

Source: DHCPv4 on VLAN 1

Status: Up

Last response: 19:58:22.289 PDT Feb 19 2019

Stratum Level: 1

Offset: 7.33mSec

Delay: 117.79mSec

Server: dns_server.comapany.com

Source: static

Status: Unknown

Last response: 12:17.17.987 PDT Feb 19 2019

Stratum Level: 1

Offset: 8.98mSec

Delay: 189.19mSec

Server: 3001:1:1::1

Source: DHCPv6 on VLAN 2

Status: Unknown

Last response:

Offset: mSec

Delay: mSec

Server: dns1.company.com

Source: DHCPv6 on VLAN 20

Status: Unknown

Last response:

Offset: mSec

Delay: mSec

Anycast servers:

Server: 176.1.11.8

Interface: VLAN 112

Status: Up

Last response: 9:53:21.789 PDT Feb 19 2019

Stratum Level: 10

Offset: 9.98mSec

Delay: 289.19mSec

Broadcast servers:

Server: 3001:1::12

Interface: VLAN 101

Last response: 9:53:21.789 PDT Feb 19 2019

Stratum Level: 255

6.23 show time-range

To display the time range configuration, use the show time-range command in User EXEC mode.

Syntax

show time-range time-range-name

Parameters

- time-range-name—Specifies the name of an existing time range.

Command Mode

User EXEC mode

Example

```
ZEQU0xxxxDL# show time-range
time-range http-allowed
absolute start 12:00 1 Jan 2019 end 12:00 31 Dec 2019
periodic Monday 12:00 to Wednesday 12:00
```

6.24 time-range

To define time ranges and to enter to Time-range Configuration mode, use the time-range command to define time ranges and to enter to Time-range Configuration mode in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

- `time-range time-range-name`
- `no time-range time-range-name`

Parameters

- `time-range-name`—Specifies the name for the time range. (Range: 1–32 characters).

Default Configuration

No time range is defined

Command Mode

Global Configuration mode

User Guidelines

After entering to Time-range Configuration mode with this command, use the absolute and periodic commands to actually configure the time-range. Multiple periodic commands are allowed in a time range. Only one absolute command is allowed.

If a time-range command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not evaluated again after the absolute end time is reached.

All time specifications are interpreted as local time.

To ensure that the time range entries take effect at the desired times, the software clock should be set by the user or by SNTP. If the software clock is not set by the user or by SNTP, the time range is not activated.

Example

```
ZEQU0xxxxDL (config)# time-range http-allowed
ZEQU0xxxxDL (config-time-range)# periodic mon 12:00 to wed 12:00
```

7 DHCP Relay Commands

7.1 ip dhcp relay enable (Global)

Use the ip dhcp relay enable Global Configuration mode command to enable the DHCP relay feature on the device. Use the no form of this command to disable the DHCP relay feature.

Syntax

- ip dhcp relay enable
- no ip dhcp relay enable

Parameters

N/A

Default Configuration

DHCP relay feature is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP relay feature on the device.

```
ZEQU0xxxxDL (config)# ip dhcp relay enable
```

7.2 ip dhcp relay enable (Interface)

Use the `ip dhcp relay enable` Interface Configuration mode command to enable the DHCP relay feature on an interface. Use the `no` form of this command to disable the DHCP relay agent feature on an interface.

Syntax

- `ip dhcp relay enable`
- `no ip dhcp relay enable`

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration mode

User Guidelines

The operational status of DHCP Relay on an interface is active if one of the following conditions exist:

- DHCP Relay is globally enabled, and there is an IP address defined on the interface.

Or

- DHCP Relay is globally enabled, there is no IP address defined on the interface, the interface is a VLAN, and option 82 is enabled.

Example

The following example enables DHCP Relay on VLAN 21.

```
ZEQU0xxxxDL(config)# interface vlan 21  
ZEQU0xxxxDL(config-if)# ip dhcp relay enable
```

7.3 ip dhcp relay address (Global)

Use the `ip dhcp relay address` Global Configuration mode command to define the DHCP servers available for the DHCP relay. Use the `no` form of this command to remove the server from the list.

Syntax

- `ip dhcp relay address ip-address`
- `no ip dhcp relay address [ip-address]`

Parameters

- `ip-address`—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip dhcp relay address` command to define a global DHCP Server IP address. To define a few DHCP Servers, use the command a few times.

To remove a DHCP Server, use the `no` form of the command with the `ip-address` argument.

The `no` form of the command without the `ip-address` argument deletes all global defined DHCP servers.

Example

The following example defines the DHCP server on the device.

```
ZEQU0xxxxDL (config)# ip dhcp relay address 176.16.1.1
```

7.4 show ip dhcp relay

Use the show ip dhcp relay EXEC mode command to display the DHCP relay information.

Syntax
show ip dhcp relay

Command Mode

User EXEC mode

Examples

Example 1. Option 82 is not supported:

```
ZEQU0xxxxDL# show ip dhcp relay
DHCP relay is Disabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 256
Number of DHCP Relays enabled on VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```

Example 2. Option 82 is supported (disabled):

```
ZEQU0xxxxDL# show ip dhcp relay
DHCP relay is Disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: gi1/0/1,po1-2
Active:
Inactive: gi1/0/1, po1-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
Active:
Inactive: 1, 2, 4, 5
Global Servers: 1.1.1.1 , 2.2.2.2
```

Example 3. Option 82 is supported (enabled):

```
ZEQU0xxxxDL# show ip dhcp relay
DHCP relay is Disabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: gi1/0/1,po1-2
Active: gi1/0/1
Inactive: po1-2
DHCP relay is enabled on VLANs: 1, 2, 4, 5
Active: 1, 2, 4, 5
Inactive:
Global Servers: 1.1.1.1 , 2.2.2.2
```

7.5 ip dhcp information option

Use the ip dhcp information option Global Configuration command to enable DHCP option-82 data insertion. Use the no form of this command to disable DHCP option-82 data insertion.

Syntax

- ip dhcp information option
- no ip dhcp information option

Parameters

N/A

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

Example

```
ZEQU0xxxxDL(config)# ip dhcp information option
```

7.6 show ip dhcp information option

The show ip dhcp information option EXEC mode command displays the DHCP Option 82 configuration.

Syntax

show ip dhcp information option

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays the DHCP Option 82 configuration.

```
ZEQU0xxxxDL# show ip dhcp information option
Relay agent Information option is Enabled
```

8 DHCP Server Commands

8.1 address (DHCP Host)

To manually bind an IP address to a DHCP client, use the address command in DHCP Pool Host Configuration mode. To remove the IP address binding to the client, use the no form of this command.

Syntax

address ip-address {mask | prefix-length} {client-identifier unique-identifier | hardware-address mac-address}

no address

Parameters

- address—Specifies the client IP address.
- mask—Specifies the client network mask.
- prefix-length—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- unique-identifier—Specifies the distinct client identification in dotted hexadecimal notation. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. For example, 01b7.0813.8811.66.
- mac-address—Specifies the client MAC address.

Default Configuration

No address are bound.

Command Mode

DHCP Pool Host Configuration mode

User Guidelines

To classify the DHCP client, DHCP server uses either the client identifier passed in Option 61, if the client-identifier keyword is configured or the client MAC address, if the hardware-address keyword is configured.

Example

The following example manually binds an IP address to a DHCP client.

```
ZEQU0xxxxDL (config)#ip dhcp pool host aaaa
ZEQU0xxxxDL (config-dhcp)# address 10.12.1.99 255.255.255.0 client-identifier
```

```
01b7.0813.8811.66
ZEU0xxxxDL (config-dhcp)#exit
ZEU0xxxxDL (config)#ip dhcp pool host bbbb
ZEU0xxxxDL (config-dhcp)# address 10.12.1.88 255.255.255.0 hardware-address
00:01:b7:08:13:88
ZEU0xxxxDL (config-dhcp)#exit
ZEU0xxxxDL (config)#
```

8.2 address (DHCP Network)

To configure the subnet number and mask for a DHCP address pool on a DHCP server, use the address command in DHCP Pool Network Configuration mode. To remove the subnet number and mask, use the no form of this command.

Syntax

address {network-number | low low-address high high-address} {mask | prefix-length}

no address

Parameters

- network-number—Specifies the IP address of the DHCP address pool.
- mask—Specifies the pool network mask.
- prefix-length—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- low low-address—Specifies the first IP address to use in the address range.
- high high-address—Specifies the last IP address to use in the address range.

Default Configuration

DHCP address pools are not configured.

If the low address is not specified, it defaults to the first IP address in the network. If the high address is not specified, it defaults to the last IP address in the network.

Command Mode

DHCP Pool Network Configuration mode

Example

The following example configures the subnet number and mask for a DHCP address pool on a DHCP server.

```
ZEQU0xxxxDL (conf ig-dhcp) # address 10.12.1.0 255.255.255.0
```

8.3 clear ip dhcp binding

To delete the dynamic address binding from the DHCP server database, use the `clear ip dhcp binding` command in Privileged EXEC mode.

Syntax

```
clear ip dhcp binding {address | *}
```

Parameters

- **address** —Specifies the binding address to delete from the DHCP database.
- ***** —Clears all dynamic bindings.

Command Mode

Privileged EXEC mode

User Guidelines

Typically, the address supplied denotes the client IP address. If the asterisk (*) character is specified as the address parameter, DHCP clears all dynamic bindings.

Use the `no ip dhcp pool` Global Configuration mode command to delete a manual binding.

Example

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
ZEQU0xxxx# clear ip dhcp binding 10.12.1.99
```

8.4 client-name

To define the name of a DHCP client, use the `client-name` command in DHCP Pool Host Configuration mode. To remove the client name, use the `no` form of this command.

Syntax

`client-name name`

`no client-name`

Parameters

- `name`—Specifies the client name, using standard ASCII characters. The client name should not include the domain name. For example, the .name Mars should not be specified as `mars.yahoo.com`. (Length: 1–32 characters).

Command Mode

DHCP Pool Host Configuration mode

Default Configuration

No client name is defined.

Example

The following example defines the string `client1` as the client name.

```
ZEQU0xxxxDL (config-dhcp)# client-name client1
```

8.5 default-router

To configure the default router list for a DHCP client, use the `default-router` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the default router list, use the `no` form of this command.

Syntax

`default-router ip-address [ip-address2 ... ip-address8]`

`no default-router`

Parameters

- `ip-address [ip-address2 ... ip-address8]`—Specifies the IP addresses of default routers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No default router is defined.

User Guidelines

The router IP address should be on the same subnet as the client subnet.

If the `auto-default-router` command is configured then the DHCP server returns an IP address defined on the input interface as a default router when an default router is not configured in the following case:

- ☐ Default router is not configurable.
- ☐ DHCP client is directly connected.
- ☐ IP Routing is enabled.
- ☐ Default router was required by the client.

Example

The following example specifies 10.12.1.99 as the default router IP address.

```
ZEQU0xxxxDL (config-dhcp)# default-router 10.12.1.99
```

8.6 dns-server

To configure the Domain Name System (DNS) IP server list available to a DHCP client, use the `dns-server` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the DNS server list, use the `no` form of this command.

Syntax

`dns-server ip-address [ip-address2 ... ip-address8]`

`no dns-server`

Parameters

- `ip-address [ip-address2 ... ip-address8]`—Specifies the IP addresses of DNS servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No DNS server is defined.

User Guidelines

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Example

The following example specifies 10.12.1.99 as the client domain name server IP address.

```
ZEQU0xxxxDL (config-dhcp)# dns-server 10.12.1.99
```

8.7 domain-name

To specify the domain name for a DHCP client, use the domain-name command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the domain name, use the no form of this command.

Syntax

domain-name domain

no domain-name

Parameters

- domain—Specifies the DHCP client domain name string. (Length: 1–32 characters).

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No domain name is defined.

Example

The following example specifies yahoo.com as the DHCP client domain name string.

```
ZEQU0xxxxDL (config-dhcp)# domain-name yahoo.com
```

8.8 ip dhcp excluded-address

To specify IP addresses that a DHCP server must not assign to DHCP clients, use the `ip dhcp excluded-address` command in Global Configuration mode. To remove the excluded IP addresses, use the `no` form of this command.

Syntax

```
ip dhcp excluded-address low-address [high-address]  
no ip dhcp excluded-address low-address [high-address]
```

Parameters

- `low-address`—Specifies the excluded IP address, or first IP address in an excluded address range.
- `high-address`—(Optional) Specifies the last IP address in the excluded address range.

Default Configuration

All IP pool addresses are assignable.

Command Mode

Global Configuration mode

User Guidelines

The DHCP server assumes that all pool addresses can be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

Example

The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199.

```
ZEQU0xxxxDL (config)#ip dhcp excluded-address 172. 16. 1. 100 172. 16. 1. 199
```

8.9 ip dhcp pool host

To configure a DHCP static address on a DHCP server and enter the DHCP Pool Host Configuration mode, use the `ip dhcp pool host` command in Global Configuration mode. To remove the address pool, use the `no` form of this command.

Syntax

`ip dhcp pool host name`

`no ip dhcp pool host name`

Parameters

- `name`—Specifies the DHCP address pool name. It can be either a symbolic string (such as `Engineering`) or an integer (such as `8`). (Length: 1–32 characters).

Default Configuration

DHCP hosts are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to the DHCP Pool Configuration mode. In this mode, the administrator can configure host parameters, such as the IP subnet number and default router list.

Example

The following example configures station as the DHCP address pool:

```
ZEQU0xxxxDL (config)#ip dhcp pool host station
ZEQU0xxxxDL (config-dhcp)#
```

8.10 ip dhcp pool network

To configure a DHCP address pool on a DHCP Server and enter DHCP Pool Network Configuration mode, use the `ip dhcp pool network` command in Global Configuration mode. To remove the address pool, use the `no` form of this command.

Syntax

`ip dhcp pool network name`

`no ip dhcp pool network name`

Parameters

- `name`—Specifies the DHCP address pool name. It can be either a symbolic string (such as ‘engineering’) or an integer (such as 8). (Length: 1–32 characters).

Default Configuration

DHCP address pools are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to DHCP Pool Network Configuration mode. In this mode, the administrator can configure pool parameters, such as the IP subnet number and default router list.

Example

The following example configures Pool1 as the DHCP address pool.

```
ZEQU0xxxxDL (config)#ip dhcp pool network Pool1
ZEQU0xxxxDL (config-dhcp)#
```

8.11 ip dhcp server

To enable the DHCP server features on the device, use the `ip dhcp server` command in Global Configuration mode. To disable the DHCP server, use the `no` form of this command.

Syntax

`ip dhcp server`

`no ip dhcp server`

Default Configuration

The DHCP server is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP server on the device:

```
ZEQU0xxxxDL (config) #ip dhcp server
```

8.12 lease

To configure the time duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client, use the lease command in DHCP Pool Network Configuration mode. To restore the default value, use the no form of this command.

Syntax

lease days [hours [minutes]] | infinite no

lease

Parameters

- days—Specifies the number of days in the lease.
- hours—(Optional) Specifies the number of hours in the lease. A days value must be supplied before configuring an hours value.
- minutes—(Optional) Specifies the number of minutes in the lease. A days value and an hours value must be supplied before configuring a minutes value.
- infinite—Specifies that the duration of the lease is unlimited.

Default Configuration

The default lease duration is 1 day.

Command Mode

DHCP Pool Network Configuration mode

Examples

The following example shows a 1-day lease.

```
ZEQU0xxxxDL (config-dhcp)#lease 1
```

The following example shows a one-hour lease.

```
ZEQU0xxxxDL (config-dhcp)#lease 0 1
```

The following example shows a one-minute lease.

```
ZEQU0xxxxDL (config-dhcp)#lease 0 0 1
```

The following example shows an infinite (unlimited) lease.

```
ZEQU0xxxxDL (config-dhcp)#lease infinite
```

8.13 netbios-name-server

To configure the NetBIOS Windows Internet Naming Service (WINS) server list that is available to Microsoft DHCP clients, use the netbios-name-server in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the NetBIOS name server list, use the no form of this command.

Syntax

```
netbios-name-server ip-address [ip-address2 ... ip-address8]
```

```
no netbios-name-server
```

Parameters

- ip-address [ip-address2 ... ip-address8]—Specifies the IP addresses of NetBIOS WINS name servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No bios server is defined.

Example

The following example specifies the IP address of a NetBIOS name server available to the DHCP client.

```
ZEQU0xxxxDL (config-dhcp)# netbios-name-server 10.12.1.90
```

8.14 netbios-node-type

To configure the NetBIOS node type for Microsoft DHCP clients, use the `netbios-node-type` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To return to default, use the `no` form of this command.

Syntax

```
netbios-node-type {b-node | p-node | m-node | h-node}
```

```
no netbios-node-type
```

Parameters

- `b-node`—Specifies the Broadcast NetBIOS node type.
- `p-node`—Specifies the Peer-to-peer NetBIOS node type.
- `m-node`—Specifies the Mixed NetBIOS node type.
- `h-node`—Specifies the Hybrid NetBIOS node type.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

`h-node` (Hybrid NetBIOS node type).

Example

The following example specifies the client's NetBIOS type as mixed.

```
ZEQU0xxxxDL(config-dhcp)# netbios node-type m-node
```

8.15 next-server

To configure the next server (siaddr) in the boot process of a DHCP client, use the next-server command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the next server, use the no form of this command.

Syntax

next-server ip-address

no next-server

Parameters

- ip-address—Specifies the IP address of the next server in the boot process.

Default Configuration

If the next-server command is not used to configure a boot server list, the DHCP server uses inbound interface helper addresses as boot servers.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

User Guidelines

The client will connect, using the SCP/TFTP protocol, to this server in order to download the configuration file.

Example

The following example specifies 10.12.1.99 as the IP address of the next server:

```
ZEQU0xxxxDL (config-dhcp) # next-server 10. 12. 1. 99
```

8.16 next-server-name

To configure the next server name (sname) in the boot process of a DHCP client, use the `next-server-name` command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the boot server name, use the `no` form of this command.

Syntax

`next-server-name name`

`no next-server-name`

Parameters

- `name`—Specifies the name of the next server in the boot process. (Length: 1–64 characters).

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No next server name is defined.

User Guidelines

The client will connect, using the SCP/TFTP protocol, to this server in order to download the configuration file.

Example

The following example specifies `www.bootserver.com` as the name of the next server in the boot process of a DHCP client.

```
ZEQU0xxxxDL(config-dhcp)# next-server www.bootserver.com
```

8.17 option

To configure the DHCP server options, use the option command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the options, use the no form of this command.

Syntax

option code {boolean {false | true} | integer value | ascii string | hex {string | none} | ip {address} | ip-list {ip-address1 [ip-address2 ...]}} [description text]

no option code

Parameters

- code—Specifies the DHCP option code. The supported values are defined in the User Guidelines.
- boolean {false | true}—Specifies a boolean value. The values are coded by integer values of one octet: 0 = false and 1 = true.
- integer value—Specifies an integer value. The option size depends on the option code.
- ascii string—Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white spaces must be delimited by quotation marks. The ASCII value is truncated to the first 160 characters entered.
- ip address—Specifies an IP address.
- ip-list {ip-address1 [ip-address2 ...]}—Specifies up to 8 IP addresses.
- hex string—Specifies dotted hexadecimal data. The hexadecimal value is truncated to the first 320 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.
- hex none—Specifies the zero-length hexadecimal string.
- description text—User description

Command Mode

DHCP Pool Network Configuration mode
DHCP Pool Host Configuration mode

User Guidelines

The option command enables defining any option that cannot be defined by other special CLI commands. A new definition of an option overrides the previous definition of this option.

The boolean keyword may be configured for the following options: 19, 20, 27, 29-31, 34, 36, and 39.

The integer keyword may be configured for the following options: 2, 13, 22-26, 35, 37-38, 132-134, and 211. The switch checks the value range and builds the value field of the size in accordance with the option definition.

The ascii keyword may be configured for the following options: 14, 17-18, 40, 64, 130, 209, and 210.

The ip keyword may be configured for the following options: 16, 28, 32, 128-129, 131, 135, and 136.

The ip-list keyword may be configured for the following options: 5, 7-11, 33, 41, 42, 45, 48, 49, 65, 68-76, and 150.

The hex keyword may be configured for any option in the range 1-254 except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255. The switch does not validate the syntax of an option defined by this format.

Examples

Example 1. The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding:

```
ZEQU0xxxxDL (config-dhcp)#option 19 boolean true description "IP Forwarding  
Enable/Disable Option"
```

Example 2. The following example configures DHCP option 2, which specifies the offset of the client in seconds from Coordinated Universal Time (UTC):

```
ZEQU0xxxxDL (config-dhcp)#option 2 integer 3600
```

Example 3. The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example:

```
ZEQU0xxxxDL (config-dhcp)#option 72 ip-list 172.16.3.252 172.16.3.253
```

8.18 show ip dhcp

To display the DHCP configuration, use the show ip dhcp command in User EXEC mode.

Syntax

show ip dhcp

Command Mode

User EXEC mode

Example

The following example displays the DHCP configuration.

```
ZEQU0xxxxDL#show ip dhcp
DHCP server is enabled.
```

8.19 show ip dhcp allocated

To display the allocated address or all the allocated addresses on the DHCP server, use the show ip dhcp allocated command in User EXEC mode.

Syntax

show ip dhcp allocated [ip-address]

Parameters

- ip-address —(Optional) Specifies the IP address.

Command Mode

User EXEC mode

Example

The following example displays the output of various forms of this command:

```
ZEQU0xxxxDL#show ip dhcp allocated
```

```
DHCP server enabled
```

```
The number of allocated entries is 3
```

IP address	Hardware address	Lease expiration	Type
172.16.1.11	00a0.9802.32de	Feb 01 1998 12:00 AM	Dynamic
172.16.3.253	02c7.f800.0422	Infinite	Automatic
172.16.3.254	02c7.f800.0422	Infinite	Static

```
ZEQU0xxxxDL#show ip dhcp allocated 172.16.1.11
```

```
DHCP server enabled
```

```
The number of allocated entries is 2
```

IP address	Hardware address	Lease expiration	Type
172.16.1.11	00a0.9802.32de	Feb 01 1998 12:00 AM	Dynamic

```
ZEQU0xxxxDL#show ip dhcp allocated 172.16.3.254
```

```
DHCP server enabled
```

```
The number of allocated entries is 2
```

IP address	Hardware address	Lease expiration	Type
172.16.3.254	02c7.f800.0422	Infinite	Static

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the host IP address.
Type	The manner in which the IP address was assigned to the host.

8.20 show ip dhcp binding

To display the specific address binding or all the address bindings on the DHCP server, use the show ip dhcp binding command in User EXEC mode.

Syntax

```
show ip dhcp binding [ip-address]
```

Parameters

- ip-address—(Optional) Specifies the IP address.

Command Mode

User EXEC mode

Examples

The following examples display the DHCP server binding address parameters.

```
ZEQU0xxxxDL# show ip dhcp binding
DHCP server enabled.
The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
```

IP address	Client Identifier	Lease Expiration	Type	State
1. 16. 1. 11	00a0. 9802. 32de	Feb 01 1998	dynamic	allocated
1. 16. 3. 23	02c7. f801. 0422	12:00AM	dynamic	expired
1. 16. 3. 24	02c7. f802. 0422		dynamic	declined
1. 16. 3. 25	02c7. f803. 0422		dynamic	pre-allocated
1. 16. 3. 26	02c7. f804. 0422		dynamic	declined

```
ZEQU0xxxxDL# show ip dhcp binding 1. 16. 1. 11
DHCP server enabled.
IP address Client Identifier Lease Expiration Type State
```

IP address	Client Identifier	Lease Expiration	Type	State
1. 16. 1. 11	00a0. 9802. 32de	Feb 01 1998 12:00 AM	dynamic	allocated

```
ZEQU0xxxxDL# show ip dhcp binding 1. 16. 3. 24
DHCP server enabled.
IP address Client Identifier Lease Expiration Type State
```

IP address	Client Identifier	Lease Expiration	Type	State
1. 16. 3. 24	02c7. f802. 0422		dynamic	declined

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Client Identifier	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the host IP address.
Type	The manner in which the IP address was assigned to the host.
State	The IP Address state.

8.21 show ip dhcp declined

To display the specific declined address or all of the declined addresses on the DHCP server, use the show ip dhcp declined command in User EXEC mode.

Syntax

```
show ip dhcp declined [ip-address]
```

Parameters

- ip-address—(Optional) Specifies the IP address.

Command Mode

User EXEC mode

Example

The following example displays the output of various forms of this command:

```
ZEQU0xxxxDL#show ip dhcp declined
DHCP server enabled
The number of declined entries is 2
IP address      Hardware address
172. 16. 1. 11   00a0. 9802. 32de
172. 16. 3. 254  02c7. f800. 0422
```

```
ZEQU0xxxxDL#show ip dhcp declined 172.16.1.11
DHCP server enabled
The number of declined entries is 2
IP address      Hardware address
172. 16. 1. 11   00a0. 9802. 32de
```

8.22 show ip dhcp excluded-addresses

To display the excluded addresses, use the `show ip dhcp excluded-addresses` command in User EXEC mode.

Syntax

`show ip dhcp excluded-addresses`

Command Mode

User EXEC mode

Example

The following example displays excluded addresses.

```
ZEQU0xxxxDL#show ip dhcp excluded-addresses
The number of excluded addresses ranges is 2
Excluded addresses:
10.1.1.212- 10.1.1.219, 10.1.2.212- 10.1.2.219
```

8.23 show ip dhcp expired

To display the specific expired address or all of the expired addresses on the DHCP server, use the show ip dhcp expired command in User EXEC mode.

Syntax

```
show ip dhcp expired [ip-address]
```

Parameters

- ip-address—(Optional) Specifies the IP.

Command Mode

User EXEC mode

Example

```
ZEQU0xxxxDL#show ip dhcp expired
DHCP server enabled
The number of expired entries is 1
IP address      Hardware address
172.16.1.11     00a0.9802.32de
172.16.3.254    02c7.f800.0422
```

```
ZEQU0xxxxDL#show ip dhcp expired 172.16.1.11
DHCP server enabled
The number of expired entries is 1
IP address      Hardware address
172.16.1.13     00a0.9802.32de
```

8.24 show ip dhcp pool host

To display the DHCP pool host configuration, use the `show ip dhcp pool host` command in User EXEC mode.

Syntax

`show ip dhcp pool host [address | name]`

Parameters

- `address`—(Optional) Specifies the client IP address.
- `name`—(Optional) Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode

User EXEC mode

Examples

Example 1. The following example displays the configuration of all DHCP host pools:

```
ZEQU0xxxxDL#show ip dhcp pool host
```

```
The number of host pools is 1
```

Name	IP Address	Hardware Address	Client Identifier

station	172.16.1.11		01b7.0813.8811.66

Example 2. The following example displays the DHCP pool host configuration of the pool named station:

```
ZEQU0xxxxDL# show ip dhcp pool host station
```

Name	IP Address	Hardware Address	Client Identifier

station	172.16.1.11		01b7.0813.8811.66

Mask: 255.255.0.0

Default router: 172.16.1.1

Client name: client1

DNS server: 10.12.1.99

Domain name: yahoo.com

NetBIOS name server: 10.12.1.90

NetBIOS node type: h-node

Next server: 10.12.1.99

Next-server-name: 10.12.1.100

Bootfile: Bootfile

Time server 10.12.1.99

Options:

Code	Type	Len	Value	Description
2	integer	4	3600	
14	ascii	16	qq/aaaa/bbb.txt	
19	boolean	1	false	"IP Forwarding Enable/Disable Option"
21	ip	4	134.14.14.1	
31	ip-list	8	1.1.1.1, 12.23.45.2	
47	hex	5	02af00aa00	

8.25 show ip dhcp pool network

To display the DHCP network configuration, use the `show ip dhcp pool network` command in User EXEC mode.

Syntax

```
show ip dhcp pool network [name]
```

Parameters

- `name`—(Optional) Specifies the DHCP pool name. (Length: 1-32 characters).

Command Mode

User EXEC mode

Examples

Example 1—The following example displays configuration of all DHCP network pools:

```
ZEQU0xxxxDL#show ip dhcp pool network
```

```
The number of network pools is 2
```

```
Name Address range mask Lease
```

```
-----
```

```
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
```

```
finance 10.1.2.8-10.1.2.178 255.255.255.0 0d:12h:0m
```

Example 2—The following example displays configuration of the DHCP network pool marketing:

```
ZEQU0xxxxDL# show ip dhcp pool network marketing
```

```
Name Address range mask Lease
```

```
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
```

```
Statistics:
```

```
All-range Available Free Pre-allocated Allocated Expired Declined
```

```
-----
```

```
162 150 68 50 20 3 9
```

```
Default router: 10.1.1.1
```

```
DNS server: 10.12.1.99
```

```
Domain name: yahoo.com
```

```
NetBIOS name server: 10.12.1.90
```

```
NetBIOS node type: h-node
```

```
Next server: 10.12.1.99
```

```
Next-server-name: 10.12.1.100
```

```
Bootfile: Bootfile
```

```
Time server 10.12.1.99
```

```
Options:
```

```
Code Type Len Value Description
```

```
-----
```

```
2 integer 4 3600
```

```
14 ascii 16 qq/aaaa/bbb.txt
```

```
19 boolean 1 false
```

```
"IP Forwarding Enable/Disable  
Option"
```

```
21 ip 4 134.14.14.1
```

```
31 ip-list 8 1.1.1.1, 12.23.45.2
```

```
47 hex 5 02af00aa00
```

8.26 show ip dhcp pre-allocated

To display the specific pre-allocated address or all the pre-allocated addresses on the DHCP server, use the show ip dhcp pre-allocated command in User EXEC mode.

Syntax

```
show ip dhcp pre-allocated [ip-address]
```

Parameters

- ip-address—(Optional) Specifies the IP.

Command Mode

User EXEC mode

Examples

```
ZEQU0xxxxDL# show ip dhcp pre-allocated
```

```
DHCP server enabled
```

```
The number of pre-allocated entries is 1
```

```
IP address      Hardware address
```

```
172.16.1.11    00a0.9802.32de
```

```
172.16.3.254  02c7.f800.0422
```

```
ZEQU0xxxxDL# show ip dhcp pre-allocated 172.16.1.11
```

```
DHCP server enabled
```

```
The number of pre-allocated entries is 1
```

```
IP address      Hardware address
```

```
172.16.1.15    00a0.9802.32de
```

8.27 show ip dhcp server statistics

To display DHCP server statistics, use the show ip dhcp server statistics command in User EXEC mode.

Syntax

```
show ip dhcp server statistics
```

Command Mode

User EXEC mode

Example

The following example displays DHCP server statistics

```
ZEQU0xxxxDL# show ip dhcp server statistics
DHCP server enabled
The number of network pools is 7
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of pre-allocated entries is 1
The number of allocated entries is 3
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
```

8.28 time-server

To specify the time servers list for a DHCP client, use the time-server command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the time servers list, use the no form of this command.

Syntax

```
time-server ip-address [ip-address2 ... ip-address8]
```

```
no time-server
```

Parameters

- ip-address [ip-address2 ... ip-address8]—Specifies the IP addresses of Time servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No time server is defined.

User Guidelines

The time server's IP address should be on the same subnet as the client subnet.

Example

The following example specifies 10.12.1.99 as the time server IP address.

```
ZEQU0xxxxDL (config-dhcp)# time-server 10. 12. 1. 99
```

9 DHCP Snooping Commands

9.1 ip dhcp snooping

Use the ip dhcp snooping Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the no form of this command to restore the default configuration.

Syntax

ip dhcp snooping

no ip dhcp snooping

Parameters

N/A

Default Configuration

DHCP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled by using the ip dhcp snooping vlan Global Configuration mode command.

Example

The following example enables DHCP Snooping on the device.

```
ZEQU0xxxxDL (config)#ip dhcp snooping
```

9.2 ip dhcp snooping vlan

Use the `ip dhcp snooping vlan` Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the `no` form of this command to disable DHCP Snooping on a VLAN.

Syntax

`ip dhcp snooping vlan vlan-id`

`no ip dhcp snooping vlan vlan-id`

Parameters

- `vlan-id`—Specifies the VLAN ID.

Default Configuration

DHCP Snooping on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

Example

The following example enables DHCP Snooping on VLAN 21.

```
ZEQU0xxxxDL(config)#ip dhcp snooping vlan 21
```

9.3 ip dhcp snooping trust

Use the ip dhcp snooping trust Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the no form of this command to restore the default configuration.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Parameters

N/A

Default Configuration

The interface is untrusted.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

Example

The following example configures gi1/0/4 as trusted for DHCP Snooping.

```
ZEQU0xxxxDL(config)#interface gi1/0/4
ZEQU0xxxxDL(config-if)#ip dhcp snooping trust
```

9.4 ip dhcp snooping information option allowed-untrusted

Use the ip dhcp snooping information option allowed-untrusted Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the no form of this command to drop these packets from an untrusted port.

Syntax

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Parameters

N/A

Default Configuration

DHCP packets with option-82 information from an untrusted port are discarded.

Command Mode

Global Configuration mode

Example

The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
ZEQU0xxxxDL (config)#ip dhcp snooping information option allowed-untrusted
```

9.5 ip dhcp snooping verify

Use the ip dhcp snooping verify Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the no form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

Syntax

ip dhcp snooping verify

no ip dhcp snooping verify

Default Configuration

The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

Command Mode

Global Configuration mode

Example

The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
ZEQU0xxxxDL(config)#ip dhcp snooping verify
```

9.6 ip dhcp snooping database

Use the ip dhcp snooping database Global Configuration mode command to enable the DHCP Snooping binding database file. Use the no form of this command to delete the DHCP Snooping binding database file.

Syntax

ip dhcp snooping database

no ip dhcp snooping database

Parameters

N/A

Default Configuration

The DHCP Snooping binding database file is not defined.

Command Mode

Global Configuration mode

User Guidelines

The DHCP Snooping binding database file resides on Flash.

To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured.

The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

Example

The following example enables the DHCP Snooping binding database file.

```
ZEQU0xxxxDL (config)#ip dhcp snooping database
```

9.7 ip dhcp snooping binding

Use the ip dhcp snooping binding Privileged EXEC mode command to configure the DHCP Snooping binding database and add dynamic binding entries to the database. Use the no form of this command to delete entries from the binding database.

Syntax

```
ip dhcp snooping binding mac-address vlan-id ip-address interface-id expiry  
{seconds | infinite}
```

```
no ip dhcp snooping binding mac-address vlan-id
```

Parameters

- mac-address—Specifies a MAC address.
- vlan-id—Specifies a VLAN number.
- ip-address—Specifies an IP address.
- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- expiry
 - seconds—Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967294).
 - infinite—Specifies infinite lease time.

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

Use the ip dhcp snooping binding command to add manually a dynamic entry to the DHCP database.

After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry would not be added to the configuration files. The entry would be displayed in the show commands as a “DHCP Snooping” entry.

An entry added by this command can override the existed dynamic entry.

An entry added by this command cannot override the existed static entry added by the ip source-guard binding command.

The entry is displayed in the show commands as a DHCP Snooping entry.

Use the `no ip dhcp snooping binding` command to delete manually a dynamic entry from the DHCP database.

A dynamic temporary entries for which the IP address is 0.0.0.0 cannot be deleted.

Example

The following example adds a binding entry to the DHCP Snooping binding database.

```
ZEQU0xxxxDL# ip dhcp snooping binding 0050.404C.73FF 23 176.10.1.1 gi1/0/4 expiry 900
```

9.8 clear ip dhcp snooping database

Use the clear ip dhcp snooping database Privileged EXEC mode command to clear the DHCP Snooping binding database.

Syntax

clear ip dhcp snooping database

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

The following example clears the DHCP Snooping binding database.

```
ZEQU0xxxxDL# clear ip dhcp snooping database
```

9.9 show ip dhcp snooping

Use the show ip dhcp snooping EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

Syntax

show ip dhcp snooping [interface-id]

Parameters

- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following example displays the DHCP snooping configuration.

```
ZEQU0xxxxDL#show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled Option 82
on untrusted port is allowed Verification of hwaddr
field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds
Interface          Trusted
-----
gi1/0/1            Yes
gi1/0/2            Yes
```

9.10 show ip dhcp snooping binding

Use the show ip dhcp snooping binding User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

Syntax

```
show ip dhcp snooping binding [mac-address mac-address] [ip-address  
ip-address] [vlan vlan-id] [interface-id]
```

Parameters

- mac-address mac-address—Specifies a MAC address.
- ip-address ip-address—Specifies an IP address.
- vlan vlan-id—Specifies a VLAN ID.
- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.-

```
ZEQU0xxxxDL#show ip dhcp snooping binding
```

```
Total number of binding: 2
```

```
Mac Address IP Address Lease (sec) Type VLAN Interface
```

```
-----
```

0050.404C.73FF	10.1.8.1	7983	snooping	3	gi1/0/1
0050.404C.7BC1	10.1.8.2	92332	snooping	3	gi1/0/2

```
-----
```

9.11 ip source-guard

Use the ip source-guard command in Configuration mode or Interface Configuration mode to enable IP Source Guard globally on a device or in Interface Configuration (Ethernet, Port-channel) mode to enable IP Source Guard on an interface.

Use the no form of this command to disable IP Source Guard on the device or on an interface.

Syntax

ip source-guard

no ip source-guard

Parameters

N/A

Default Configuration

IP Source Guard is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

IP Source Guard must be enabled globally before enabling IP Source Guard on an interface.

IP Source Guard is active only on DHCP snooping untrusted interfaces, and if at least one of the interface VLANs are DHCP snooping enabled.

Example

The following example enables IP Source Guard on gi1/0/4.

```
ZEQU0xxxxDL (config)#interface gi1/0/4
ZEQU0xxxxDL (config-if)#ip source-guard
```

9.12 ip source-guard binding

Use the ip source-guard binding Global Configuration mode command to configure the static IP source bindings on the device. Use the no form of this command to delete the static bindings.

Syntax

ip source-guard binding mac-address vlan-id ip-address interface-id

no ip source-guard binding mac-address vlan-id

Parameters

- mac-address—Specifies a MAC address.
- vlan-id—Specifies a VLAN number.
- ip-address—Specifies an IP address.
- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

No static binding exists.

Command Mode

Global Configuration mode

User Guidelines

Use the ip source-guard binding command to add a static entry to the DHCP database.

An entry added by this command can override the existed entry.

Use the no ip source-guard binding command to delete an entry from the DHCP database.

Example

The following example configures the static IP source bindings.

```
ZEQU0xxxxDL(config)#ip source-guard binding 0050.404C.73FF 23 176.10.1.1 gi1/0/4
```

9.13 ip source-guard tcam retries-freq

Use the ip source-guard tcam retries-freq Global Configuration mode command to set the frequency of retries for TCAM resources for inactive IP Source Guard addresses. Use the no form of this command to restore the default configuration.

Syntax

ip source-guard tcam retries-freq {seconds | never}

no ip source-guard tcam retries-freq

Parameters

- seconds—Specifies the retries frequency in seconds. (Range: 10–600)
- never—Disables automatic searching for TCAM resources.

Default Configuration

The default retries frequency is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses. Use this command to change the search frequency or to disable automatic retries for TCAM space.

The ip source-guard tcam locate command manually retries locating TCAM resources for the inactive IP Source Guard addresses.

The show ip source-guard inactive EXEC mode command displays the inactive IP Source Guard addresses.

Example

The following example sets the frequency of retries for TCAM resources to 2 minutes.

```
ZEQU0xxxxDL (config)#ip source-guard tcam retries-freq 120
```

9.14 ip source-guard tcam locate

Use the ip source-guard tcam locate Privileged EXEC mode command to manually retry to locate TCAM resources for inactive IP Source Guard addresses.

Syntax

```
ip source-guard tcam locate
```

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every 60 seconds the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Execute the ip source-guard tcam retries-freq command with the never keyword to disable automatic retries for TCAM space, and then execute this command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

The show ip source-guard inactive EXEC mode command displays the inactive IP source guard addresses.

Example

The following example manually retries to locate TCAM resources.

```
ZEQU0xxxxDL# ip source-guard tcam locate
```

9.15 show ip source-guard configuration

Use the show ip source-guard configuration EXEC mode command to display the IP source guard configuration for all interfaces or for a specific interface.

Syntax

show ip source-guard configuration [interface-id]

Parameters

- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following example displays the IP Source Guard configuration.

```
ZEQU0xxxxDL# show ip source-guard configuration
IP source guard is globally enabled.
Interface                               State
-----                               -
gi1/0/1                               Enabled
gi1/0/2                               Enabled
gi1/0/3                               Enabled
gi1/0/4                               Enabled
```

9.16 show ip source-guard status

Use the show ip source-guard status EXEC mode command to display the IP Source Guard status.

Syntax

show ip source-guard status [mac-address mac-address] [ip-address ip-address] [vlan vlan] [interface-id]

Parameters

- mac-address mac-address—Specifies a MAC address.
- ip-address ip-address—Specifies an IP address.
- vlan vlan-id—Specifies a VLAN ID.
- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following examples display the IP Source Guard status.

```
ZEQU0xxxxDL# show ip source-guard status
IP Source Guard: Enabled
```

Interface	Filter	Status	IP Address	MAC Address	VLAN Type	
gi1/0/1	IP	Active	10.1.8.1	0060.704C.73FF	3	DHCP
gi1/0/2	IP	Active	10.1.8.2	0060.704C.7BC1	3	Static
gi1/0/3	IP	Active	Deny all	0060.704C.7BC3	4	DHCP
gi1/0/4	IP	Inactive				

9.17 show ip source-guard inactive

Use the show ip source-guard inactive EXEC mode command to display the IP Source Guard inactive addresses.

Syntax

```
show ip source-guard inactive
```

Parameters

N/A

Command Mode

User EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Use the ip source-guard tcam retries-freq command to change the retry frequency or to disable automatic retries for TCAM space.

Use the ip source-guard tcam locate command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

This command displays the inactive IP source guard addresses.

Example

The following example displays the IP source guard inactive addresses.

```
ZEQU0xxxxDL# show ip source-guard inactive
TCAM resources search frequency: 60 seconds
```

Interface	Filter	IP address	MAC address	VLAN	Type	Reason
gi1/0/2	IP	10. 1. 8. 32	0060. 704C. 8	3	DHCP	Resource
gi1/0/3	IP		3FF			Problem
gi1/0/4	I					Trust port

9.18 show ip source-guard statistics

Use the show ip source-guard statistics EXEC mode command to display the Source Guard dynamic information (permitted stations).

Syntax

show ip source-guard statistics [vlan vlan-id]

Parameters

- vlan-id—Display the statistics on this VLAN.

Command Mode

User EXEC mode

Example

ZEQU0xxxxDL#show ip source-guard statistics		
VLAN	statically Permitted Stations	DHCP Snooping Permitted Stations
----	-----	-----
2	2	3

9.19 ip arp inspection

Use the `ip arp inspection` Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the `no` form of this command to disable ARP inspection.

Syntax

`ip arp inspection`

`no ip arp inspection`

Parameters

N/A

Default Configuration

ARP inspection is disabled.

Command Mode

Global Configuration mode

User Guidelines

Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

Example

The following example enables ARP inspection on the device.

```
ZEQU0xxxxDL (config) #ip arp inspection
```

9.20 ip arp inspection vlan

Use the `ip arp inspection vlan` Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the `no` form of this command to disable ARP inspection on a VLAN.

Syntax

`ip arp inspection vlan vlan-id`

`no ip arp inspection vlan vlan-id`

Parameters

- `vlan-id`—Specifies the VLAN ID.

Default Configuration

DHCP Snooping based ARP inspection on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables ARP inspection on a VLAN based on the DHCP snooping database. Use the `ip arp inspection list assign` command to enable static ARP inspection.

Example

The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
ZEQU0xxxxDL (config)#ip arp inspection vlan 23
```

9.21 ip arp inspection trust

Use the ip arp inspection trust Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the no form of this command to restore the default configuration.

Syntax

ip arp inspection trust

no ip arp inspection trust

Parameters

N/A

Default Configuration

The interface is untrusted.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The device does not check ARP packets that are received on the trusted interface; it only forwards the packets.

For untrusted interfaces, the device intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The device drops invalid packets and logs them in the log buffer according to the logging configuration specified with the ip arp inspection logging interval command.

Example

The following example configures gi1/0/3 as a trusted interface.

```
ZEQU0xxxxDL(config)# interface gi1/0/3
ZEQU0xxxxDL(config-if)# ip arp inspection trust
```

9.22 ip arp inspection validate

Use the `ip arp inspection validate` Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the `no` form of this command to restore the default configuration.

Syntax

`ip arp inspection validate`

`no ip arp inspection validate`

Parameters

N/A

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- **Source MAC address:** Compares the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
- **Destination MAC address:** Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
- **IP addresses:** Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example executes ARP inspection validation.

```
ZEQU0xxxxDL (config)#ip arp inspection validate
```

9.23 ip arp inspection list create

Use the `ip arp inspection list create` Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the `no` form of this command to delete the list.

Syntax

`ip arp inspection list create name`

`no ip arp inspection list create name`

Parameters

- `name`—Specifies the static ARP binding list name. (Length: 1–32 characters).

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip arp inspection list assign` command to assign the list to a VLAN.

Example

The following example creates the static ARP binding list ‘servers’ and enters the ARP list configuration mode.

```
ZEQU0xxxxDL(config)# ip arp inspection list create servers
```

9.24 ip mac

Use the ip mac ARP-list Configuration mode command to create a static ARP binding. Use the no form of this command to delete a static ARP binding.

Syntax

ip ip-address mac mac-address

no ip ip-address mac mac-address

Parameters

- ip-address—Specifies the IP address to be entered to the list.
- mac-address—Specifies the MAC address associated with the IP address.

Default Configuration

No static ARP binding is defined.

Command Mode

ARP-list Configuration mode

Example

The following example creates a static ARP binding.

```
ZEQU0xxxxDL (config)#ip arp inspection list create servers
ZEQU0xxxxDL (config-arp-list)#ip 172.16.1.1 mac 0050.404C.7321
ZEQU0xxxxDL (config-arp-list)#ip 172.16.1.2 mac 0050.404C.7322
```

9.25 ip arp inspection list assign

Use the `ip arp inspection list assign` Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the `no` form of this command to delete the assignment.

Syntax

`ip arp inspection list assign vlan-id name`

`no ip arp inspection list assign vlan-id`

Parameters

- `vlan-id`—Specifies the VLAN ID.
- `name`—Specifies the static ARP binding list name.

Default Configuration

No static ARP binding list assignment exists.

Command Mode

Global Configuration mode

Example

The following example assigns the static ARP binding list `Servers` to VLAN 37.

```
ZEQU0xxxxDL (config)#ip arp inspection list assign 37 servers
```

9.26 ip arp inspection logging interval

Use the ip arp inspection logging interval Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the no form of this command to restore the default configuration.

Syntax

ip arp inspection logging interval {seconds | infinite}

no ip arp inspection logging interval

Parameters

- seconds—Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- infinite—Specifies that SYSLOG messages are not generated.

Default Configuration

The default minimum ARP SYSLOG message logging time interval is 5 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
ZEQU0xxxxDL(config)#ip arp inspection logging interval 60
```

9.27 show ip arp inspection

Use the show ip arp inspection EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

Syntax

show ip arp inspection [interface-id]

Parameters

- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following example displays the ARP inspection configuration.

```
ZEQU0xxxxDL# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222 seconds
```

Interface	Trusted
gi1/0/1	Yes
gi1/0/2	Yes

9.28 show ip arp inspection list

Use the show ip arp inspection list Privileged EXEC mode command to display the static ARP binding list.

Syntax

show ip arp inspection list

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the static ARP binding list.

```
ZEQU0xxxxDL# show ip arp inspection list
```

```
List name: servers
```

```
Assigned to VLANs: 1,2
```

IP	ARP
-----	-----
172.16.1.1	0060.704C.7322
172.16.1.2	0060.704C.7322

9.29 show ip arp inspection statistics

Use the show ip arp inspection statistics EXEC command to display statistics for the following types of packets that have been processed by this feature: Forwarded, Dropped, IP/MAC Validation Failure.

Syntax

show ip arp inspection statistics [vlan vlan-id]

Parameters

- vlan-id—Specifies VLAN ID.

Command Mode

User EXEC mode

User Guidelines

To clear ARP Inspection counters use the clear ip arp inspection statistics command. Counters values are kept when disabling the ARP Inspection feature.

Example

ZEUQ0xxxxDL#show ip arp inspection statistics			
Vlan	Forwarded Packets	Dropped Packets	IP/MAC Failures
-----	-----	-----	-----
2	1500100	80	

9.30 clear ip arp inspection statistics

Use the clear ip arp inspection statistics Privileged EXEC mode command to clear statistics ARP Inspection statistics globally.

Syntax

clear ip arp inspection statistics [vlan vlan-id]

Parameters

- vlan-id—Specifies VLAN ID.

Command Mode

Privileged EXEC mode

Example

```
ZEQU0xxxx) #clear ip arp inspection statistics
```

10 DHCPv6 Commands

10.1 clear ipv6 dhcp client

To restart DHCP for an IPv6 client on an interface, use the `clear ipv6 dhcp client` command in Privileged EXEC mode.

Syntax

`clear ipv6 dhcp client interface-id`

Parameters

- `interface-id`—Interface identifier.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This command restarts DHCP for an IPv6 client on a specified interface after first releasing and unconfiguring previously-acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Example

The following example restarts the DHCP for IPv6 client on VLAN 100:

```
ZEQU0xxxxDL# clear ipv6 dhcp client vlan 100
```

10.2 ipv6 dhcp client information refresh

To configure the refresh time for IPv6 client information refresh time on a specified interface if the DHCPv6 server reply does not include the Information Refresh Time, use the `ipv6 dhcp client information refresh` command in Interface Configuration mode. To return to the default value of the refresh time, use the `no` form of this command.

Syntax

- `ipv6 dhcp client information refresh seconds | infinite`
- `no ipv6 dhcp client information refresh`

Parameters

- `seconds`—The refresh time, in seconds. The value cannot be less than the minimal acceptable refresh time configured by the `ipv6 dhcp client information refresh` command. The maximum value that can be used is 4,294,967,294 seconds (0xFFFFFFFFE).
- `infinite`—Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface Configuration mode

User Guidelines

The `ipv6 dhcp client information refresh` command specifies the information refresh time. If the server does not send an information refresh time option then a value configured by the command is used.

Use the `infinite` keyword, to prevent refresh, if the server does not send an information refresh time option.

Example

The following example configures an upper limit of 2 days:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ipv6 dhcp client information refresh 172800
ZEQU0xxxxDL(config-if)# exit
```

10.3 ipv6 dhcp client information refresh minimum

To configure the minimum acceptable refresh time on the specified interface, use the `ipv6 dhcp client information refresh minimum` command in Interface Configuration mode. To remove the configured refresh time, use the `no` form of this command.

Syntax

`ipv6 dhcp client information refresh minimum seconds | infinite no ipv6`

`dhcp client information refresh minimum`

Parameters

- `seconds`—The refresh time, in seconds. The minimum value that can be used is 600 seconds. The maximum value that can be used is 4,294,967,294 seconds (0xFFFFFFFF).
- `infinite`—Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface Configuration mode

User Guidelines

The `ipv6 dhcp client information refresh minimum` command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in the following situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

If you configure the `infinite` keyword client never refreshes the information.

Example

The following example configures an upper limit of 2 days:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ipv6 dhcp client information refresh 172800
ZEQU0xxxxDL(config-if)# exit
```

10.4 ipv6 dhcp duid-en

To set the Vendor Based on Enterprise Number DHCPv6 Unique Identified (DUID-EN) format, use the `ipv6 dhcp duid-en` command in Global Configuration mode.

To return to the default value, use the `no` form of this command.

Syntax

- `ipv6 dhcp duid-en enterprise-number identifier`
- `no ipv6 dhcp duid-en`

Parameters

- `enterprise-number`—The vendor's registered Private Enterprise number as maintained by IANA.
- `identifier`—The vendor-defined non-empty hex string (up to 64 hex characters). If the number of the character is not even '0' is added at the right. Each 2 hex characters can be separated by a period or colon.

Default Configuration

DUID Based on Link-layer Address (DUID-LL) is used. The base MAC Address is used as a Link-layer Address.

Command Mode

Global Configuration mode

User Guidelines

By default, the DHCPv6 uses the DUID Based on Link-layer Address (see RFC3315) with the Base MAC Address as a Link-layer Address.

Use this command to change the DUID format to the Vendor Based on Enterprise Number.

Examples

Example 1. The following sets the DUID-EN format:

```
ZEQU0xxxxDL (config)# ipv6 dhcp duid-en 9 0CC084D303000912
```

Example 2. The following sets the DUID-EN format using colons as delimiter:

```
ZEQU0xxxxDL (config)# ipv6 dhcp duid-en 9 0C:C0:84:D3:03:00:09:12
```

10.5 ipv6 dhcp relay destination (Global)

To specify a globally-defined relay destination address to which client messages are forwarded, use the `ipv6 dhcp relay destination` command in Global Configuration mode. To remove a relay destination address, use the `no` form of this command.

Syntax

- `ipv6 dhcp relay destination {ipv6-address [interface-id]} | interface-id`
- `no ipv6 dhcp relay destination [{ipv6-address [interface-id]} | interface-id]`

Parameters

- `ipv6-address [interface-id]`—Relay destination IPv6 address in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons. There are the following types of relay destination address:
 - Link-local Unicast address. A user must specify the `interface-id` argument for this kind of address.
 - Global Unicast IPv6 address. If the `interface-id` argument is omitted then the Routing table is used.
- `interface-id`—Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the well-known link-local Multicast address `All_DHCP_Relay_Agents_and_Servers` (FF02::1:2) through the link to which the output interface is connected.

Default Configuration

There is no globally-defined relay destination.

Command Mode

Global Configuration mode

User Guidelines

The `ipv6 dhcp relay destination` command specifies a destination address to which client messages are forwarded. The address is used by all DHCPv6 relays running on the switch. Up to 100 addresses can be defined.

When a relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per interface and globally.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination.

Unspecified, loopback, and Multicast addresses are not acceptable as the relay destination.

Use the `no` form of the command with the `ipv6-address` and `interface-id` arguments to remove only the given globally-defined address with the given output interface.

Use the `no` form of the command with the `ipv6-address` argument to remove only the given globally-defined address for all output interfaces.

The `no` form of the command without the arguments removes all the globally-defined addresses.

Examples

Example 1. The following example sets the relay unicast link-local destination address per VLAN 200:

```
ZEQU0xxxxDL (config)# ipv6 dhcp relay destination FE80::1:2 vlan 200
```

Example 2. The following example sets that client messages are forwarded to VLAN 200:

```
ZEQU0xxxxDL (config)# ipv6 dhcp relay destination vlan 200
```

Example 3. The following example sets the unicast global relay destination address:

```
ZEQU0xxxxDL (config)# ipv6 dhcp relay destination 3002::1:2
```

10.6 ipv6 dhcp relay destination (Interface)

To specify a destination address to which client messages are forwarded and to enable DHCP for IPv6 relay service on the interface, use the `ipv6 dhcp relay destination` command in Interface Configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the `no` form of this command.

Syntax

- `ipv6 dhcp relay destination [{ipv6-address [interface-id]} | interface-id]`
- `no ipv6 dhcp relay destination [{ipv6-address [interface-id]} | interface-id]`

Parameters

- `ipv6-address [interface-id]`—Relay destination IPv6 address in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons. There are the following types of relay destination address:
 - Link-local Unicast address. A user must specify the `interface-id` argument for this kind of address.
 - Global Unicast IPv6 address. If the `interface-id` argument is omitted then the Routing table is used.
- `interface-id`—Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the well-known link-local Multicast address `All_DHCP_Relay_Agents_and_Servers` (FF02::1:2) through the link to which the output interface is connected.

Default Configuration

The relay function is disabled, and there is no relay destination on an interface.

Command Mode

Interface Configuration mode

User Guidelines

This command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. Up to 10 addresses can be defined per one interface and up to 100 addresses can be defined per switch.

DHCPv6 Relay inserts the Interface-id option if an IPv6 global address is not defined on the interface on which the relay is running. The Interface-id field of the option is the interface name (a value of the `ifName` field of the `ifTable`) on which the relay is running.

When relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per interface and globally.

The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a Unicast address of a server or another relay agent, or it may be a Multicast address. There are two types of relay destination addresses:

- A link-local Unicast or Multicast IPv6 address, for which a user must specify an output interface.
- A global Unicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a Unicast or Multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a Multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local Multicast addresses are not acceptable as the relay destination.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface.

Use the no form of the command with arguments to remove a specific address. Use the no form of the command without arguments to remove all the defined addresses and to disable the relay on the interface.

Examples

Example 1. The following example sets the relay Unicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
ZEQU0xxxxDL (config)# interface vlan 100
ZEQU0xxxxDL (config-if)# ipv6 dhcp relay destination FE80::1:2 vlan 200
ZEQU0xxxxDL (config-if)# exit
```

Example 2. The following example sets the relay well known Multicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
ZEQU0xxxxDL (config)# interface vlan 100
ZEQU0xxxxDL (config-if)# ipv6 dhcp relay destination vlan 200
ZEQU0xxxxDL (config-if)# exit
```

Example 3. The following example sets the Unicast global relay destination address and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
ZEQU0xxxxDL (config)# interface vlan 100  
ZEQU0xxxxDL (config-if)# ipv6 dhcp relay destination 3002::1:2  
ZEQU0xxxxDL (config-if)# exit
```

Example 4. The following example enables DHCPv6 relay on VLAN 100:

```
ZEQU0xxxxDL (config)# interface vlan 100  
ZEQU0xxxxDL (config-if)# ipv6 dhcp relay destination  
ZEQU0xxxxDL (config-if)# exit
```

Example 5. The following example disables DHCPv6 relay on VLAN 100:

```
ZEQU0xxxxDL (config)# interface vlan 100  
ZEQU0xxxxDL (config-if)# no ipv6 dhcp relay destination  
ZEQU0xxxxDL (config-if)# exit
```

10.7 show ipv6 dhcp

To display the Dynamic DHCP unique identifier (DUID) on a specified device, use the `show ipv6 dhcp` command in User EXEC mode. This information is relevant for DHCPv6 clients and DHCPv6 relays.

Syntax

```
show ipv6 dhcp
```

Parameters

NA

Command Mode

User EXEC mode

User Guidelines

This command uses the DUID, which is based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID.

Examples

Example 1. The following is sample output from this command when the switch's DUID format is vendor based on enterprise number:

```
ZEQU0xxxxDL# show ipv6 dhcp
The switch's DHCPv6 unique identifier (DUID) is:
0002000000090CC084D303000912
  Format is: 2
  Enterprise Number is: 9
  Identifier : 0CC084D303000912
```

Example 2. The following is sample output from this command when the switch's DUID format is the vendor-based on link-layer address:

```
ZEQU0xxxxDL# show ipv6 dhcp
```

```
The switch' s DHCPv6 unique identifier (DUID) is: 000300010024012607AA
```

```
Format is: 3
```

```
Hardware type is: 1
```

```
MAC Address is: 0024.0126.07AA
```

Example 3. The following is sample output from this command when the switch's DUID format is vendorbased on link-layer address and DHCPv6 Relay is supported:

```
ZEQU0xxxxDL# show ipv6 dhcp
```

```
The switch' s DHCPv6 unique identifier (DUID) is: 000300010024012607AA
```

```
Format is: 3
```

```
Hardware type is: 1
```

```
MAC Address is: 0024.0126.07AA
```

```
Relay Destinations:
```

```
2001:001:250:A2FF:FEBF:A056
```

```
2001:1001:250:A2FF:FEBF:A056
```

```
2001:1011:250:A2FF:FEBF:A056 via VLAN 100
```

```
FE80::250:A2FF:FEBF:A056 via VLAN 100
```

```
FE80::250:A2FF:FEBF:A056 via VLAN 200
```

10.8 show ipv6 dhcp interface

To display DHCP for IPv6 interface information, use the `show ipv6 dhcp interface` command in User EXEC mode.

Syntax

`show ipv6 dhcp interface [interface-id]`

Parameters

- `interface-id`—Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If no interfaces are specified in the command, all interfaces on which DHCP for IPv6 (client or server) is enabled are displayed. If an interface is specified in the command, only information about the specified interface is displayed.

Note. This new output format is supported starting with the SW version supporting statefull configuration

Example

The following is sample output from this command when DHCPv6 client is enabled:

```
ZEQUOxxxxDL# show ipv6 dhcp interface
VLAN 100 is in client mode
  DHCP Operational mode is enabled
  Stateless Service is enabled
  Reconfigure service is enabled
  Information Refresh MinimumTime: 600 seconds
  Information Refresh Time: 86400 seconds
  Received Information Refresh Time: 3600 seconds
  Remain Information Refresh Time: 411 seconds
  DHCP server:
    Address FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
  Preference: 20
  DNS Servers: 1001::1, 2001::10
  DNS Domain Search List: company.com beta.org
  SNTP Servers: 2004::1
  POSIX Timezone string: EST5EDT4, M3. 2. 0/02:00, M11. 1. 0/02:00
  Configuration Server: config.company.com
  Configuration Path Name: qqg/config/aaa_config.cfg
  Indirect Image Path Name: qqg/config/aaa_image_name.txt
VLAN 110 is in client mode
  DHCP Operational mode is disabled (IPv6 is not enabled)
  Stateless Service is enabled
  Reconfigure service is enabled
```


Information Refresh MinimumTime: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds
VLAN 1000 is in client mode
DHCP Operational mode is disabled (Interface status is DOWN)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh MinimumTime: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds
VLAN 1010 is in relay mode
DHCP Operational mode is enabled
Relay source interface: VLAN 101
Relay destinations:
2001:001:250:A2FF:FEBF:A056
FE80::250:A2FF:FEBF:A056 via FastEthernet 1/0/1
VLAN 2000 is in client mode
DHCP Operational mode is disabled (Interface status is DOWN)
Stateless Service is enabled
Reconfigure service is enabled
Information Refresh MinimumTime: 600 seconds
Information Refresh Time: 86400 seconds
Remain Information Refresh Time: 0 seconds
DHCP server:
Address FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
Preference: 20
Received Information Refresh Time: 3600 seconds
DNS Servers: 1001::1, 2001::10
DNS Domain Search List: company.com beta.org
SNTP Servers: 2004::1
POSIX Timezone string: EST5EDT4, M3. 2. 0/02:00, M11. 1. 0/02:00
Configuration Server: config.company.com
Configuration Path Name: qq/qq/config/aaa_config.cfg
Indirect Image Path Name: qq/qq/config/aaa_image_name.txt

11 DNS Client Commands

11.1 clear host

Use the clear host command in privileged EXEC mode to delete dynamic hostname-to-address mapping entries from the DNS client name-to-address cache.

Syntax

clear host {hostname | *}

Parameters

- hostname—Name of the host for which hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.
- *—Specifies that all the dynamic hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.

Default Configuration

No hostname-to-address mapping entries are deleted from the DNS client name-to-address cache.

Command Mode

Privileged EXEC mode

User Guidelines

To remove the dynamic entry that provides mapping information for a single hostname, use the hostname argument. To remove all the dynamic entries, use the * keyword.

To define a static hostname-to-address mappings in the DNS hostname cache, use the ip host command.

To delete a static hostname-to-address mappings in the DNS hostname cache, use the no ip host command.

Example

The following example deletes all dynamic entries from the DNS client name-to-address cache.

```
ZEQU0xxxx# clear host *
```

11.2 ip domain lookup

Use the ip domain lookup command in Global Configuration mode to enable the IP Domain Naming System (DNS)-based host name-to-address translation.

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

Syntax

ip domain lookup

no ip domain lookup

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

The following example enables DNS-based host name-to-address translation.

```
ZEQU0xxxxDL(config)# ip domain lookup
```

11.3 ip domain name

Use the `ip domain name` command in Global Configuration mode. to define a default domain name that the switch uses to complete unqualified hostnames (names without a dotted-decimal domain name).

To delete the static defined default domain name, use the `no` form of this command.

Syntax

`ip domain name name`

`no ip domain name`

Parameters

name—Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. Length: 1–158 characters. Maximum label length of each domain level is 63 characters.

Default Configuration

No default domain name is defined.

Command Mode

Global Configuration mode

User Guidelines

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and the default domain name appended to it before being added to the host table.

Domain names and host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

The maximum size of each domain level is 63 characters. The maximum name size is 158 bytes.

Example

The following example defines the default domain name as ‘www.website.com’.

```
ZEQU0xxxxDL (config)# ip domain name website.com
```

11.4 ip domain polling-interval

Use the ip domain polling-interval command in Global Configuration mode to specify the polling interval.

Use the no form of this command to return to the default behavior.

Syntax

ip domain polling-interval seconds

no ip domain polling-interval

Parameters

seconds—Polling interval in seconds. The range is from $2 \cdot (R+1) \cdot T$ to 3600.

Default Configuration

The default value is $2 \cdot (R+1) \cdot T$, where

- R is a value configured by the ip domain retry command.
- T is a value configured by the ip domain timeout command.

Command Mode

Global Configuration mode

User Guidelines

Some applications communicate with the given IP address continuously. DNS clients for such applications, which have not received resolution of the IP address or have not detected a DNS server using a fixed number of retransmissions, return an error to the application and continue to send DNS Request messages for the IP address using the polling interval.

Example

The following example shows how to configure the polling interval of 100 seconds:

```
ZEQU0xxxxDL (config)# ip domain polling-interval 100
```

11.5 ip domain retry

Use the `ip domain retry` command in Global Configuration mode to specify the number of times the device will send Domain Name System (DNS) queries when there is no replay.

To return to the default behavior, use the `no` form of this command.

Syntax

`ip domain retry number`

`no ip domain retry`

Parameters

number—Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 16.

Default Configuration

The default value is 1.

Command Mode

Global Configuration mode

User Guidelines

The number argument specifies how many times the DNS query will be sent to a DNS server until the switch decides that the DNS server does not exist.

Example

The following example shows how to configure the switch to send out 10 DNS queries before giving up:

```
ZEQU0xxxxDL (config)# ip domain retry 10
```

11.6 ip domain timeout

Use the `ip domain timeout` command in Global Configuration mode to specify the amount of time to wait for a response to a DNS query.

To return to the default behavior, use the `no` form of this command.

Syntax

`ip domain timeout seconds`

`no ip domain timeout`

Parameters

`seconds`—Time, in seconds, to wait for a response to a DNS query. The range is from 1 to 60.

Default Configuration

The default value is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

Use the command to change the default time out value. Use the `no` form of this command to return to the default time out value.

Example

The following example shows how to configure the switch to wait 50 seconds for a response to a DNS query:

```
ZEQU0xxxxDL(config)# ip domain timeout 50
```

11.7 ip host

Use the `ip host` Global Configuration mode command to define the static host name-to-address mapping in the DNS host name cache.

Use the `no` form of this command to remove the static host name-to-address mapping.

Syntax

```
ip host hostname address1 [address2...address8]
```

```
no ip host name ip host name [address1...address8]
```

Parameters

- `hostname`—Name of the host. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters).
- `address1`—Associated host IP address (IPv4 or IPv6, if IPv6 stack is supported).
- `address2...address8`—Up to seven additional associated IP addresses, delimited by a single space (IPv4 or IPv6, if IPv6 stack is supported).

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

An IP application will receive the IP addresses in the following order:

1. IPv6 addresses in the order specified by the command.
2. IPv4 addresses in the order specified by the command.

Use the `no` format of the command with the `address1...address8` argument to delete the specified addresses. The entry is deleted if all its addresses are deleted.

Example

The following example defines a static host name-to-address mapping in the host cache.

```
ZEQU0xxxxDL (config)# ip host accounting.website.com 176.10.23.1
```

11.8 ip name-server

Use the ip name-server command in Global Configuration mode to specify the address of one or more name servers to use for name and address resolution.

Use the no form of this command to remove the static specified addresses.

Syntax

```
ip name-server server1-address [server-address2...erver-address8]
```

```
no ip name-server [server-address1...server-address8]
```

Parameters

- server-address1—IPv4 or IPv6 addresses of a single name server.
- server-address2...server-address8—IPv4 or IPv6 addresses of additional name servers.

Default Configuration

No name server IP addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

The preference of the servers is determined by the order in which they were entered.

Each ip name-server command replaces the configuration defined by the previous one (if one existed).

Example

The following example shows how to specify IPv4 hosts 172.16.1.111, 172.16.1.2, and IPv6 host 2001:0DB8::3 as the name servers:

```
ZEQU0xxxxDL (config) # ip name-server 172.16.1.111 172.16.1.2 2001:0DB8::3
```

11.9 show hosts

Use the show hosts command in privileged EXEC mode to display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

Syntax

```
show hosts [all | hostname]
```

Parameters

- all—The specified host name cache information is to be displayed for all configured DNS views. This is the default.
- hostname—The specified host name cache information displayed is to be limited to entries for a particular host name.

Command Mode

Privileged EXEC mode

Default Configuration

Default is all.

User Guidelines

This command displays the default domain name, a list of name server hosts, and the cached list of host names and addresses.

Example

The following is sample output with no parameters specified:

ZEQU0xxxxDL# **show hosts**

Name/address lookup is enabled

Domain Timeout: 3 seconds

Domain Retry: 4 times

Domain Polling Interval: 10 seconds

Default Domain Table

Domain	Source	Interface	Preference
example.com	static		
companyaaa.com	dhcpv6	vlan 100	1
companybbb.com	dhcpv6	vlan 100	2
companyccc.com	dhcpv6	vlan 1100	1

Name Server Table

IP Address	Source	Interface	Preference
192.0.2.204	static		1
192.0.2.205	static		2
192.0.2.105	static		3
2002:0:22AC::11:231A:0BB4	DHCPv6	vlan 100	1
192.1.122.20	DHCPv4	vlan 1	1
154.1.122.20	DHCPv4	vlan 1	2

Casche Table

Flags: (STD/DYN, OK/Ne/??)

STA - Static, DYN - Dynamic

OK - Okay, Ne - Negative Cache, ?? - No Response

Host	Addresses	Type	State	Remaining TTL
example1.company.com	173.0.2.30	Ipv4	DYN, OK	
example2.companyccc.com	no resolution	Ipv4	DYN, ??	
example3.companyccc.com	120.0.2.27	Ipv4	STD, OK	
example4.companyccc.com	173.0.2.30	IPV4	STD, OK	
example5.companyccc.com	no resolution	Ipv4	DYN, Ne	

12 Ethernet Configuration Commands

12.1 interface

To enter Interface configuration mode in order to configure an interface, use the interface Global Configuration mode command.

Syntax

interface interface-id

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, port-channel, VLAN, range, IP interface or tunnel.

Default Configuration

None

Command Mode

Global Configuration mode

Examples

Example 1—For Ethernet ports:

```
ZEQU0xxxxDL (config) # interface gi1/0/1
ZEQU0xxxxDL (config-if) #
```

Example 2—For port channels (LAGs):

```
ZEQU0xxxxDL (config) # interface po1
ZEQU0xxxxDL (config-if) #
```

12.2 interface range

To execute a command on multiple ports at the same time, use the interface range command.

Syntax

`interface range interface-id-list`

Parameters

`interface-id-list`—Specify list of interface IDs. The interface ID can be one of the following types: Ethernet port, VLAN, or port-channel

Default Configuration

None

Command Mode

Interface (Ethernet, Port Channel, VLAN) Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it does not stop the execution of the command on other interfaces.

Example

```
ZEQU0xxxxDL(config)# interface range gi1/0/1-4
ZEQU0xxxxDL(config-if-range)#
```

12.3 shutdown

To disable an interface, use the shutdown Interface Configuration mode command. To restart a disabled interface, use the no form of this command.

Syntax

shutdown

no shutdown

Parameters

This command has no arguments or keywords.

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration mode

User Guidelines

The shutdown command set a value of ifAdminStatus (see RFC 2863) to DOWN. When ifAdminStatus is changed to DOWN, ifOperStatus will be also changed to DOWN.

The DOWN state of ifOperStatus means that the interface does not transmit/receive messages from/to higher levels. For example, if you shut down a VLAN, on which an IP interface is configured, bridging into the VLAN continues, but the switch cannot transmit and receive IP traffic on the VLAN.

Notes:

- If the switch shuts down an Ethernet port it additionally shuts down the port MAC sublayer too.
- If the switch shuts down a port channel it additionally shuts down all ports of the port channel too.

Examples

Example 1—The following example disables gi1/0/4 operations.

```
ZEQU0xxxxDL(config)# interface gi1/0/4
ZEQU0xxxxDL(config-if)# shutdown
ZEQU0xxxxDL(config-if)#
```

Example 2—The following example restarts the disabled Ethernet port.

```
ZEQU0xxxxDL (config) # interface gi1/0/4  
ZEQU0xxxxDL (config-if) # no shutdown  
ZEQU0xxxxDL (config-if) #
```

Example 3—The following example shuts down vlan 100.

```
ZEQU0xxxxDL (config) # interface vlan 100  
ZEQU0xxxxDL (config-if) # shutdown  
ZEQU0xxxxDL (config-if) #
```

Example 4—The following example shuts down Port Channel 3.

```
ZEQU0xxxxDL (config) # interface po3  
ZEQU0xxxxDL (config-if) # shutdown  
ZEQU0xxxxDL (config-if) #
```

12.4 operation time

To control the time that the port is up, use the operation time Interface (Ethernet, Port Channel) Configuration mode command. To cancel the time range for the port operation time, use the no form of this command.

Syntax

operation time time-range-name

no operation time

Parameters

- time-range-name—Specifies a time range the port operates (in up state). When the Time Range is not in effect, the port is shutdown. (Range: 1–32 characters)

Default Configuration

There is no time range configured on the port authorized state.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The operation time command influences the port if the port status is up. This command defines the time frame during which the port stays up and at which time the port will be shutdown. While the port is in shutdown because of other reasons, this command has no effect.

The following example activates an operation time range (named "morning") on port gi1/0/1.

```
ZEQU0xxxxDL (config) # interface gi1/0/1
ZEQU0xxxxDL (config-if) # operation time morning
```

12.5 description

To add a description to an interface, use the description Interface (Ethernet, Port Channel) Configuration mode command. To remove the description, use the no form of this command.

Syntax description

string no description

Parameters

string—Specifies a comment or a description of the port to assist the user. (Length: 1–64 characters).

Default Configuration

The interface does not have a description.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example adds the description ‘SW#3’ to gi1/0/4.

```
ZEQU0xxxxDL (config) # interface gi1/0/4
ZEQU0xxxxDL (config-if) # description SW#3
```

12.6 speed

To configure the speed of a given Ethernet interface when not using auto-negotiation, use the speed Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

speed {10 | 100 | 1000 | 10000}

no speed

Parameters

- 10—Forces 10 Mbps operation
- 100—Forces 100 Mbps operation
- 1000—Forces 1000 Mbps operation
- 10000—Forces 10000 Mbps operation

Default Configuration

The port operates at its maximum speed capability.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The no speed command in a port-channel context returns each port in the port-channel to its maximum capability.

Example

The following example configures the speed of gi1/0/4 to 100 Mbps operation.

```
ZEQU0xxxxDL(config)# interface gi1/0/4
ZEQU0xxxxDL(config-if)# speed 100
```

12.7 duplex

To configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation, use the duplex Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

`duplex {half | full}`

`no duplex`

Parameters

- `half`—Forces half-duplex operation.
- `full`—Forces full-duplex operation.

Default Configuration

The interface operates in full duplex mode.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example configures gi1/0/1 to operate in full duplex mode.

```
ZEQU0xxxxDL (config)# interface gi1/0/1  
ZEQU0xxxxDL (config-if)# duplex full
```

12.8 negotiation

To enable auto-negotiation operation for the speed and duplex parameters and master-slave mode of a given interface, use the negotiation Interface (Ethernet, Port Channel) Configuration mode command. To disable auto-negotiation, use the no form of this command.

Syntax

negotiation [capability [capability2... capability5]] [preferred {master | slave}]

no negotiation

Parameters

- Capability—(Optional) Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h, 100f, 1000f, 10000f).
 - 10h—Advertise 10 half-duplex
 - 10f—Advertise 10 full-duplex
 - 100h—Advertise 100 half-duplex
 - 100f—Advertise 100 full-duplex
 - 1000f—Advertise 1000 full-duplex
 - 10000f—Advertise 10000 full-duplex
- Preferred—(Optional) Specifies the master-slave preference:
 - Master—Advertise master preference
 - Slave—Advertise slave preference

Default Configuration

If capability is unspecified, defaults to list of all the capabilities of the port and preferred slave mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables auto-negotiation on gi1/0/1.

```
ZEQU0xxxxDL (config)# interface gi1/0/1
ZEQU0xxxxDL (config-if)# negotiation
```

12.9 flowcontrol

To configure the Flow Control on a given interface, use the flowcontrol Interface (Ethernet, Port Channel) Configuration mode command. To disable Flow Control, use the no form of this command.

Syntax

flowcontrol {auto | on | off}

no flowcontrol

Parameters

- auto—Specifies auto-negotiation of Flow Control.
- on—Enables Flow Control.
- off—Disables Flow Control.

Default Configuration

Flow control is Disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the negotiation command to enable flow control auto.

Example

The following example enables Flow Control on port gi1/0/1

```
ZEQU0xxxxDL (config)# interface gi1/0/1
ZEQU0xxxxDL (config-if)# flowcontrol on
```

12.10 **mdix**

To enable cable crossover on a given interface, use the **mdix** Interface (Ethernet) Configuration mode command. To disable cable crossover, use the **no** form of this command.

Syntax

mdix {on | auto}

no mdix

Parameters

- **on**—Enables manual MDIX.
- **auto**—Enables automatic MDI/MDIX.

Default Configuration

The default setting is Auto.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example enables automatic crossover on port gi1/0/1.

```
ZEQU0xxxxDL (config) # interface gi1/0/1  
ZEQU0xxxxDL (config-if) # mdix auto
```

12.11 back-pressure

To enable back pressure on a specific interface, use the back-pressure Interface (Ethernet) Configuration mode command. To disable back pressure, use the no form of this command.

Syntax

back-pressure

no back-pressure

Parameters

This command has no arguments or keywords.

Default Configuration

Back pressure is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Back-pressure cannot be enabled whenEEE is enabled.

Example

The following example enables back pressure on port gi1/0/1.

```
ZEQU0xxxxDL (config)# interface gi1/0/1  
ZEQU0xxxxDL (config-if)# back-pressure
```

12.12 **port jumbo-frame**

To enable jumbo frames on the device, use the port jumbo-frame Global Configuration mode command. To disable jumbo frames, use the no form of this command.

Syntax

port jumbo-frame

no port jumbo-frame

Parameters

This command has no arguments or keywords.

Default Configuration

Jumbo frames are disabled on the device.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after resetting the device.

Example

The following example enables jumbo frames on the device.

```
ZEQU0xxxxDL (conf ig) # port jumbo-frame
```

12.13 clear counters

To clear counters on all or on a specific interface, use the clear counters Privileged EXEC mode command.

Syntax

clear counters [interface-id [- | ,]]

Parameters

[interface-id [- | ,]]—(Optional) Specifies one or the range interface ID. The interface ID can be one range of the following types: Ethernet port or port-channel.

Default Configuration

All counters are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears the statistics counters for gi1/0/1.

```
ZEQU0xxxxDL# clear counters gi1/0/25-26
```

12.14 set interface active

To reactivate an interface that was shut down, use the set interface active Privileged EXEC mode command.

Syntax

```
set interface active {interface-id}
```

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

User Guidelines

This command is used to activate interfaces that were configured to be active, but were shut down by the system.

Example

The following example reactivates gi1/0/1.

```
ZEQU0xxxxDL# set interface active gi1/0/1
```

12.15 errdisable recovery cause

To enable automatic re-activation of an interface after an Err-Disable shutdown, use the errdisable recovery cause Global Configuration mode command. To disable automatic re-activation, use the no form of this command.

Syntax

errdisable recovery cause {all | port-security | acl-deny | storm-control }

no errdisable recovery cause {all | port-security | acl-deny | storm-control }

Parameters

- all—Enables the error recovery mechanism for all reasons described below.
- port-security—Enables the error recovery mechanism for the port security Err-Disable state.
- acl-deny—Enables the error recovery mechanism for the ACL Deny Err-Disable state.
- storm-control—Enables the error recovery mechanism for the Storm Control Shutdown state.

Default Configuration

Automatic re-activation is disabled.

Command Mode

Global Configuration mode

Example

The following example enables automatic re-activation of an interface after all states.

```
ZEQU0xxxxDL (config)# errdisable recovery cause all
```

12.16 **errdisable recovery interval**

To set the error recovery timeout interval use the **errdisable recovery interval** Global Configuration mode command. To return to the default configuration, use the **no** form of this command.

Syntax

errdisable recovery interval seconds

no errdisable recovery interval

Parameters

seconds—Specifies the error recovery timeout interval in seconds. (Range: 30–86400)

Default Configuration

The default error recovery timeout interval is 300 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the error recovery timeout interval to 10 minutes.

```
ZEQU0xxxxDL (config)# errdisable recovery interval 600
```

12.17 errdisable recovery reset

To reactivate one or more interfaces that were shut down by a given application, use the `errdisable recovery reset` Privileged EXEC mode command. A single interface, multiple interfaces or all interfaces can be specified.

Syntax

`errdisable recovery reset {all | port-security | acl-deny | storm-control | interface interface-id}`

Parameters

- `all`—Reactivate all interfaces regardless of their state.
- `port-security`—Reactivate all interfaces in the Port Security Err-Disable state.
- `acl-deny`—Reactivate all interfaces in the ACL Deny Err-Disable state.
- `storm-control`—Reactivate all interfaces in the Storm Control Shutdown state.
- `interface interface-id`—Reactivate interfaces that were configured to be active, but were shut down by the system.

Default Configuration

None.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example reactivates interface `gi1/0/1`:

```
ZEQU0xxxxDL# errdisable recovery reset interface gi1/0/1
```

Example 2—The following example reactivates all interfaces regardless their state:

```
ZEQU0xxxxDL# errdisable recovery reset all
```

Example 3—The following example enables all interfaces in the port security Err-Disable state

```
ZEQU0xxxxDL# errdisable recovery reset port-security
```

12.18 **show interfaces configuration**

To display the configuration for all configured interfaces or for a specific interface, use the `show interfaces configuration` Privileged EXEC mode command.

Syntax

```
show interfaces configuration [interface-id | detailed]
```

Parameters

- `interface-id`—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- `detailed`—(Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display all interfaces. If `detailed` is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configuration of all configured interfaces:

ZEQU0xxxxDL# **show interfaces configuration**

Port	Type	Duplex	Speed	Neg	Flow control	Admin State	Back Pressure	Mdix Mode
gi1/0/1	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Auto
gi1/0/2	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Auto
:								
gi1/0/24	1G-Copper	Full	1000	Enabled	Off	Up	Disabled	Auto
te1/0/25	10G-Fiber	Full	10000	Disabled	Off	Up	Disabled	Off
te1/0/26	10G-Fiber	Full	10000	Disabled	Off	Up	Disabled	Off
te1/0/27	10G-Fiber	Full	10000	Disabled	Off	Up	Disabled	Off
te1/0/28	10G-Fiber	Full	10000	Disabled	Off	Up	Disabled	Off

Ch	Type	Speed	Neg	Flow control	Admin State
Po1	--	--	Enabled	Off	Up
Po2	--	--	Enabled	Off	Up
:					
Po31	--	--	Enabled	Off	Up
Po32	--	--	Enabled	Off	Up

12.19 show interfaces status

To display the status of all interfaces or of a specific interface, use the show interfaces status Privileged EXEC mode command.

Syntax

show interfaces status [interface-id | detailed]

Parameters

- interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed—(Optional) Displays information for non-present ports in addition to present ports.

Command Mode

Privileged EXEC mode

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Example

The following example displays the status of all configured interfaces.

ZEQU0xxxxDL# show interfaces status

Port	Type	Duplex	Speed	Neg	Flow ctrl	Link State	Back Pressure	Mdix Mode
gi1/0/1	1G-Copper	--	--	--	--	Down	--	--
gi1/0/2	1G-Copper	--	--	--	--	Down	--	--
:								
gi1/0/27	10G-Fiber	--	--	--	--	Down	--	--
gi1/0/28	10G-Fiber	--	--	--	--	Down	--	--

Ch	Type	Duplex	Speed	Neg	Flow control	Link State
Po1	--	--	--	--	--	Not Present
Po2	--	--	--	--	--	Not Present
:						
Po31	--	--	--	--	--	Not Present
Po32	--	--	--	--	--	Not Present

12.20 show interfaces advertise

To display auto-negotiation advertisement information for all configured interfaces or for a specific interface, use the show interfaces advertise Privileged EXEC mode command.

Syntax

show interfaces advertise [interface-id | detailed]

Parameters

- interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed—(Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Examples

The following examples display auto-negotiation information.

```
ZEQU0xxxxDL# show interfaces advertise
Port      Type      Neg      Preferred Operational Link Advertisement
-----
gi1/0/1    1G-Copper Enable    Master    1000f, 100f, 10f, 10h
gi1/0/2    1G-Copper Enable    Slave    1000f
.
.
.
te1/0/25   10G-Fiber Enable    Slave
te1/0/26   10G-Fiber Enable    Slave
.
.
.
Ch         Type      Neg      Preferred Operational Link Advertisement
-----
Po1        Unknown   Enabled   Slave
Po2        Unknown   Enabled   Slave
.
.
.
Po31       Unknown   Enabled   Slave
Po32       Unknown   Enabled   Slave

ZEQU0xxxxDL# show interfaces advertise gi1/0/1
Port:gi1/0/1
Type: 1G-Copper
Link state: Up
Auto Negotiation: Enabled
Preference: Master
```

	10h	10f	100h	100f	1000f
Admin Local link Advertisement	yes	yes	yes	yes	yes
Oper Local link Advertisement	yes	yes	yes	yes	yes
Remote Local link Advertisement	no	no	yes	yes	yes
Priority Resolution	-	-	-	-	yes

12.21 **show interfaces description**

To display the description for all configured interfaces or for a specific interface, use the `show interfaces description` Privileged EXEC mode command.

Syntax

`show interfaces description [interface-id | detailed]`

Parameters

- `interface-id`—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- `detailed`—(Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display description for all interfaces. If `detailed` is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the description of all configured interfaces.

```
ZEQU0xxxxDL# show interfaces description
```

Port	Description
-----	-----
gi1/0/1	Port that should be used for management only
gi1/0/2	
:	
te1/0/27	
te1/0/28	

Ch	Description
-----	-----
Po1	Output
Po2	
:	
Po31	
Po32	

12.22 show interfaces counters

To display traffic seen by all the physical interfaces or by a specific range interface, use the show interfaces counters Privileged EXEC mode command.

Syntax
show interfaces counters [interface-id [- | ,] | detailed]

Parameters

- interface-id [- | ,]—(Optional) Specifies one or the range interface IDs. The interface ID can be one or the range of the following types: Ethernet port or port-channel.
- detailed—(Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

Display counters for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode
Privileged EXEC mode

Example

The following example displays traffic seen by all the physical interfaces.

ZEQU0xxxxDL# show interfaces counters gi1/0/1

Port	InUcastPkts	InMcastPkts	InBcastPkts	InOctets
-----	-----	-----	-----	-----
gi1/0/1	0	0	0	0
Port	OutUcastPkts	OutMcastPkts	OutBcastPkts	OutOctets
-----	-----	-----	-----	-----
gi1/0/1	0	1	35	7051

FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0

Received Pause Frames: 0
Transmitted Pause Frames: 0

The following table describes the fields shown in the display.

Field	Description
InOctets	Number of received octets.
InUcastPkts	Number of received Unicast packets.
InMcastPkts	Number of received Unicast packets.
InBcastPkts	Number of received broadcast packets.
OutOctets	Number of transmitted octets.
OutUcastPkts	Number of transmitted Unicast packets.
OutMcastPkts	Number of transmitted Unicast packets.
OutBcastPkts	Number of transmitted Broadcast packets.
FCS Errors	Number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Number of frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	Number of frames that are involved in more than one collision and are subsequently transmitted successfully.
SQE Test Errors	Number of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.
Deferred Transmissions	Number of frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	Number of times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	Number of frames for which transmission fails due to excessive collisions.
Oversize Packets	Number of frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Number of frames for which reception fails due to an internal MAC sublayer receive error.

Received Pause Frames	Number of MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Number of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

12.23 **show ports jumbo-frame**

To display the whether jumbo frames are enabled on the device, use the show ports jumbo-frame Privileged EXEC mode command.

Syntax

```
show ports jumbo-frame
```

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays whether jumbo frames are enabled on the device.

```
ZEQU0xxxxDL# show ports jumbo-frame
```

```
Jumbo frames are disabled  
Jumbo frames will be enabled after reset
```

12.24 show errdisable recovery

To display the Err-Disable configuration of the device, use the show errdisable recovery Privileged EXEC mode command.

Syntax

show errdisable recovery

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the Err-Disable configuration.

ZEQU0xxxxDL# **show errdisable recovery**

Timer interval: 300 Seconds

Reason	Automatic Recovery
-----	-----
port-security	Disable
acl-deny	Enable
storm-control	Disable

12.25 **show errdisable interfaces**

To display the Err-Disable state of all interfaces or of a specific interface, use the `show errdisable interfaces` Privileged EXEC mode command.

Syntax

`show errdisable interfaces [interface-id]`

Parameters

- `interface`—(Optional) Port or port-channel number.

Default Configuration

Display for all interfaces.

Command Mode

Privileged EXEC mode

Example

The following example displays the Err-Disable state of `gi1/0/1`.

```
ZEQU0xxxxDL# show errdisable interfaces
```

Interface	Reason
-----	-----
gi1/0/1	acl-deny

12.26 **clear switchport monitor**

To clear monitored statistics on all or on a specific interface or interface list, use the `clear switchport monitor` Privileged EXEC mode command.

Syntax

`clear switchport monitor [interface-id-list]`

Parameters

`interface-id-list`—(Optional) Specifies a list of interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Default Configuration

All monitored statistics are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears the monitored statistics for `gi1/0/1`.

```
ZEQU0xxxxDL# clear switchport monitor gi1/0/1
```

12.27 **show switchport monitor**

To display the monitored statistics gathered by a specific interface, use the show switchport monitor Privileged EXEC mode command.

Syntax

```
show switchport monitor interface-id {seconds | minutes | hours } [utilization | tx | rx | frames]
```

```
show switchport monitor interface-id {days | weeks}
```

```
show switchport monitor utilization [interface-id]
```

Parameters

- interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- seconds— last 20 samples, sampled every 15 seconds.
- minutes —last 60 samples, sampled every 60 seconds (every round minute according to system time).
- hours —last 24 samples, sampled every 60 minutes (every round hour according to system time).
- days —last 7 samples, sampled every 24 hours (midnight to midnight according to system time).
- weeks —last 12 samples, sampled every 7 days (midnight saturday to midnight saturday according to system time).
- utilization —shows per time frame the utilization calculated.
- rx —shows received counters statistics.
- tx —shows sent counters statistics.
- frames —show received counters statistics collected per packet size.

Default Configuration

Display monitored statistics for an interface or all interface in case of show switchport monitor utilization command.

Command Mode

Privileged EXEC mode

User Guidelines

The show switchport monitor utilization is used to show a utilization summary per interface of the last time frame in each time frame(i.e. last minute, last hour, last day and last week). The show switchport monitor interface-id is used to show monitored statistics samples

collected per time frame and per counter types.

Examples

Example 1—The following example displays monitored statistics utilization seen by interface gi1/0/1.

ZEQU0xxxxDL#

show switchport monitor utilization gi1/0/1

	Last Minute Utilization		Last Hour Utilization		Last Day Utilization		Last Week Utilization	
Interface	RX	TX	RX	TX	RX	TX	RX	TX
gi1/0/1	0	0	0	0	0	0	0	0

Example 2—The following example displays monitored Tx statistics gathered in minutes time frame seen by interface gi1/0/1.

```
ZEQU0xxxxDL# show switchport monitor gi1/0/1 minutes tx
```

Sample Time	Unicast Frames Sent	Broadcast Frames Sent	Multicast Frames Sent	Total Octets Sent
05:32:00	0	0	0	0
05:33:00	0	0	0	0
05:34:00	0	0	0	0
:				
06:29:00	0	0	0	0
06:30:00	0	0	0	0
06:31:00	0	0	0	0

(~) Not all samples are available.

The following table describes the fields shown in the display.

Field	Description
Time	Time stamp of the current sample in system real time clock. For seconds, minutes and hours format is: hh:mm:ss. For days and weeks format is: <day of week> dd/mm/yy.
Good Octets Received	Number of received octets.
Good Unicast frames Received	Number of received Unicast packets.
Good Multicast frames Received	Number of received Unicast packets.
Good Broadcast frames Received	Number of received broadcast packets.
Good Octets Sent	Number of transmitted octets.
Good Unicast frames Sent	Number of transmitted Unicast packets. Sent
Good Multicast frames Sent	Nmber of transmitted Unicast packets. Sent
Good Broadcast frames Sent	Number of transmitted Broadcast packets.
Frames of 64 bytes	Number of received packets size of 64 bytes.
Frames of 65-127 bytes	Number of received packets size of 65-127 bytes.

Frames of 128-255	Number of received packets size of bytes 128-255 bytes.
Frames of 256-511	Number of received packets size of bytes 256-511 bytes.
Frames of 512-1023	Number of received packets size of bytes 512-1023 bytes.
Frames of 1024-1518	Number of received packets size of bytes 1024-1518 bytes.
Rx Error Frames Received	Number of frames received that are an integral number of octets in length but do not pass the FCS check.
Rx Utilization	Utilization in percentage for Received frames on the interface.
Tx Utilization	Utilization in percentage for Sent frames on the interface.
Rx/Tx Utilization	An average of the Rx Utilization and the Tx Utilization in percentage on the interface.

13 File System Commands

13.1 File Specification

The files may be located on:

- Network: TFTP servers and/or SCP servers - Network files
- Master FLASH - Flash files
- mass-storage connected to a SD Card port of Master - SD Card files. Only one mass-storage is supported.

Note. Although inside the switch supports the File System on FLASH of all stack units the File System CLI commands allow access only to flash files on Master. Needed file synchronizations between Master and other units is performed by the switch automatically.

Uniform Resource Locators (URLs) are used to specify the location of a file or a directory. The URL has the following syntax:

```
<url> ::= tftp://<location>/<file-path> |  
scp://[<username>:<password>@]<location>/<file-path> | sdcard://<file-path> |  
flash://<file-path> | <current-directory>[/<file-path>] |  
<higher-directory>[/<file-path>] | <file-path>  
<username> ::= string up to 70 characters  
<password> ::= string up to 70 characters  
<location> ::= <ipv4-address> | <ipv6-address> | <dns-name>  
<current-directory> ::= [{sdcard | flash}]:[.]  
<higher-directory> ::= [{sdcard | flash}]:..  
<file-path> ::= [<directories-path>]/<filename>  
<directories-path> ::= <directory-name> | <directories-path>/<directory-name> The  
maximum number of directories in <directories-path> is 16.  
<directory-name> ::= string up to 63 characters  
<filename> ::= string up to 63 characters
```

Filenames and directory names consist only of characters from the portable filename character set. The set includes the following characters:

- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- a b c d e f g h i j k l m n o p q r s t u v w x y z
- <space>
- 0 1 2 3 4 5 6 7 8 9 . _ -

The last three characters are the <period>, <underscore>, and <hyphen> characters, respectively. If an URL includes spaces it must be enclosed by the " characters.

For example:

"flash://aaa it/alpha/file 125"

The maximal length of URL is 160 characters

The following File systems are supported on SD Card:

- FAT32—Full support.
- NTFS—Partially support: read only.

The switch supports the following predefined URL aliases:

- active-image—The predefined URL alias specifies the Active Image file. This file has the following permissions:
 - readable
 - executable
- inactive-image—The predefined URL alias specifies the Inactive Image file. This file has the following permissions:
 - readable
 - executable
- running-config—The predefined URL alias specifies the Running Configuration File.
- startup-config—The predefined URL alias specifies the Startup Configuration File. This file has the following permissions:
 - readable
- localization. The predefined URL alias specifies the Secondary Language Dictionary file. This file has the following permissions:
 - readable
- logging. The predefined URL alias specifies the Syslog file. This file has the following permissions:
 - readable
- mirror-config. The predefined URL alias specifies the Mirror Configuration file. This file has the following permissions:
 - readable

Example

Example 1. The following example specifies a file on TFTP server using an IPv4 address:

```
tftp://1.1.1.1/aaa/cfg/file.txt
```

Example 2. The following example specifies a file on TFTP server using an IPv6 address:

```
tftp://3000:1:2::11/aaa/cfg/file.txt
```

Example 3. The following example specifies a file on TFTP server using a DNS name:

```
tftp://files.export.com/aaa/cfg/file.txt
```

Example 4. The following example specifies a file on FLASH:

```
flash://aaa/cfg/file.txt
```

Example 5. The following example specifies files using the current directory:

```
./cfg/file.txt
```

```
cfg/file.txt
```

Example 6. The following example specifies a file using the higher directory:

```
../cfg/file.txt
```

Example 7. The following example specifies a file on mass-storage device connected to the SD Card slot:

```
sdcard://aaa/cfg/file.txt
```

Example 8. The following example specifies files on mass-storage device connected to the SD Card slot using the current directory:

```
sdcard:aaa/cfg/file.txt
```

```
sdcard:./aaa/cfg/file.txt
```

Example 9. The following example specifies a file on mass-storage device connected to the SD Card slot using the higher directory:

```
sdcard:../aaa/cfg/file.txt
```

13.2 System Flash Files

The system files used by the switch are in the `flash://system/` directory. A user cannot add, delete, and rename the system files and directories, a user cannot create new directories under the system directory.

The system files are divided to the following groups:

- Inner System files. The files are created by the switch itself. For example the Syslog file.
- Files installed/Uninstalled by user. This group includes the following files:
 - Active and Inactive Images
 - Startup Configuration
 - Secondary Language Dictionary

The following boot commands install/uninstall these files:

- `boot config`
- `boot localization`
- `boot system`

Additionally, the following commands from previous versions can be used too:

- `copy (copy running-config startup-config)`
- `write`

Note. Reset to Factory Default removes all files from the FLASH except the following files:

- `active-image`
- `inactive-image`
- `mirror-config`
- `localization`

The flash://system/ directory contains the following directories:

- flash://system/images/—The directory contains the Active and Inactive Image files.
- flash://system/configuration/—The directory contains the Startup and Mirror Configuration files.
- flash://system/localization/—The directory contains the Secondary Language Dictionary file.
- flash://system/syslog/—The directory contains the Syslog file.
- flash://system/applications/—The directory contains inner system files managed by the switch applications.

13.3 Flash File System on Stack

The CLI commands provide access only to files located on Master FLASH. The switch performs automatic synchronization of files between Master and slaves:

- The Backup's Flash File system is fully synchronized with the Master's Flash File System.
- For non-Backup slave's File system only the following files are synchronized:
 - Active Image file
 - Inactive Image file
 - Secondary Language Dictionary file
 - All other files and directories are deleted.

13.4 boot config

To install a file as Startup Configuration after reload, use the boot config command in Privileged EXEC mode. To uninstall the Startup configuration file, use the no form of this command. To use SD card boot function, save the configuration file as “sd_config.cfg”, insert SD card in SD card slot, then turn on device.

Syntax

boot config startup-config-url

boot config running-config

no boot config

Parameters

- startup-config-url—the url of a file. The predefined URLs cannot be configured.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use the boot config startup-config-url command to install Startup Configuration from the startup-config-url file. The file must be a text file containing CLI commands. The command performs the following actions:

- Copies the file into the system directory flash://system/configuration/
- Converts the file format from the text format in the inner binary format.
- Installs the converted file as Startup Configuration. The previous Startup Configuration file is deleted.
- Installs Startup Configuration on Backup.

Use the boot config running-config command to install Startup Configuration from Running Configuration.

Use the no boot config command, to uninstall Startup Configuration. The uninstalled file is deleted.

Example

Example 1. The following example installs Startup Configuration from a TFTP server:

```
ZEQU0xxxxDL (config)# boot config  
tftp://1.1.1./confiration-files/config-v1.9.cfg
```

Example 2. TThe following example installs Startup Configuration from FLASH:

```
ZEQU0xxxxDL (config)# boot config  
flash://confiration-files/config-v1.9.cfg
```

Example 3. The following example unsets the current Startup Configuration:

```
ZEQU0xxxxDL (config)# no boot config
```

Example 4. The following example installs Startup Configuration from the Running Configuration file:

```
ZEQU0xxxxDL (config)# boot config running-config
```

13.5 boot localization

To install a file as the Secondary Language Dictionary file, use the boot localization command in Privileged EXEC mode. To return to the default, use the no form of this command.

Syntax

boot localization dictionary-url

no boot localization

Parameters

- dictionary-url—the url of a file. The predefined URLs cannot be configured.

Default Configuration

Default language.

Command Mode

Privileged EXEC mode

User Guidelines

Use the boot dictionary dictionary-url command to install Secondary Language Dictionary from the dictionary-url file. The command performs the following actions:

- Copies the file into the system directory flash://system/localization/
- Validates its format. If the file does not have the correct format the file is deleted and the command is finished with an error.
- Installs the copied file as Secondary Language Dictionary. The previous Secondary Language Dictionary file is deleted.
- Installs Secondary Language Dictionary on all the all other stack units.

Use the no boot dictionary command, to uninstall Secondary Language Dictionary. The uninstalled file is deleted.

Example

Example 1. The following example installs the Secondary Language Dictionary file from a TFTP server:

```
ZEQU0xxxxDL (config) # boot localization  
tftp://196.1.1.1/web-dictionaries/germany-dictionary.cfg
```

Example 2. The following example installs the Secondary Language Dictionary file from FLASH:

```
ZEQU0xxxxDL (config) # boot localization  
flash://web-dictionaries/germany-dictionary.cfg
```

13.6 boot system

To install the system (active) image that the switch loads at startup, use the boot system command in Privileged EXEC mode. To use SD card boot function, save the firmware file as “sd_runtime.rom”, insert SD card in SD card slot, then turn on device.

Syntax

boot system image-url

boot system inactive-image

Parameters

- image-url—The URL of a file. The predefined URLs cannot be configured.

Default Configuration

No default.

Command Mode

Privileged EXEC mode

User Guidelines

Use the boot system image-url command to install a new active image from the image-url file. The command performs the following actions:

- Copies the file into the system directory flash://system/image/
- Validates its format. If the file does not have the correct image format the file is deleted and the command is finished with an error.
- Installs the copied file as the active image that will be used be loaded at startup. The previous active image file is save as inactive image. The previous inactive image is deleted.
- Installs the new active image in all stack units.

Use the boot system inactive-image command to set the inactive image as active one and the active image as inactive one.

The command installs the inactive image as active in all stack units.

Use the show bootvar / show version command to display information about the active and inactive images.

Example

Example 1. The following example sets a new active image from a TFTP server:

```
ZEQU0xxxxDL (config)# boot system tftp://192.168.2.3/image/image-v1-1.rom
```

Example 2. The following example sets a new active image from FLASH:

```
ZEQU0xxxxDL (config)# boot system flash://images/image-v1-1.rom
```

Example 3. The following example sets the inactive image:

```
ZEQU0xxxxDL (config)# boot system inactive-image
```

13.7 cd

To change the current directory or file system, use the `cd` command in User EXEC mode.

Syntax

`cd url`

Parameters

- `url`—Specifies a directory on FLASH or on SD Card.

Default Configuration

The flash root directory (`flash://`)

Command Mode

User EXEC mode

User Guidelines

When a terminal session is started the current directory of the session is set to `flash://`. Use the `cd` command to change the current directory.

Example

Example 1. The following example sets a new current directory on FLASH:

```
ZEQU0xxxxDL> pwd
flash://
ZEQU0xxxxDL> cd date/aaa
ZEQU0xxxxDL> pwd
flash://date/aaa
```

Example 2. The following example sets a new current directory on SD Card:

```
ZEQU0xxxxDL> pwd
flash://
ZEQU0xxxxDL> cd sdcard://
ZEQU0xxxxDL> pwd
sdcard://
```

13.8 copy

To copy any file from a source to a destination, use the copy command in Privileged EXEC mode.

Syntax

copy src-url dst-url

copy src-url running-config

copy running-config startup-config

Parameters

- src-url—The location URL of the source file to be copied. The predefined URL aliases can be configured.
- dst-url—The URL of the destination file or the directory to be copied. The predefined URL aliases cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The following guidelines are relevant:

- You cannot copy one network file to another network file.
- Use the copy src-url dst-url command to copy any file. If the dst-url argument defines an existed flash file the command fails if this file does not have the writable permission. If the dst-url argument defines a directory file then the file is copied into the directory with the same name. No file format validation or conversion is performed. If the src-url argument and dst-url arguments define flash files the dst-url file will have the permissions of the src-url file. If the src-url argument defines a non-flash file and the dst-url argument defines a flash files the dst-url file will have the following permissions:
 - readable
 - writable
- Use the copy src-url running-config command to add a file to the Running Configuration file.
- The copy running-config startup-config command has exactly the same functionality as the boot config command with the running-config keyword.

Example

Example 1. The following example copies file file1 from the TFTP server 172.16.101.101 to the flash://aaaa/file1 file:

```
ZEQU0xxxxDL# copy tftp://172.16.101.101/file1 flash://aaa/file1
```

Example 2. The following example saves the Startup configuration file in the tftp://172.16.101.101/config.txt file:

```
ZEQU0xxxxDL# copy startup-config tftp://172.16.101.101/config.txt
```

Example 3. The following example copies the Running Configuration file to the Startup configuration:

```
ZEQU0xxxxDL# copy running-config startup-config
```

Example 4. The following example copies the Syslog file to a TFTP server:

```
ZEQU0xxxxDL# copy logging tftp://1.1.1.1/syslog.txt
```

Example 5. The following example copies a file from the mass-storage device connected to the SD Card slot to Flash:

```
ZEQU0xxxxDL# copy sdcard://aaa/file1.txt flash://dir1/file2
```

13.9 delete

To delete a local file, use the delete command in Privileged EXEC mode.

Syntax

delete url

delete startup-config

delete localization

Parameters

- url—Specifies the local URL of the local file to be deleted. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The delete url command cannot delete a network file.

Use the delete startup-config command to delete the Startup Configuration file. Use the delete localization command to delete the Secondary Language Dictionary file.

Example

Example 1. The following example deletes the file called 'backup/config' from FLASH:

```
ZEQU0xxxxDL# cd flash://backup/  
ZEQU0xxxxDL# delete aaa.ttt  
Delete flash://backup/aaa.ttt? [Y/N]Y
```

Example 2. The following example deletes the file called 'aaa/config' from the mass-storage device connected to the SD Card slot:

```
ZEQU0xxxxDL# delete sdcard://aaa/config  
Delete sdcard://aaa/config? [Y/N]Y
```

13.10 dir

To display a list of files on a file system, use the dir command in User EXEC mode.

Syntax

dir [url]

Parameters

- url—Specifies the local URL of the directory to be displayed. The predefined and network URLs cannot be configured. If the argument is omitted the current directory is used.

Command Mode

User EXEC mode

User Guidelines

The command cannot be applied to a network directory.

Use the dir command without the argument to display the current directory.

Examples

The following example displays the flash://mng/ directory:

```
ZEQU0xxxxDL> dir flash://system/
```

Permissions

d-directory

r-readable

w-writable

x-executable

163116K of 224552K are free

Directory of flash://system/

Permission	File Size	Last Modified	File Name
dr--	608	2017/06/19 05:44:28	/applications
dr--	160	2018/07/11 04:48:06	/certificates
dr--	304	2019/03/24 06:17:47	/configuration
dr-x	640	2018/07/14 05:31:17	/images
dr--	160	2017/02/03 07:05:00	/localization
dr--	224	2017/06/19 05:44:03	/sna
dr--	224	2017/06/19 05:44:03	/syslog

13.11 **mkdir**

To create a new directory, use the **mkdir** command in Privileged EXEC mode.

Syntax

mkdir url

Parameters

- **url**—Specifies the URL of the created directory. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The **mkdir** command cannot be applied to a network directory.

The **mkdir** command cannot create a directory into the **flash://system/** directory. All directories defined in the **url** argument except the created one must exist.

Example

Example 1. The following example creates a directory on FLASH:

```
ZEQU0xxxxDL# mkdir flash://date/aaa/
```

Example 2. The following example creates a directory on the mass-storage device connected to the SD Card slot:

```
ZEQU0xxxxDL# mkdir sdcard://newdir/
```

13.12 more

To display the contents of a file, use the more command in User EXEC mode.

Syntax

more url

Parameters

- url—Specifies the local URL or predefined file name of the file to display.

Command Mode

User EXEC mode

User Guidelines

The command cannot be applied to a network file.

The more running-config command displays the same output as the show running-config command regardless the specified format.

The more startup-config command displays the same output as the show startup-config command regardless the specified format.

The more active-image and more inactive-image commands display only the version number of the image regardless the specified format.

Example

The following example displays the running configuration file contents:

```
ZEQU0xxxxDL> more running-config
:
line console
exec-timeout 0
exit
line telnet
exec-timeout 0
exit
:
```

13.13 pwd

To show the current directory, use the pwd command in User EXEC mode.

Syntax

pwd [sdcard: | flash:]

Parameters

- sdcard:—Display the current directory on the SD Card driver.
- flash:—Display the current directory on the FLASH driver.

Command Mode

User EXEC mode

User Guidelines

Use the pwd sdcard: | flash: command to show the current directory on the specified driver.
Use the pwd command to show the current directory set by the recent cd command.

Example

The following example uses the cd command to change the current directory and then uses the pwd command to display that current directory:

```
ZEQU0xxxxDL> pwd

flash://
ZEQU0xxxxDL> cd date/aaa
ZEQU0xxxxDL> pwd
flash://date/aaa
```

13.14 **reboot**

To reboot the operating system, use the reboot command in Privileged EXEC mode.

Syntax

reboot

reboot {in hhh:mm | mmm | at hh:mm [day month]}

reboot cancel

Parameters

- in hhh:mm | mmm—Schedules a reboot of the image to take effect in the specified minutes or hours and minutes. The reboot must take place within approximately 24 days.
- at hh:mm—Schedules a reboot of the image to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reboot is scheduled to take place at the specified time and date. If you do not specify the month and day, the reboot takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reboot for midnight. The reboot must take place within 24 hours.
- day—Number of the day in the range from 1 to 31.
- month—Month of the year. (Range: Jan–Dec)
- cancel—Cancels a scheduled reboot.

Command Mode

Privileged EXEC mode

User Guidelines

Use the reboot command to reboot the switch.

Use the reboot {in hhh:mm | mmm | at hh:mm [day month]} command the command to specify scheduled switch reboot.

The at keyword can be configured only if the system clock has been set on the switch.

When you specify the reboot time using the at keyword, if you specify the month and day, the reboot takes place at the specified time and date. If you do not specify the month and day, the reboot takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reboot for midnight. The reboot must take place within 24 days.

Use the reboot cancel command to cancel the scheduled reboot.

To display information about a scheduled reboot, use the show reboot command.

Example

Example 1. The following example reboots the switch:

```
ZEQU0xxxxDL# reboot
```

This command will reset the whole system and disconnect your current session. Do you want to continue? (Y/N) [Y]

Example 2. The following example reboots the image in 10 minutes:

```
ZEQU0xxxxDL# reboot in 10
```

This command will reset the whole system and disconnect your current session. Reboot is scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10 minutes). Do you want to continue? (Y/N) [Y]

Example 3. The following example reboots the image at 12:10 24 Aug:

```
ZEQU0xxxxDL# reboot at 12:10 24 Aug
```

This command will reset the whole system and disconnect your current session. Reboot is scheduled for 12:10:00 UTC Sun Aug 24 2014 (in 1 hours and 12 minutes). Do you want to continue ? (Y/N) [N]

Example 4. The following example reboots the image at 13:00:

```
ZEQU0xxxxDL# reboot at 13:00 soft
```

This command will reset the whole system and disconnect your current session. Reboot is scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour and 3 minutes). Do you want to continue? (Y/N) [Y]

Example 5. The following example cancels a reboot.

```
ZEQU0xxxxDL# reboot cancel
```

Reboot cancelled.

13.15 rename

To rename a local file or directory, use the rename command in Privileged EXEC mode.

Syntax

rename url new-url

Parameters

- url—Specifies the URL of the file or directory to be renamed. The predefined and network URLs cannot be configured.
- new-url—Specifies the new URL of the renamed file or directory. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The url and new-url arguments must specify the same driver. The

command cannot rename a network file or network directory.

The command cannot rename a file or directory into the flash://system directory.

Examples

Example 1. The following example renames the flash://bin/text1.txt file to flash://archive/text1sav.txt:

```
ZEQU0xxxxDL# cd flash://archive
```

```
ZEQU0xxxxDL# rename flash://bin/text1.txt ./text1sav.txt
```

Example 2. The following example renames the flash://a/b directory to the flash://e/g/h directory:

```
ZEQU0xxxxDL# pwd
flash://a/b/c/d
ZEQU0xxxxDL> dir flash://a
Permissions
  · d-directory
  · r-readable
  · w-writable
  · x-executable
134560K of 520000K are free
Directory of flash://a
```

File Name	Permission	File Size	Last Modified
-----	-----	-----	-----
b	drw-	472148	Dec 13 2010 15:49:36

```
ZEQU0xxxxDL> dir flash://e/g/h
Permissions
  · d-directory
  · r-readable
  · w-writable
  · x-executable
134560K of 520000K are free
Directory of flash://e/g/h
```

File Name	Permission	File Size	Last Modified
-----	-----	-----	-----

```
ZEQU0xxxxDL# rename flash://a/b flash://e/g/h
ZEQU0xxxxDL# pwd
flash://e/g/h/c/d
ZEQU0xxxxDL> dir flash://a
Permissions
  · d-directory
  · r-readable
  · w-writable
  · x-executable
134560K of 520000K are free
Directory of flash://mng/
```

File Name	Permission	File Size	Last Modified
-----	-----	-----	-----

```
ZEQU0xxxxDL> dir flash://e/g/h
Permissions
  · d-directory
  · r-readable
  · w-writable
  · x-executable
134560K of 520000K are free
Directory of flash://e/g/h
```

File Name	Permission	File Size	Last Modified
-----	-----	-----	-----
c	drw-	720148	Dec 12 2010 17:49:36

13.16 **rmdir**

To remove a local directory, use the **rmdir** command in Privileged EXEC mode.

Syntax

rmdir url

Parameters

- **url**—Specifies the URL of the file or directory to be deleted. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

Only empty directory can be deleted.

The command cannot remove a network directory.

The command cannot remove a directory into the flash://system directory.

Example

Example 1. The following example removes the directory called ‘backup/config/’ from FLASH:

```
ZEQU0xxxxDL# rmdir flash://backup/config/  
Remove flash://backup/config? [Y/N]Y
```

Example 2. The following example removes the directory called ‘aaa/config’ from the mass-storage device connected to the SD Card slot:

```
ZEQU0xxxxDL# rmdir sdcard://aaa/config/  
Remove directory sdcard://aaa/config? [Y/N]Y
```

13.17 **show bootvar / show version**

To display the active system image file that was loaded by the device at startup, and to display the system image file that will be loaded after rebooting the switch, use the show bootvar or show version command in User EXEC mode.

Syntax

show bootvar

show version

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

The show bootvar and show version commands have the same functionality.

Example

Example 1. The following example gives an example of the command output after reload:

```
ZEQU0xxxxDL# show bootvar
Active-image: flash://system/images/pn36241c_v10000.rom
  Version: 1.0.0.00
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 04-Jul-2019
  Time: 15:03:07
Inactive-image: flash://system/images/pn36241c_v10002.rom
  Version: 1.0.0.02
  MD5 Digest: 3FA000012857D8855AABC7577AB8999
  Date: 04-Aug-2019
  Time: 11:13:17
```

Example 2. This example continues the inactive one, after applying the boot system tftp://1.1.1.1/ pn36241c_v10000.rom command:

```
ZEQU0xxxxDL# show bootvar
Active-image: flash://system/images/pn36241c_v10000.rom
  Version: 1.0.0.00
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2017
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/pn36241c_v10001.rom
  Version: 1.0.0.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2017
  Time: 23:11:17
  Active after reboot
```

Example 3. This example continues the inactive one, after a system reload:

```
ZEQU0xxxxDL# show bootvar
Active-image: flash://system/images/pn36241c_v10001.rom
  Version: 1.0.0.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2017
  Time: 23:11:17
Inactive-image: flash://system/images/pn36241c_v10000.rom
  Version: 1.0.0.00
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2017
  Time: 15:03:07
```

Example 4. This example continues the inactive one, after applying the boot system inactive-image command:

```
ZEQU0xxxxDL# show bootvar
Active-image: flash://system/images/pn36241c_v10001.rom
  Version: 1.0.0.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2017
  Time: 23:11:17
  Inactive after reboot
Inactive-image: flash://system/images/pn36241c_v10000.rom
  Version: 1.0.0.00
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2017
  Time: 15:03:07
  Active after reboot
```

Example 5. This example continues the inactive one, after a system reload:

```
ZEQU0xxxxDL# show bootvar
Active-image: flash://system/images/pn36241c_v10000.rom
  Version: 1.0.0.00
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2017
  Time: 15:03:07
Inactive-image: flash://system/images/pn36241c_v10000.rom
  Version: 1.0.0.00
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2017
  Time: 15:03:07
```

13.18 **show reboot**

To display the reboot status on the switch, use the show reboot command in User EXEC mode.

Syntax

show reboot

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

You can use the show reboot command to display a pending image reboot. To cancel the reboot, use the reboot command with the cancel keyword.

Example

Example 1. The following example displays information when scheduled reboot has been configured:

```
ZEQU0xxxxDL> show reboot  
Reload is scheduled to occur in 16 hours and 38 minutes.
```

Example 2. The following example displays information when scheduled reload has not been configured:

```
ZEQU0xxxxDL> show reload  
Scheduled-reload is not configured.
```

13.19 **show running-config**

To display the contents of the currently running configuration file, use the show running-config command in Privileged EXEC mode.

show running-config [interface interface-id-list | detailed | brief]

Parameters

- interface interface-id-list—Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.
- detailed—Displays configuration with SSL and SSH keys.
- brief—Displays configuration without SSL and SSH keys.

Default Configuration

All interfaces are displayed. If the detailed or brief keyword is not specified, the brief keyword is applied.

Command Mode

Privileged EXEC mode

Example

The following example displays the running configuration file contents.

```
ZEQU0xxxxDL# show running-config

config-file-header
ZEQU0xxxxDL
v1.0.0.00 / RLINUX_913_129
CLI v1.0
@
!
unit-type-control-start
unit-type unit 1 network gi uplink te
unit-type unit 2 network gi uplink te
unit-type-control-end
!
interface vlan 1
ip address 192.168.11.101 255.255.255.0
!
interface vlan 2
ip address 192.168.12.101 255.255.255.0
!
interface vlan 100
ip address 192.168.10.101 255.255.255.0
!
interface GigabitEthernet1/0/1
!
.
.
.
interface TenGigabitEthernet1/0/28
!
hostname ZEQU0xxxxDL
```

13.20 **show startup-config**

To display the Startup Configuration file contents, use the `show startup-config` command in Privileged EXEC mode.

Syntax

```
show startup-config [interface interface-id-list]
```

Parameters

- `interface interface-id-list`—Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.

Command Mode

Privileged EXEC mode

Example

The following example displays the startup configuration file contents.

```
ZEQU0xxxxDL# show startup-config

config-file-header
ZEQU0xxxxDL
v1.0.0.00 / RLINUX_913_129
CLI v1.0
@
!
unit-type-control-start
unit-type unit 1 network gi uplink te
unit-type unit 2 network gi uplink te
unit-type-control-end
!
interface vlan 1
ip address 192.168.11.101 255.255.255.0
!
interface vlan 2
ip address 192.168.12.101 255.255.255.0
!
interface vlan 100
ip address 192.168.10.101 255.255.255.0
!
interface GigabitEthernet1/0/1
!
.
.
.
interface TenGigabitEthernet1/0/28
!
hostname ZEQU0xxxxDL
```

13.21 write

To save the running configuration to the startup configuration file, use the write command in Privileged EXEC mode.

Syntax

write

write memory

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

Use the write command or the write memory command to save the Running Configuration file into the Startup Configuration file.

Examples

The following example shows how to overwrite the startup-config file with the running-config file with the write command.

ZEQU0xxxxDL# **write**

Overwrite file [startup-config] ?[Yes/press any key for no]....15-

Sep-2019 11:27

:48 %COPY-I-FILECPY: Files Copy - source URL running-config

destination

URL flash://startup-config

15-Sep-2019 11:27:50 %COPY-N-TRAP: The copy operation was completed

successfully

Copy succeeded

14 GARP VLAN Registration Protocol (GVRP)

Commands

14.1 clear gvrp statistics

To clear GVRP statistical information for all interfaces or for a specific interface, use the clear gvrp statistics Privileged EXEC mode command.

Syntax

clear gvrp statistics [interface-id]

Parameters

Interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP statistics are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears all GVRP statistical information on gi1/0/4.

```
ZEQU0xxxxDL# clear gvrp statistics gi1/0/4
```

14.2 gvrp enable (Global)

To enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally, use the `gvrp enable` Global Configuration mode command. To disable GVRP on the device, use the `no` form of this command.

Syntax

`gvrp enable`

`no gvrp enable`

Parameters

This command has no arguments or keywords.

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

Example

The following example enables GVRP globally on the device.

```
ZEQU0xxxxDL(config)# gvrp enable
```

14.3 gvrp enable (Interface)

To enable GVRP on an interface, use the `gvrp enable Interface (Ethernet, Port Channel) Configuration mode` command. To disable GVRP on an interface, use the `no` form of this command.

Syntax

`gvrp enable`

`no gvrp enable`

Parameters

This command has no arguments or keywords.

Default Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

An access port does not dynamically join a VLAN because it is always a member of a single VLAN only. Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID must be manually defined as the untagged VLAN ID.

Example

The following example enables GVRP on `gi1/0/4`.

```
ZEQU0xxxxDL (config) # interface gi1/0/4
ZEQU0xxxxDL (config-if) # gvrp enable
```

14.4 gvrp registration-forbid

To deregister all dynamic VLANs on a port and prevent VLAN creation or registration on the port, use the `gvrp registration-forbid` Interface Configuration mode command. To allow dynamic registration of VLANs on a port, use the `no` form of this command.

Syntax

`gvrp registration-forbid`

`no gvrp registration-forbid`

Parameters

This command has no arguments or keywords.

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example forbids dynamic registration of VLANs on `gi1/0/2`.

```
ZEQU0xxxxDL(config-if)# interface gi1/0/2
ZEQU0xxxxDL(config-if)# gvrp registration-forbid
```

14.5 gvrp vlan-creation-forbid

To disable dynamic VLAN creation or modification, use the `gvrp vlan-creation-forbid` Interface Configuration mode command. To enable dynamic VLAN creation or modification, use the `no` form of this command.

Syntax

`gvrp vlan-creation-forbid`

`no gvrp vlan-creation-forbid`

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables dynamic VLAN creation on `gi1/0/3`.

```
ZEQU0xxxxDL (config-if) # interface gi1/0/3  
ZEQU0xxxxDL (config-if) # gvrp vlan-creation-forbid
```

14.6 show gvrp configuration

To display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP, use the show gvrp configuration EXEC mode command.

Syntax

show gvrp configuration [interface-id | detailed]

Parameters

- interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed—(Optional) Displays information for non-present ports in addition to present ports.

Default Configuration

All GVRP statistics are displayed for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

User EXEC mode

Example

The following example displays GVRP configuration.

ZEQU0xxxxDL# show gvrp configuration

GVRP Feature is currently Disabled on the device.
Maximum VLANs: 4094

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers(milliseconds)		
				Join	Leave	Leave All
gi1/0/1	Enabled	Forbidden	Disabled	600	200	10000
gi1/0/2	Enabled	Normal	Enabled	1200	400	10000

14.7 show gvrp error-statistics

Use the show gvrp error-statistics EXEC mode command to display GVRP error statistics for all interfaces or for a specific interface.

Syntax

show gvrp error-statistics [interface-id]

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP error statistics are displayed.

Command Mode

User EXEC mode

Example

The following example displays GVRP error statistics.

ZEQU0xxxxDL# show gvrp error-statistics

GVRP Error Statistics:

Legend:

INVPROT : Invalid Protocol Id
INVATYP : Invalid Attribute Type INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value INVEVENT: Invalid Event

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
-----	-----	-----	-----	-----	-----
gi1/0/1	0	0	0	0	0
gi1/0/2	0	0	0	0	0
gi1/0/3	0	0	0	0	0
gi1/0/4	0	0	0	0	0

14.8 show gvrp statistics

To display GVRP statistics for all interfaces or for a specific interface, use the show gvrp statistics EXEC mode command.

Syntax

show gvrp statistics [interface-id]

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP statistics are displayed.

Command Mode

User EXEC mode

Example

The following example displays GVRP statistical information.

ZEQU0xxxxDL# show gvrp statistics

GVRP Statistics:

Legend:

rJE : Join Empty Received	rJIn: Join In Received
rEmp : Empty Received	rLIn: Leave In Received
rLE : Leave Empty Received	rLA : Leave All Received
sJE : Join Empty Sent	sJIn: Join In Sent
sEmp : Empty Sent	sLIn: Leave In Sent
sLE : Leave Empty Sent	sLA : Leave All Sent

Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
gi1/0/1	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/2	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/3	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/4	0	0	0	0	0	0	0	0	0	0	0	0

15 IGMP Commands

15.1 clear ip igmp snooping counters

To clear the Internet Group Management Protocol (IGMP) interface counters, use the `clear ip igmp snooping counters` command in Privileged EXEC mode.

Syntax

`clear ip igmp snooping counters [interface-id]`

Parameters

- `interface-id`—(Optional) Interface Identifier

Command Mode

Privileged EXEC mode

User Guidelines

Use the `clear ip igmp snooping counters` command to clear the IGMP counters, which keep track of the number of joins and leaves received. If you omit the optional `interface-id` argument, the `clear ip igmp snooping counters` command clears the counters on all interfaces.

Example

The following example clears the counters for VLAN 100:

```
ZEQU0xxxxDL# clear ip igmp snooping counters vlan 100
```

15.2 ip igmp last-member-query-count

To configure the Internet Group Management Protocol (IGMP) last member query counter, use the `ip igmp last-member-query-count` command in Interface Configuration mode. To restore the default value, use the `no` form of this command.

Syntax

`ip igmp last-member-query-count count`

`no ip igmp last-member-query-count`

Parameters

`count`—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default Configuration

A value of IGMP Robustness variable.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp snooping robustness-variable` command to change the IGMP last member query counter.

Example

The following example changes a value of the IGMP last member query counter to 3:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ip igmp last-member-query-count 3
ZEQU0xxxxDL(config-if)# exit
```

15.3 ip igmp snooping last-member-query-interval

To configure the Internet Group Management Protocol (IGMP) last member query interval, use the `ip igmp snooping last-member-query-interval` command in Interface.

Configuration mode. To restore the default IGMP query interval, use the `no` form of this command.

Syntax

`ip igmp snooping last-member-query-interval milliseconds`

`no ip igmp snooping last-member-query-interval`

Parameters

- `milliseconds`—Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–25500).

Default Configuration

The default IGMP last member query interval is 1000 milliseconds.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp snooping last-member-query-interval` command to configure the IGMP last member query interval on an interface.

Example

The following example shows how to increase the the IGMP last member query interval to 1500 milliseconds:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ip igmp snooping last-member-query-interval 1500
ZEQU0xxxxDL(config-if)# exit
```

15.4 ip igmp snooping query-interval

To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the `ip igmp snooping query-interval` command in Interface Configuration mode. To restore the default IGMP query interval, use the `no` form of this command.

Syntax

`ip igmp snooping query-interval seconds`

`no ip igmp snooping query-interval`

Parameters

- `seconds`—Frequency, in seconds, at which the switch sends IGMP query messages from the interface. The range is from 30 to 18000.

Default Configuration

The default IGMP query interval is 125 seconds.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp snooping query-interval` command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

The query interval must be bigger than the maximum query response time.

Example

The following example shows how to increase the frequency at which the IGMP querier sends IGMP host-query messages to 180 seconds:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ip igmp snooping query-interval 180
ZEQU0xxxxDL(config-if)# exit
```

15.5 ip igmp snooping query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the `ip igmp snooping query-max-response-time` command in Interface Configuration mode. To restore the default value, use the `no` form of this command.

Syntax

`ip igmp snooping query-max-response-time seconds`

`no ip igmp snooping query-max-response-time`

Parameters

- `seconds`—Maximum response time, in seconds, advertised in IGMP queries. (Range: 5–20)

Default Configuration

10 seconds.

Command Mode

Interface Configuration mode

User Guidelines

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

This command controls how much time the hosts have to answer an IGMP query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

The maximum query response time must be less than the query interval.

Note. If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Example

The following example configures a maximum response time of 8 seconds:

```
ZEQU0xxxxDL (config)# interface vlan 100
ZEQU0xxxxDL (config-if)# ip igmp snooping query-max-response-time 8
ZEQU0xxxxDL (config-if)# exit
```

15.6 ip igmp snooping robustness-variable

To configure the Internet Group Management Protocol (IGMP) robustness variable, use the `ip igmp snooping robustness-variable` command in Interface Configuration mode. To restore the default value, use the `no` form of this command.

Syntax

`ip igmp snooping robustness-variable count`

`no ip igmp snoping robustness`

Parameters

- `count`—The number of expected packet loss on a link. Parameter range. (Range: 1–7).

Default Configuration

The default value is 2.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp snooping robustness-variable` command to change the IGMP robustness variable.

Example

The following example changes a value of the IGMP robustness variable to 3:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ip igmp snooping robustness-variable 3
ZEQU0xxxxDL(config-if)# exit
```

15.7 ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the `ip igmp version` command in Interface Configuration mode. To restore the default value, use the `no ip igmp version` command.

Syntax

`ip igmp version {1 | 2 | 3}`

`no ip igmp version`

Parameters

- 1—IGMP Version 1.
- 2—IGMP Version 2.
- 3—IGMP Version 3.

Default Configuration

2

Command Mode

Interface Configuration mode

User Guidelines

Use the command to change the default version of IGMP>

Example

The following example configures the router to use IGMP Version 2:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ip igmp version 2
ZEQU0xxxxDL(config-if)# exit
```

15.8 show ip igmp snooping counters

To display the Internet Group Management Protocol (IGMP) traffic counters, use the `show ip igmp snooping counters` command in User EXEC mode.

Syntax

`show ip igmp snooping counters [interface-id]`

Parameters

- `interface-id`—(Optional) Interface Identifier.

Command Mode

User EXEC mode

User Guidelines

Use the `show ip igmp snooping counters` command to check if the expected number of IGMP protocol messages have been received and sent.

If you omit the optional `interface-id` argument, the `show ip igmp snooping counters` command displays counters of all interfaces.

Example

The following example displays the IGMP protocol messages received and sent:

```
ZEQU0xxxxDL# show ip igmp snooping counters vlan 100
```

```
VLAN 100
```

```
Elapsed time since counters cleared:00:00:21
Failed received Joins: 0
Total IGMPv1 received messages: 0
Total IGMPv2 received messages: 10
Total IGMPv3 received messages: 0
Total invalid received messages: 0
General Sent Queries: 0
Specific Sent Queries: 0
```

15.9 show ip igmp groups

To display the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the `show ip igmp groups` command in User EXEC mode.

Syntax

```
show ip igmp groups [group-name | group-address | interface-id] [detail]
```

Parameters

- `group-name | group-address`—(Optional) IP address or name of the multicast group.
- `interface-id`—(Optional) Interface identifier.
- `detail`—(Optional) Displays detailed information about individual sources.

Command Mode

User EXEC mode

User Guidelines

Use the `show ip igmp groups [detail]` command to display all directly connected groups.

Use the `show ip igmp groups [group-name | group-address] [detail]` command to display one given directly connected group.

Use the `show ip igmp groups interface-id [detail]` command to display all groups directly connected to the given interface.

Examples

Example 1. The following is sample output from the show ip igmp groups command. It shows all of the groups joined by VLAN 100:

```
ZEQU0xxxxDL# show ip igmp groups vlan 100
```

IGMP Connected Group Membership

Expires: never - switch itself has joined the group

Group Address	Interface	Expires
224. 1. 1. 1	VLAN 100	00:01:30
224. 10. 12. 79	VLAN 100	never
225. 1. 1. 1	VLAN 100	00:00:27

Example 2. The following is sample output from the show ip igmp groups command using the detail keyword:

```
ZEQU0xxxxDL# show ip igmp groups detail
```

Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state

Interface: VLAN 100

Group: 225. 1. 1. 1

Router mode: INCLUDE

Last reporter: 10. 0. 119. 133

Group Timer Expires: 00:20:11

Group source list:

Source Address	Expires
20. 1. 1. 1	00:04:08
120. 1. 1. 1	00:02:01

Group: 226. 1. 1. 2

Router mode: EXCLUDE

Last reporter: 100. 1. 12. 130

Group Timer Expiry: 00:22:12

Exclude Mode Expiry (Filter) Timer: 00:10:11

Group source list:

Source Address	Expires
2. 2. 2. 1	00:04:08
192. 168. 1. 1	00:04:08
12. 1. 1. 10	00:00:00
40. 3. 4. 2	00:00:00

15.10 **show ip igmp groups summary**

To display the number of (*, G) and (S, G) membership reports present in the Internet Group Management Protocol (IGMP) cache, use the `show ip igmp groups summary` command in User EXEC mode.

Syntax

```
show ip igmp groups summary
```

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

The `show ip igmp groups summary` command displays the number of directly connected multicast groups.

Example

The following is sample output from the `show ip igmp groups summary` command:

```
ZEQU0xxxxDL# show ip igmp groups summary
```

IGMP Route Summary

```
No. of (*,G) routes = 5
```

```
No. of (S,G) routes = 0
```

Field Descriptions:

```
No. of (*,G) routes = 5—Displays the number of groups present in the IGMP cache.
```

```
No. of (S,G) routes = 0—Displays the number of include and exclude mode sources present in the IGMP cache.
```

15.11 show ip igmp interface

To display multicast-related information about an interface, use the `show ip igmp interface` command in User EXEC mode.

Syntax

```
show ip igmp interface [interface-id]
```

Parameters

- `interface-id`—(Optional) Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If you omit the optional `interface-id` argument, the `show ip igmp interface` command displays information about all interfaces.

Example

The following is sample output from the `show ip igmp interface` command for interface `vlan 100`:

```
ZEQU0xxxxDL# show ip igmp interface vlan 100
```

```
VLAN 100 is up
```

```
Administrative IGMP Querier IP address is 1.1.1.1
```

```
Operational IGMP Querier IP address is 1.1.1.1
```

```
Current IGMP version is 3
```

```
Administrative IGMP robustness variable is 2 seconds
```

```
Operational IGMP robustness variable is 2 seconds
```

```
Administrative IGMP query interval is 125 seconds
```

```
Operational IGMP query interval is 125 seconds
```

```
Administrative IGMP max query response time is 10 seconds
```

```
Operational IGMP max query response time is 10 seconds
```

```
Administrative Last member query response interval is 1000 milliseconds
```

```
Operational Last member query response interval is 1000 milliseconds
```

16 IGMP Proxy Commands

16.1 ip igmp-proxy

To add downstream interfaces to an IGMP proxy tree, use the `ip igmp-proxy` command in Interface Configuration mode. To remove downstream from interfaces to an IGMP proxy tree, use the `no` form of this command.

Syntax

`ip igmp-proxy upstream-interface-id`

`no ip igmp-proxy`

Parameters

- `upstream-interface-id`—Upstream Interface identifier.

Default Configuration

The protocol is disabled on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp-proxy` command to add downstream interfaces to an IGMP proxy tree. If the proxy tree does not exist it is created.

Use the `no` format of the command to remove the downstream interface. When the last downstream interface is removed from the proxy tree it is deleted too.

Examples

Example 1. The following example adds a downstream interface to an IGMP Proxy process with `vlan 200` as its Upstream interface:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ip igmp-proxy vlan 200
ZEQU0xxxxDL(config-if)# exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with `vlan 200` as its Upstream interface:

```
ZEQU0xxxxDL(config)# interface range vlan 100-105
ZEQU0xxxxDL(config-if)# ip igmp-proxy vlan 200
ZEQU0xxxxDL(config-if)# exit
```

16.2 ip igmp-proxy downstream protected

To disable forwarding of IP Multicast traffic from downstream interfaces, use the `ip igmp-proxy downstream protected` command in Global Configuration mode. To allow forwarding from downstream interfaces, use the `no` form of this command.

Syntax

`ip igmp-proxy downstream protected`

`no ip igmp-proxy downstream protected`

Parameters

This command has no arguments or keywords.

Default Configuration

Forwarding from downstream interfaces is allowed.

Command Mode

Global Configuration mode

User Guidelines

Use the `ip igmp-proxy downstream protected` command to block forwarding from downstream interfaces.

Example

The following example prohibits forwarding from downstream interfaces:

```
ZEQU0xxxxDL (conf ig)# ip igmp-proxy downstream protected
```

16.3 ip igmp-proxy downstream protected interface

To disable or enable forwarding of IP Multicast traffic from a given downstream interface, use the `ip igmp-proxy downstream protected interface` command in Interface Configuration mode. To return to default, use the `no` form of this command.

Syntax

`ip igmp-proxy downstream protected interface {enabled | disabled}`

`no ip igmp-proxy downstream protected interface`

Parameters

- `enabled`—Downstream interface protection on the interface is enabled. IPv4 Multicast traffic arriving on the interface will not be forwarded.
- `disabled`—Downstream interface protection on the interface is disabled. IPv4 Multicast traffic arriving on the interface will be forwarded.

Default Configuration

Global downstream protection configuration (see the `ip igmp-proxy downstream protected` command)

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip igmp-proxy downstream protected interface disabled` command to block forwarding from the given downstream interface.

Use the `ip igmp-proxy downstream protected interface enabled` command to allow forwarding from the given downstream interface.

The command can be configured only for a downstream interface. When a downstream interface is removed from the IGMP Proxy tree the configuration is removed too.

Example

The following example prohibits forwarding from downstream interface `vlan 100`:

```
ZEQU0xxxxDL(config)# interface vlan100
ZEQU0xxxxDL(config-if)# ip igmp-proxy downstream protected interface enabled
ZEQU0xxxxDL(config-if)# exit
```

16.4 ip igmp-proxy ssm

To define the Source Specific Multicast (SSM) range of IP Multicast addresses, use the `ip igmp-proxy ssm` command in Global Configuration mode. To disable the SSM range, use the `no` form of this command.

Syntax

```
ip igmp-proxy ssm {default | range access-list}
```

```
no ip igmp-proxy ssm
```

Parameters

- `default`—Defines the SSM range access list to 232.0.0.0/8 (see rfc4607).
- `range access-list`—Specifies the standard IP access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global Configuration mode

User Guidelines

A new `ip igmp-proxy ssm` command overrides the previous `ip igmp-proxy ssm` command. Use the `no ip igmp-proxy ssm` command to remove all defined ranges.

Example

The following example shows how to configure SSM service for the default IP address range and the IP address ranges defined by access list `list1`:

```
ZEQU0xxxxDL(config)# ip access-list list1 permit 224.2.151.0/24
ZEQU0xxxxDL(config)# ip access-list list1 deny 224.2.152.141
ZEQU0xxxxDL(config)# ip access-list list1 permit 224.2.152.0/24
ZEQU0xxxxDL(config)# ip igmp-proxy ssm range list1
```

16.5 show ip igmpproxy interface

To display information about interfaces configured for IGMP Proxy, use the show ip igmpproxy interface command in User EXEC mode or Privileged EXEC mode.

Syntax

```
show ip igmpproxy interface [interface-id]
```

Parameters

- interface-id—(Optional) Display IGMP Proxy information about the interface.

Command Mode User

EXEC mode Privileged

EXEC mode

User Guidelines

The show ip igmp-proxy interface command is used to display all interfaces where the IGMP Proxy is enabled or to display the IGMP Proxy configuration for a given interface.

Examples

Example 1. The following example displays IGMP Proxy status on all interfaces where the IGMP Proxy is enabled:

```
ZEQU0xxxxDL# show ip igmpproxy interface
```

* - the switch is the Querier on the interface

IP Forwarding is enabled

IP Multicast Routing is enabled

IGMP Proxy is enabled

Global Downstream interfaces protection is disabled

SSM Access List Name:list1

Interface	Type	Interface Protection
vlan 100	upstream	
*vlan 102	downstream	enabled
*vlan 110	downstream	default
vlan 113	downstream	disabled

Example 2. The following is sample output from the show ip igmp-proxy interface command for given upstream interface:

```
ZEQU0xxxxDL# show ip igmpproxy interface vlan 100
```

```
* - the switch is the Querier on the interface
```

```
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downstream interfaces protection is disabled
SSM Access List Name:
IP Multicast Traffic Discarding from Downstream interfaces is disabled
vlan 100 is a Upstream interface
Downstream interfaces:
*vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the show ip igmp-proxy interface command for given downstream interface:

```
ZEQU0xxxxDL# show ip igmpproxy interface vlan 102
```

```
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downstream interfaces protection is disabled
vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Downstream Interface protection is enabled
SSM Access List Name: default
Upstream interface: vlan 100
```

Example 4. The following is sample output from the show ip igmp-proxy interface command for an interface on which IGMP Proxy is disabled:

```
ZEQU0xxxxDL# show ip igmpproxy interface vlan 1
```

```
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is disabled
```

17 IGMP Snooping Commands

17.1 ip igmp snooping (Global)

To enable Internet Group Management Protocol (IGMP) snooping, use the `ip igmp snooping` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ip igmp snooping`

`no ip igmp snooping`

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables IGMP snooping.

```
ZEQU0xxxxDL (config)# ip igmp snooping
```

17.2 ip igmp snooping vlan

To enable IGMP snooping on a specific VLAN, use the `ip igmp snooping vlan` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ip igmp snooping vlan vlan-id`

`no ip igmp snooping vlan vlan-id`

Parameters

- `vlan-id`—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can be enabled only on static VLANs. IGMPv1, IGMPv2, and IGMPv3 Snooping are supported.

To activate IGMP snooping, bridge multicast filtering must be enabled by the `bridge multicast filtering` command.

The user guidelines of the `bridge multicast mode` command describes the configuration that is written into the FDB as a function of the FDB mode and the IGMP version that is used in the network.

Example

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 2
```

17.3 ip igmp snooping vlan mrouter

To enable automatic learning of Multicast router ports on a VLAN, use the `ip igmp snooping vlan mrouter` command in Global Configuration mode. To remove the configuration, use the no form of this command.

Syntax

```
ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp
```

```
no ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp
```

Parameters

- `vlan-id`—Specifies the VLAN.

Default Configuration

Learning pim-dvmrp is enabled.

Command Mode

Global Configuration mode

User Guidelines

Multicast router ports are learned according to:

- Queries received on the port
- PIM/PIMv2 received on the port
- DVMRP received on the port
- MRDISC received on the port
- MOSPF received on the port

You can execute the command before the VLAN is created.

Example

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

17.4 ip igmp snooping vlan mrouter interface

To define a port that is connected to a Multicast router port, use the `ip igmp snooping mrouter interface` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ip igmp snooping vlan vlan-id mrouter interface interface-list
```

```
no ip igmp snooping vlan vlan-id mrouter interface interface-list
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies the list of interfaces. The interfaces can be one of the following types: Ethernet port or Port-channel.

Default Configuration

No ports defined

Command Mode

Global Configuration mode

User Guidelines

A port that is defined as a Multicast router port receives all IGMP packets (reports and queries) as well as all Multicast data.

You can execute the command before the VLAN is created.

Example

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 mrouter interface gi1/0/1
```

17.5 ip igmp snooping vlan forbidden mrouter

To forbid a port from being defined as a Multicast router port by static configuration or by automatic learning, use the `ip igmp snooping vlan forbidden mrouter` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list`

`no ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list`

Parameters

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies a list of interfaces. The interfaces can be of one of the following types: Ethernet port or Port-channel.

Default Configuration

No ports defined.

Command Mode

Global Configuration mode

User Guidelines

A port that is a forbidden mrouter port cannot be a Multicast router port (i.e. cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

Example

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 forbidden mrouter interface gi1/0/1
```

17.6 ip igmp snooping vlan static

To register an IP-layer Multicast address to the bridge table, and to add static ports to the group defined by this address, use the `ip igmp snooping vlan static` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
```

```
no ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
```

Parameter

- `vlan-id`—Specifies the VLAN.
- `ip-address`—Specifies the IP Multicast address.
- `interface interface-list`—(Optional) Specifies a list of interfaces. The interfaces can be of one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

Static Multicast addresses can only be defined on static VLANs. You can execute the command before the VLAN is created.

You can register an entry without specifying an interface. Using the `no` command without a port-list removes the entry.

Example

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 static 239.2.2.2 interface gi1/0/1
```

17.7 ip igmp snooping querier

To enable globally the IGMP Snooping querier, use the `ip igmp snooping querier` command in Global Configuration mode. To disable the IGMP Snooping querier globally, use the `no` form of this command.

Syntax

`ip igmp snooping querier`

`no ip igmp snooping querier`

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

To run the IGMP Snooping querier on a VLAN, you have enable it globally and on the VLAN.

Example

The following example disables the IGMP Snooping querier globally:

```
ZEQU0xxxxDL(config)# no ip igmp snooping querier
```

17.8 ip igmp snooping vlan querier

To enable the IGMP Snooping querier on a specific VLAN, use the `ip igmp snooping vlan querier` command in Global Configuration mode. To disable the IGMP Snooping querier on the VLAN interface, use the `no` form of this command.

Syntax

```
ip igmp snooping vlan vlan-id querier
```

```
no ip igmp snooping vlan vlan-id querier
```

Parameters

- `vlan-id`—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The IGMP Snooping querier can be enabled on a VLAN only if IGMP Snooping is enabled for that VLAN.

Example

The following example enables the IGMP Snooping querier on VLAN 1:

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 querier
```

17.9 ip igmp snooping vlan querier address

To define the source IP address that the IGMP snooping querier uses, use the `ip igmp snooping vlan querier address` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ip igmp snooping vlan vlan-id querier address ip-address
```

```
no ip igmp snooping vlan vlan-id querier address
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `ip-address`—Source IP address.

Default Configuration

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier. If there are multiple IP addresses, the minimum IP address defined on the VLAN is used.

Command Mode

Global Configuration mode

User Guidelines

If an IP address is not configured by this command, and no IP address is configured for the querier's VLAN, the querier is disabled.

Example

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 querier address 10.5.234.205
```

17.10 ip igmp snooping vlan querier election

To enable IGMP Querier election mechanism of an IGMP Snooping querier on a specific VLAN, use the `ip igmp snooping vlan querier election` command in Global Configuration mode. To disable Querier election mechanism, use the `no` form of this command.

Syntax

`ip igmp snooping vlan vlan-id querier election`

`no ip igmp snooping vlan vlan-id querier election`

Parameters

- `vlan-id`—Specifies the VLAN.

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

Use the `no` form of the `ip igmp snooping vlan querier election` command to disable IGMP Querier election mechanism on a VLAN.

If the IGMP Querier election mechanism is enabled, the IGMP Snooping querier supports the standard IGMP Querier election mechanism specified in RFC2236 and RFC3376.

If IGMP Querier election mechanism is disabled, IGMP Snooping Querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an IGMP query from another Querier

- it starts sending General Query messages. Once the switch acts as a Querier, it will stop sending General Query messages if it detects another Querier on the VLAN. In this case, the switch will resume sending General Query messages if it does hear another Querier for Query Passive interval that equals to

$\text{<Robustness>*<Query Interval> + 0.5*<Query Response Interval>}$.

See the `ip igmp robustness`, `ip igmp query-interval`, and `ip igmp query-max-response-time` commands for configurations of these parameters.

It is recommended to disable IGMP Querier election mechanism if there is an IPM Multicast router on the VLAN.

Example

The following example disables IGMP Snooping Querier election on VLAN 1:

```
ZEQU0xxxxDL (config)# no ip igmp snooping vlan 1 querier election
```

17.11 ip igmp snooping vlan querier version

To configure the IGMP version of an IGMP Snooping querier on a specific VLAN, use the `ip igmp snooping vlan querier version` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ip igmp snooping vlan vlan-id querier version {2 | 3}
```

```
no ip igmp snooping vlan vlan-id querier version
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `querier version 2`—Specifies that the IGMP version would be IGMPv2.
- `querier version 3`—Specifies that the IGMP version would be IGMPv3.

Default Configuration

IGMPv2.

Command Mode

Global Configuration mode

Example

The following example sets the version of the IGMP Snooping Querier VLAN 1 to 3:

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 querier version 3
```

17.12 ip igmp snooping vlan immediate-leave

To enable the IGMP Snooping Immediate-Leave processing on a VLAN, use the `ip igmp snooping vlan immediate-leave` Global Configuration mode command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ip igmp snooping vlan vlan-id immediate-leave`

`no ip igmp snooping vlan vlan-id immediate-leave`

Parameters

- `vlan-id`—Specifies the VLAN ID value. (Range: 1–4094).

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

The following example enables IGMP snooping immediate-leave feature on VLAN 1.

```
ZEQU0xxxxDL(config)# ip igmp snooping vlan 1 immediate-leave
```

17.13 show ip igmp snooping groups

To display the Multicast groups learned by the IGMP snooping, use the show ip igmp snooping groups command in User EXEC mode.

Syntax

show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address] [source ip-address]

Parameters

- vlan vlan-id—(Optional) Specifies the VLAN ID.
- address ip-multicast-address—(Optional) Specifies the IP multicast address.
- source ip-address—(Optional) Specifies the IP source address.

Command Mode

User EXEC mode

User Guidelines

To see all Multicast groups learned by IGMP snooping, use the show ip igmp snooping groups command without parameters.

Use the show ip igmp snooping groups command with parameters to see a needed subset of all Multicast groups learned by IGMP snooping

To see the full Multicast address table (including static addresses), use the show bridge multicast address-table command.

Example

The following example shows sample output:

ZEQU0xxxxDL# show ip igmp snooping groups vlan 1					
ZEQU0xxxxDL# show ip igmp snooping groups					
Vlan	Group	Source	Include Ports	Exclude Ports	Comp.
	Address	Address			Mode
1	239.255.255.250 *		gi1/0/1		v2

17.14 show ip igmp snooping interface

To display the IGMP snooping configuration for a specific VLAN, use the show ip igmp snooping interface command in User EXEC mode.

Syntax

```
show ip igmp snooping interface vlan-id
```

Parameters

- `vlan-id`—Specifies the VLAN ID.

Command Mode

User EXEC mode

Example

The following example displays the IGMP snooping configuration for VLAN 1000

```
ZEQU0xxxxDL# show ip igmp snooping interface 1000
```

```
IGMP Snooping is globally enabled
```

```
IGMP Snooping Querier is globally enabled
```

```
VLAN 1000
```

```
IGMP Snooping is enabled
```

```
IGMP snooping last immediate leave: enable
```

```
Automatic learning of Multicast router ports is enabled
```

```
IGMP Snooping Querier is enabled
```

```
IGMP Snooping Querier operation state: is running
```

```
IGMP Snooping Querier version: 2
```

```
IGMP Snooping Querier election is enabled
```

```
IGMP Snooping Querier address: 194.12.10.166
```

```
IGMP snooping robustness: admin 2 oper 2
```

```
IGMP snooping query interval: admin 125 sec oper 125 sec
```

```
IGMP snooping query maximum response: admin 10 sec oper 10 sec
```

```
IGMP snooping last member query counter: admin 2 oper 2
```

```
IGMP snooping last member query interval: admin 1000 msec oper 500 msec
```

```
Groups that are in IGMP version 1 compatibility mode: 231.2.2.3, 231.2.2.3
```

17.15 show ip igmp snooping mrouter

To display information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN, use the show ip igmp snooping mrouter command in User EXEC mode.

Syntax

show ip igmp snooping mrouter [interface vlan-id]

Parameters

- interface vlan-id—(Optional) Specifies the VLAN ID.

Command Mode

User EXEC mode

Example

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000:

ZEQU0xxxxDL# show ip igmp snooping mrouter interface 1000

Vlan	Dynamic	Static	Forbidden
1000	gi1/0/1	gi1/0/2	gi1/0/3-4

18 IP Addressing Commands

IP addresses and Layer 2 Interfaces

IP addresses can be configured on the following Layer 2 interfaces:

- Ethernet port
- Port channel
- VLAN

Lists of Commands

18.1 ip address

Use the `ip address` Interface Configuration (Ethernet, VLAN, Port-channel) mode command to define an IP address for an interface. Use the `no` form of this command to remove an IP address definition.

Syntax

```
ip address ip-address {mask | /prefix-length} [default-gateway-ip-address]
```

```
no ip address
```

In-Band interfaces:

```
ip address ip-address {mask | /prefix-length}
```

```
no ip address [ip-address]
```

Parameters

- `ip-address`—Specifies the IP address.
- `mask`—Specifies the network mask of the IP address.
- `prefix-length`—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8–30)
- `default-gateway-ip-address`—Specifies the default gateway IP address. The route is gotten a metric of 6 for an In-Band interface.

Default Configuration

No IP address is defined for interfaces.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ip address` command to define a static IP address on an interface. In-Band interfaces

Multiple IP addresses are supported. A new defined IP address is added on the interface.

Defining a static IP address on an interface stops a DHCP client running on the interface and removes the IP address assigned by the DHCP client.

If a configured IP address overlaps another configured one a warning message is displayed. To change an existed IP address, delete the existed one and add the new one.

Examples

Example 1. The following example configures VLAN 1 with IP address 192.168.1.27 and subnet mask 255.255.255.0.

```
ZEQU0xxxxDL (config)# interface vlan 1  
ZEQU0xxxxDL (config-if)# ip address 192. 168. 1. 27 255. 255. 255. 0
```

Example 2. The following example configures 3 overlapped IP addresses.

```
ZEQU0xxxxDL (config)# interface vlan 1  
ZEQU0xxxxDL (config-if)# ip address 1. 1. 1. 1 255. 0. 0. 0  
ZEQU0xxxxDL (config)# exit  
ZEQU0xxxxDL (config)# interface vlan 2  
ZEQU0xxxxDL (config-if)# ip address 1. 2. 1. 1 255. 255. 0. 0  
ZEQU0xxxxDL (config)# exit  
ZEQU0xxxxDL (config)# interface vlan 3  
ZEQU0xxxxDL (config-if)# ip address 1. 3. 1. 1 255. 255. 0. 0  
ZEQU0xxxxDL (config)# exit
```

18.2 ip address dhcp

Use the ip address dhcp Interface Configuration (Ethernet, VLAN, Port-channel) mode command to acquire an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the no form of this command to release an acquired IP address.

Syntax

ip address dhcp

no ip address dhcp

Parameters

N/A

Command Mode

Interface Configuration mode

User Guidelines

Use the ip address dhcp command to enable DHCP client on the interface.

The ip address dhcp command removes all the manually configured addresses on the interface.

The default route (Default Gateway) received in DHCP Router option (Option 3) is assigned a metric of 8 for an In-Band interface.

Use the no form of the command to disable DHCP client on interface.

Example

The following example acquires an IP address for VLAN 100 from DHCP.

```
ZEQU0xxxxDL(config)# interface vlan100
ZEQU0xxxxDL(config-if)# ip address dhcp
```

18.3 renew dhcp

Use the `renew dhcp` Privileged EXEC mode command to renew an IP address that was acquired from a DHCP server for a specific interface.

Syntax

```
renew dhcp interface-id [force-autoconfig]
```

Parameters

- `interface-id`—Specifies an interface.
- `force-autoconfig` - If the DHCP server holds a DHCP option 67 record for the assigned IP address, the record overwrites the existing device configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `renew dhcp` command to renew a DHCP address on an interface.

This command does not enable DHCP client on an interface and if DHCP client is not enabled on the interface, the command returns an error message.

Example

The following example renews an IP address on VLAN 19 that was acquired from a DHCP server:

```
ZEQU0xxxxDL# renew dhcp vlan 19
```

18.4 ip default-gateway

The ip default-gateway Global Configuration mode command defines a default gateway (device). Use the no form of this command to restore the default configuration.

Syntax

```
ip default-gateway ip-address  
no ip default-gateway [ip-address]
```

Parameters

- ip-address—Specifies the default gateway IP address.

Command Mode

Global Configuration mode

Default Configuration

No default gateway is defined.

User Guidelines

Use the ip default-gateway command to defines a default gateway (default route). The ip default-gateway command adds the default route with metric of 6 for the gateway connected on an In-Band interface.

Use the no ip default-gateway ip-address command to delete one default gateway.

Use the no ip default-gateway command to delete all default gateways.

Example

The following example defines default gateway 192.168.1.1.

```
ZEQU0xxxxDL (config) # ip default-gateway 192. 168. 1. 1
```

18.5 show ip interface

Use the show ip interface EXEC mode command to display the usability status of configured IP interfaces.

Syntax

show ip interface [interface-id]

Parameters

- interface-id—Specifies an interface ID on which IP addresses are defined.

Default Configuration

All IP addresses.

Command Mode

User EXEC mode

Examples

Example 1 - The following example displays all configured IP addresses and their types:

ZEQU0xxxxDL# **show ip interface**

IP Address	I/F	I/F Status admin/oper	Type	Directed Broadcast	Prec	Redirect	Status
192. 168. 10. 101/24	vlan 1	UP/UP	Static	disable	No	enable	Valid
192. 168. 11. 101/24	vlan 4	UP/DOWN	Static	disable	No	enable	Valid

Example 2 - The following example displays the IP addresses configured on the given L2 interfaces and their types:

ZEQU0xxxxDL# **show ip interface vlan 1**

IP Address	I/F	I/F Status admin/oper	Type	Directed Broadcast	Prec	Redirect	Status
192. 168. 11. 101/24	vlan 1	UP/UP	Static	disable	No	enable	Valid

18.6 arp

Use the arp Global Configuration mode command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the no form of this command to remove an entry from the ARP cache.

Syntax

arp ip-address mac-address [interface-id]

no arp ip-address

Parameters

- ip-address—IP address or IP alias to map to the specified MAC address.
- mac-address—MAC address to map to the specified IP address or IP alias.
- interface-id—Address pair is added for specified interface.

Command Mode

Global Configuration mode

Default Configuration

No permanent entry is defined.

If no interface ID is entered, address pair is relevant to all interfaces.

User Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware (MAC) addresses. Because most hosts support dynamic address resolution, static ARP cache entries generally do not need to be specified.

Example

The following example adds IP address 192.168.100.200 and MAC address 00:50:40:03:e4:24 to the ARP table.

```
ZEQU0xxxxDL(config)# arp 192.168.100.200 00:50:40:03:e4:24 vlan100
```

18.7 arp timeout (Global)

Use the arp timeout Global Configuration mode command to set the time interval during which an entry remains in the ARP cache. Use the no form of this command to restore the default configuration.

Syntax

arp timeout seconds

no arp timeout

Parameters

- seconds—Specifies the time interval (in seconds) during which an entry remains in the ARP cache. (Range: 1–40000000).

Default Configuration

The default ARP timeout is 60000 seconds, if IP Routing is enabled, and 300 seconds if IP Routing is disabled.

Command Mode

Global Configuration mode

Example

The following example configures the ARP timeout to 12000 seconds.

```
ZEQU0xxxxDL(config)# arp timeout 12000
```

18.8 Ip arp proxy disable

Use the `ip arp proxy disable` Global Configuration mode command to globally disable proxy Address Resolution Protocol (ARP). Use the `no` form of this command reenables proxy ARP.

Syntax

`ip arp proxy disable`

`no ip arp proxy disable`

Parameters

N/A

Default

Enabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command overrides any proxy ARP interface configuration. The command is supported only when IP Routing is enabled.

Example

The following example globally disables ARP proxy.

```
ZEQU0xxxxDL (config) # ip arp proxy disable
```

18.9 ip proxy-arp

Use the ip proxy-arp Interface Configuration mode command to enable an ARP proxy on specific interfaces. Use the no form of this command disable it.

Syntax

ip proxy-arp

no ip proxy-arp

Default Configuration

ARP Proxy is disabled.

Command Mode

Interface Configuration mode

User Guidelines

This configuration can be applied only if at least one IP address is defined on a specific interface.

The command is supported only when IP Routing is enabled.

Example

The following example enables ARP proxy when the switch is in router mode.

```
ZEQU0xxxxDL(config-if)# ip proxy-arp
```

18.10 clear arp-cache

Use the clear arp-cache Privileged EXEC mode command to delete all dynamic entries from the ARP cache.

Syntax

clear arp-cache

Command Mode

Privileged EXEC mode

Example

The following example deletes all dynamic entries from the ARP cache.

```
ZEQU0xxxxDL# clear arp-cache
```

18.11 show arp

Use the show arp Privileged EXEC mode command to display entries in the ARP table.

Syntax

```
show arp [ip-address ip-address] [mac-address mac-address] [interface-id]
```

Parameters

- ip-address ip-address—Specifies the IP address.
- mac-address mac-address—Specifies the MAC address.
- interface-id—Specifies an interface ID.

Command Mode

Privileged EXEC mode

User Guidelines

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

If an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

Example

The following example displays entries in the ARP table.

```
ZEQU0xxxxDL# show arp
```

```
Total number of entries: 3
```

VLAN	Interface	IP address	HW address	status
vlan 1	gi1/0/1	10.7.1.102	00:50:40:04:DB:4B	dynamic
vlan 1	gi1/0/2	10.7.1.135	00:50:40:00:2A:A4	static
vlan 2	gi1/0/1	11.7.1.135	00:50:40:00:2A:A4	dynamic

18.12 show arp configuration

Use the show arp configuration privileged EXEC command to display the global and interface configuration of the ARP protocol.

Syntax

show arp configuration

Parameters

This command has no arguments or key words.

Command Mode

Privileged EXEC mode

Example

ZEQU0xxxxDL# **show arp configuration**

Global configuration:

ARP Proxy: disabled
ARP Refresh: enabled
ARP timeout: 60000 Seconds

Interface configuration:

VLAN 1:

ARP Proxy: enabled
ARP timeout: 60000 Seconds (Global)

VLAN 2:

ARP Proxy: disabled
ARP timeout: 60000 Seconds (Global)

VLAN 100:

ARP Proxy: enabled
ARP timeout: 60000 Seconds (Global)

18.13 interface ip

Use the interface ip Global Configuration mode command to enter the IP Interface Configuration mode.

Syntax

```
interface ip ip-address
```

Parameters

- ip-address—Specifies one of the IP addresses of the device.

Command Mode

Global Configuration mode

Example

The following example enters the IP interface configuration mode.

```
ZEQU0xxxxDL (config) # interface ip 192.168.1.1  
ZEQU0xxxxDL (config-ip) #
```

18.14 ip helper-address

Use the ip helper-address Global Configuration mode command to enable the forwarding of UDP Broadcast packets received on an interface to a specific (helper) address. Use the no form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

Syntax

```
ip helper-address {ip-interface | all} address [udp-port-list]
```

```
no ip helper-address {ip-interface | all} address
```

Parameters

- ip-interface—Specifies the IP interface.
- all—Specifies all IP interfaces.
- address—Specifies the destination broadcast or host address to which to forward UDP broadcast packets. A value of 0.0.0.0 specifies that UDP broadcast packets are not forwarded to any host.
- udp-port-list—Specifies the destination UDP port number to which to forward Broadcast packets. (Range: 1–65535). This can be a list of port numbers separated by spaces.

Default Configuration

Forwarding of UDP Broadcast packets received on an interface to a specific (helper) address is disabled.

If udp-port-list is not specified, packets for the default services are forwarded to the helper address.

Command Mode

Global Configuration mode

User Guidelines

This command forwards specific UDP Broadcast packets from one interface to another, by specifying a UDP port number to which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Many helper addresses may be defined. However, the total number of address-port pairs is limited to 128 for the device.

The setting of a helper address for a specific interface has precedence over the setting of a helper address for all the interfaces.

Forwarding of BOOTP/DHCP (ports 67, 68) cannot be enabled with this command. Use the DHCP relay commands to relay BOOTP/DHCP packets.

Example

The following example enables the forwarding of UDP Broadcast packets received on all interfaces to the UDP ports of a destination IP address and UDP port 1 and 2.

```
ZEQU0xxxxDL(config)# ip helper-address all 172.16.9.9 49 53 1 2
```

18.15 show ip helper-address

Use the show ip helper-address Privileged EXEC mode command to display the IP helper addresses configuration on the system.

Syntax

show ip helper-address

Parameters

This command has no arguments or key words.

Command Mode

Privileged EXEC mode

User Guidelines

Example

The following example displays the IP helper addresses configuration on the system:

ZEQU0xxxxDL# **show ip helper-address**

Interface	Helper Address	UDP Ports
-----	-----	-----
192. 168. 1. 1	172. 16. 8. 8	37, 42, 49, 53, 137, 138
192. 168. 2. 1	172. 16. 9. 9	37, 49

18.16 show ip dhcp client interface

Use the show ip dhcp client interface command in User EXEC or Privileged EXEC mode to display DHCP client interface information.

Syntax

```
show ip dhcp client interface [interface-id]
```

Parameters

- interface-id—Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If no interfaces are specified, all interfaces on which DHCP client is enabled are displayed. If an interface is specified, only information about the specified interface is displayed.

Example

The following is sample output of the show ip dhcp client interface command:

```
ZEQU0xxxxDL# show ip dhcp client interface
```

```
VLAN 100 is in client mode
```

```
Address: 170.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
```

```
Default Gateway: 170.10.100.1
```

```
DNS Servers: 115.1.1.1, 87.12.34.20
```

```
DNS Domain Search List: company.com
```

```
Host Name: switch_floor7
```

```
Configuration Server Addresses: 192.1.1.1 202.1.1.1
```

```
Configuration Path Name: qqg/config/aaa_config.dat
```

```
Image Path Name: qqg/image/aaa_image.ros
```

```
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
```

```
VLAN 1200 is in client mode
```

```
Address: 180.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
```

```
Default Gateway: 180.10.100.1
```

```
DNS Servers: 115.1.1.1, 87.12.34.20
```

```
DNS Domain Search List: company.com
```

```
Host Name: switch_floor7
```

```
Configuration Server Addresses: configuration.company.com
```

```
Configuration Path Name: qqg/config/aaa_config.dat
```

```
Image Path Name: qqg/image/aaa_image.ros
```

```
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
```

19 IP Routing Protocol-Independent Commands

19.1 directed-broadcast

Use the directed-broadcast IP Interface Configuration mode command to enable the translation of a directed broadcast to physical broadcasts. Use the no form of this command to disable this function.

Syntax

directed-broadcast

no directed-broadcast

Default Configuration

Translation of a directed broadcast to physical broadcasts is disabled. All IP directed broadcasts are dropped.

Command Mode

IP Configuration mode

Example

The following example enables the translation of a directed broadcast to physical broadcasts.

```
ZEQU0xxxxDL(config)# interface ip 192.168.1.1  
ZEQU0xxxxDL(config-ip)# directed-broadcast
```

19.2 ip redirects

Use the ip redirects command in IP Interface Configuration mode to enable the sending of ICMP redirect messages to re-send a packet through the same interface on which the packet was received. To disable the sending of redirect messages, use the no form of this command.

Syntax

ip redirects

no ip redirects

Parameters

N/A.

Default Configuration

The sending of ICMP redirect messages is enabled.

Command Mode

IP Configuration mode

Example

The following example disables the sending of ICMP redirect messages on IP interface 1.1.1.1 and re-enables the messages on IP interface 2.2.2.2:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1
ZEQU0xxxxDL(config-ip)# no ip redirects
ZEQU0xxxxDL(config-ip)# exit
ZEQU0xxxxDL(config)# interface ip 2.2.2.2
ZEQU0xxxxDL(config-ip)# ip redirects
ZEQU0xxxxDL(config-ip)# exit
```

19.3 ip route

To establish static routes, use the `ip route` command in global configuration mode. To remove static routes, use the `no` form of this command.

Syntax

```
ip route prefix {mask | /prefix-length} {{ip-address [metric value] }
```

```
no ip route prefix {mask | /prefix-length} [ip-address]
```

Parameters

- `prefix`—IP route prefix for the destination.
- `mask`—Prefix mask for the destination.
- `/prefix-length`—Prefix mask for the destination. Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- `ip-address`—IP address of the next hop that can be used to reach that network.
- `metric value`—Metric of the route. The default metric is 4 for the Next Hop on an In-Band interface. Range: 1–255.

Default Configuration

No static routes are established.

Command Mode

Global Configuration mode

User Guidelines

Use the `no ip route` command without the `ip-address` parameter to remove all static routes to the given subnet.

Use the `no ip route` command with the `ip-address` parameter to remove only one static route to the given subnet via the given next hop.

Examples

Example 1—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using mask:

```
ZEQU0xxxxDL (config) # ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

Example 2—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using prefix length :

```
ZEQU0xxxxDL (config) # ip route 172. 31. 0. 0 /16 172. 31. 6. 6 metric 2
```

Example 3—The following example shows how to remove all static routes to network 192.168.1.0/24:

```
ZEQU0xxxxDL (config) # no ip route 192. 168. 1. 0 /24
```

Example 4—The following example shows how to remove one static route to network 192.168.1.0/24 via 1.1.1.1:

```
ZEQU0xxxxDL (config) # no ip route 192. 168. 1. 0 /24 1. 1. 1. 1
```

19.4 ip routing

To enable IP routing, use the ip routing command in global configuration mode. To disable IP routing, use the no form of this command.

Syntax

ip routing

no ip routing

Parameters

This command has no arguments or keywords.

Default Configuration

IP routing is enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the command to enable IP Routing.

Example The following example enables IP routing

```
ZEQU0xxxxDL (config) # ip routing
```

19.5 show ip route

To display the current state of the routing table, use the show ip route command in user EXEC or privileged EXEC mode.

Syntax

```
show ip route [address ip-address {mask [longer-prefixes]} [protocol | static |  
icmp | connected]
```

Parameters

- address ip-address—IP address about which routing information should be displayed.
- mask—The value of the subnet mask.
- longer-prefixes—Specifies that only routes matching the IP address and mask pair should be displayed.
- protocol—The name of the origin of the protocol to be displayed. Use one of the following arguments:
 - rip—Displays routes added by RIP
- connected—Displays connected routes.
- icmp—Displays routes added by ICMP Direct.
- static—Displays static routes.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Use this command without parameters to display the whole IPv6 Routing table. Use this command with parameters to specify required routes.

Examples

Example 1. The following is sample output from the show ip route command when IP Routing is not enabled:

```
ZEQU0xxxxDL# show ip route
```

```
Maximum Parallel Paths: 1 (1 after reset)
```

```
IP Forwarding: enabled
```

```
Codes: > - best, C - connected, S - static
```

```
S      10.2.1.0/24 [1/4] via 192.168.10.254, 20:04:46, vlan 100
```

```
C      192.168.10.0/24 is directly connected, vlan 100
```

```
C      192.168.11.0/24 is directly connected, vlan 1
```

19.6 show ip route summary

Use the show ip route summary command in User EXEC or Privileged EXEC mode to display the current contents of the IP routing table in summary format.

Syntax

```
show ip route summary
```

Parameters

N/A.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Example

The following is sample output from the show ip route summary command:

```
ZEQU0xxxxDL# show ip route summary
```

```
IP Routing Table Summary - 60 entries
```

```
35 connected, 25 static
```

```
Number of prefixes:
```

```
/16: 15, /18: 10, /22: 15, /24: 20
```

20 IP Setup Interface Commands

20.1 ip setup interface

Enable/Disable ip setup interface function status.

Syntax

ip setup interface

no ip setup interface

Parameters

N/A

Default Configuration

Enable mode is default

Command Mode

Global Configuration mode

User Guidelines

Use this command to change ip setup interface status.

Example

The following example sets enable/disable for ip setup interface.

```
ZEQU0xxxxDL (config)# ip setup interface
ZEQU0xxxxDL (config)# no ip setup interface
```

20.2 show ip setup interface

To display ip setup interface status, use show ip setup interface command.

Syntax

show ip setup interface

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to display the current ip setup interface status.

Example

Example1 : ip setup interface status is enabled.

```
ZEQU0xxxxDL# show ip setup interface
IP Setup Interface
-----
Enabled
```

Example2 : ip setup interface status is disabled.

```
ZEQU0xxxxDL# show ip setup interface
IP Setup Interface
-----
Disabled
```

21 IP System Management Commands

21.1 ping

Use the ping EXEC mode command to send ICMP echo request packets to another node on the network.

Syntax

```
ping [ip] {ipv4-address | hostname} [size packet_size] [count packet_count]  
[timeout time_out] [source source-address]
```

```
ping ipv6 {ipv6-address | hostname} [size packet_size] [count packet_count]  
[timeout time_out] [source source-address]
```

Parameters

- ip—Use IPv4 to check the network connectivity.
- ipv6—Use IPv6 to check the network connectivity.
- ipv4-address—IPv4 address to ping.
- ipv6-address—Unicast or Multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified.
- hostname—Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- size packet_size—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64–1518, IPv6: 68–1518)
- count packet_count—Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered, it pings until stopped (0–65535).
- time time-out—Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds (50–65535).
- source source-address—Source address (Unicast IPv4 address or global Unicast IPv6 address).

Default Usage

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Press Esc to stop pinging. Following are sample results of the ping command:

- Destination does not respond—If the host does not respond, a “no answer from host” appears within 10 seconds.
- Destination unreachable—The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable—The switch found no corresponding entry in the route table.

When using the ping ipv6 command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the IPv6Z format. If the egress interface is not specified, the default interface is selected.

When using the ping ipv6 command with a Multicast address, the information displayed is taken from all received echo responses.

When the source keyword is configured and the source address is not an address of the switch, the command is halted with an error message and pings are not sent.

Examples

Example 1 - Ping an IP address.

```
ZEQU0xxxxDL> ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

Example 2 - Ping a site.

```
ZEQU0xxxxDL> ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:
64 bytes from 66.218.71.198: icmp_seq=0. time=11 ms
64 bytes from 66.218.71.198: icmp_seq=1. time=8 ms
64 bytes from 66.218.71.198: icmp_seq=2. time=8 ms
64 bytes from 66.218.71.198: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

Example 3 - Ping an IPv6 address.

```
ZEQU0xxxxDL> ping ipv6 3003::11
Pinging 3003::11 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/12/50
```

```
ZEQU0xxxxDL> ping ipv6 FF02::1
Pinging FF02::1 with 64 bytes of data:
64 bytes from FF02::1: icmp_seq=1. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=1050 ms
64 bytes from FF02::1: icmp_seq=2. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=1050 ms
64 bytes from FF02::1: icmp_seq=3. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=70 ms
64 bytes from FF02::1: icmp_seq=4. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=1050 ms
64 bytes from FF02::1: icmp_seq=4. time=70 ms
64 bytes from FF02::1: icmp_sq=4. time=1050 ms
---- FF02::1 PING Statistics----
4 packets transmitted, 12 packets received
```

21.2 Ssh

This feature is not supported.

To start an encrypted session with a remote networking device, use the ssh command in user EXEC or privileged EXEC mode.

Syntax

```
ssh {ip-address | hostname} [port] [keyword...]
```

Parameters

- ip-address—Specifies the destination host IP address (IPv4 or IPv6).
- hostname—Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- port—Specifies the decimal TCP port number. The default port is the SSH port (22).
- keyword—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

Keywords Table

Options	Description
/password password	Specifies the password to use when logging in on the remote networking device running the SSH server. If the keyword is not specified, the password configured by the ip ssh-client password command is used. If this keyword is specified the the /user keyword must be specified too.
/source-interface interface-id	Specifies the source interface which minimal IPv4/v6 address will be used as the source IPv4/v6 address. If the keyword is not specified, the source IPv4/IPv6 address configured by the ip ssh-client source-interface command is used.
/user user-name	Specifies the user name to use when logging in on the remote networking device running the SSH server. If the keyword is not specified, the user name configured by the ip ssh-client username command is used. If this keyword is specified the /password keyword must be specified too.

Default Configuration

The default port is the SSH port (22) on the host.

Command Mode

Privileged EXEC mode

User Guidelines

The ssh command enables the switch to make a secure, encrypted connection to another switch running an SSH server. This connection provides functionality that is similar to that of a Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Only one SSH terminal connection can be active at the same time.

Examples

Example 1. The following example sets a secure session between the local device and the edge device HQedge. The user name and password configured by the ip ssh-client username and ip ssh-client password commands are used.

```
ZEQU0xxxxDL> ssh HQedge
```

Example 2. The following example sets a secure session between the local device and the edge device 1.1.1.1. The user name is HQhost and the password is a password configured by the ip ssh-client password command.

```
ZEQU0xxxxDL> ssh 1.1.1.1 /user HQhost
```

Example 3. The following example sets a secure session between the local device and the edge device HQedge. The user name is HQhost and the password is ar3245ddd.

```
ZEQU0xxxxDL> ssh HQedge /user HQhost /password ar3245ddd
```

Example 4. The following example sets a lookback interface as a source interface:

```
ZEQU0xxxxDL> ssh HQedge /source-interface loopback1
```

21.3 telnet

The telnet EXEC mode command logs on to a host that supports Telnet.

Syntax

telnet {ip-address | hostname} [port] [keyword...]

Parameters

- ip-address—Specifies the destination host IP address (IPv4 or IPv6).
- hostname—Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- port—Specifies the decimal TCP port number or one of the keywords listed in the Ports table in the User Guidelines.
- keyword—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

Default Configuration

The default port is the Telnet port (23) on the host.

Command Mode

Privileged EXEC mode

User Guidelines

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions.

Keywords Table

Options	Description
/echo	Enables local echo.
/quiet	Prevents onscreen display of all messages from the software.
/source-interfac	Specifies the source interface. e
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Returns to the System Command Prompt.

Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Example

The following example displays logging in to IP address 172.16.10.50 via Telnet.

```
ZEQU0xxxxDL> telnet 172. 16. 10. 50
```

21.4 traceroute

To display the routes that packets will take when traveling to their destination, use the traceroute EXEC mode command.

Syntax

```
traceroute ip {ipv4-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address]
```

```
traceroute ipv6 {ipv6-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address]
```

Parameters

- ip—Use IPv4 to discover the route.
- ipv6—Use IPv6 to discover the route.
- ipv4-address—IPv4 address of the destination host.
- ipv6-address—IPv6 address of the destination host.
- hostname—Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- size packet_size—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- ttl max-ttl—The largest TTL value that can be used. The default is 30. The traceroute command terminates when the destination is reached or when this value is reached. (Range: 1–255)
- count packet_count—The number of probes to be sent at each TTL level. The default count is 3. (Range: 1–10)
- timeout time_out—The number of seconds to wait for a response to a probe packet. The default is 3 seconds. (Range: 1–60)
- source ip-address—One of the interface addresses of the device to use as a source address for the probes. The device selects the optimal source address by default. (Range: Valid IP address)

Default Usage

N/A

Command Mode
Privileged EXEC mode

User Guidelines

The traceroute command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The traceroute command sends several probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet can result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the traceroute command prints an asterisk (*).

The traceroute command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

The traceroute ipv6 command is not relevant to IPv6 link local addresses.

Example

```
ZEQU0xxxxDL> traceroute ip aaa.bbb.ccc.ddd.com
```

Type Esc to abort.

Tracing the route to aaa.bbb.ccc.ddd.com (111.222.111.35)

1 i2-gateway.eee.com (192.67.123.45) 0 msec 0 msec 0 msec

2 Ita.main.core.NET (111.23.1.213) 0 msec 0 msec 0 msec

3 pana.fun.net (198.123.255.52) 10 msec 10 msec 10 msec

4 pana.fun2.net (198.123.255.62) 10 msec 10 msec 10 msec

5 aaa.bbb.ccc.ddd.com (111.222.111.35) 21 msec 21 msec 21 msec

Trace completed

The following table describes the significant fields shown in the display:

Field	Description
1	Indicates the sequence number of the router in the path to the host.
i2-gateway.eee.com	Host name of this router.
192.67.123.45	IP address of this router.
1 msec 1 msec 1	Round-trip time for each of the probes that msec are sent.

The following are characters that can appear in the traceroute command output:

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation required and DF is set.

H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded
S	Source route failed.
U	Port unreachable.

22 IPv6 Commands

22.1 clear ipv6 neighbors

Use the clear ipv6 neighbors command in privileged EXEC mode to delete all entries in the IPv6 neighbor discovery cache, except static entries.

Syntax

clear ipv6 neighbors

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Example

The following example deletes all entries, except static entries, in the neighbor discovery cache:

```
ZEQU0xxxxDL# clear ipv6 neighbors
```

22.2 ipv6 address

Use the `ipv6 address` command in Interface Configuration mode to configure a global unicast IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface. To remove the address from the interface, use the `no` form of this command.

Syntax

`ipv6 address ipv6-address/prefix-length`

`no ipv6 address [ipv6-address/prefix-length]`

Parameters

- `ipv6-address`—Specifies the global unicast IPv6 address assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- `prefix-length`—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration mode

User Guidelines

The `ipv6 address` command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the `no IPv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

Example

The following example defines the IPv6 global address `2001:DB8:2222:7272::72` on `vlan 100`:

```
ZEQU0xxxxDL (config) # interface vlan 100
ZEQU0xxxxDL (config-if) # ipv6 address 2001:DB8:2222:7272::72/64
ZEQU0xxxxDL (config-if) # exit
```

22.3 ipv6 address anycast

Use the `ipv6 address anycast` command in Interface Configuration mode to configure a global unicast IPv6 Anycast address and enable IPv6 processing on an interface. To remove the address from the interface, use the `no` form of this command.

Syntax

```
ipv6 address ipv6-prefix/prefix-length anycast
```

```
no ipv6 address [ipv6-prefix/prefix-length]
```

Parameters

- `ipv6-address`—Specifies the global unicast IPv6 address assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- `prefix-length`—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration mode

User Guidelines

An Anycast address is an address that is assigned to a set of interfaces that typically belong to different nodes. A packet sent to an Anycast address is delivered to the closest interface—as defined by the routing protocols in use—identified by the Anycast address. Anycast addresses are syntactically indistinguishable from Unicast addresses because Anycast addresses are allocated from the Unicast address space. Nodes to which the Anycast address is assigned must be explicitly configured to recognize that the address is an Anycast address.

Anycast addresses can be used only by a router, not a host, and Anycast addresses must not be used as the source address of an IPv6 packet.

The subnet router Anycast address has a prefix concatenated by a series of zeros (the interface ID). The subnet router Anycast address can be used to reach a router on the link that is identified by the prefix in the subnet router Anycast address.

The `ipv6 address anycast` command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the `no` form of the `ipv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example enables IPv6 processing on the interface, assigns the prefix `2001:0DB8:1:1::/64` to the interface, and configures the IPv6 Anycast address `2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE`:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
ZEQU0xxxxDL(config-if)# exit
```

22.4 ipv6 address autoconfig

Use the `ipv6 address autoconfig` command in Interface Configuration mode to enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages. To disable automatic configuration of IPv6 addresses and to remove the automatically configured address from the interface, use the `no` form of this command.

Syntax

`ipv6 address autoconfig`

`no ipv6 address autoconfig`

Parameters

N/A.

Default Configuration

Stateless Auto configuration is enabled.

Command Mode

Interface Configuration mode

User Guidelines

This command enables IPv6 on an interface (if it was disabled) and causes the switch to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the eui-64 based addresses to the interface.

Stateless auto configuration is applied only when IPv6 Forwarding is disabled. When IPv6 forwarding is changed from disabled to enabled, and stateless auto configuration is enabled the switch stops stateless auto configuration and removes all stateless auto configured ipv6 addresses from all interfaces.

When IPv6 forwarding is changed from enabled to disabled and stateless auto configuration is enabled the switch resumes stateless auto configuration.

Additionally the `ipv6 address autoconfig` command enables on the interface the DHCPv6 Stateless client to receive DHCP stateless information and this information is received from a DHCPv6 server regardless whether IPv6 Forwarding is enabled or not.

Using the `no` form of the `ipv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example assigns the IPv6 address automatically:

```
ZEQU0xxxxDL(config)# interface vlan 100  
ZEQU0xxxxDL(config-if)# ipv6 address autoconfig  
ZEQU0xxxxDL(config-if)# exit
```

22.5 ipv6 address eui-64

Use the `ipv6 address eui-64` command in Interface Configuration mode to configure a global unicast IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address. To remove the address from the interface, use the `no` form of this command.

Syntax

```
ipv6 address ipv6-prefix/prefix-length eui-64  
no ipv6 address [ipv6-prefix/prefix-length eui-64]
```

Parameters

- `ipv6-prefix`—Specifies the global unicast IPv6 address assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- `prefix-length`—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration mode

User Guidelines

If the value specified for the `prefix-length` argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

The IPv6 address is built from `ipv6-prefix` and the EUI-64 Interface ID by the following way:

- The first `prefix-length` bits are taken from `ipv6-prefix`.
- If `prefix-length < 64` then
 - The following `(64-prefix-length)` bits are filled by 0s.
 - The last 64 bits are taken from the EUI-64 Interface ID.
- If `prefix-length` equals to 64 then the following 64 bits are taken from the EUI-64 Interface ID.

- If prefix-length > 64 then the following (128-prefix-length) bits are taken from the last (64-(prefix-length -64)) bits of the EUI-64 Interface ID.

If the switch detects another host using one of its IPv6 addresses, it adds the IPv6 address and displays an error message on the console.

Using the no form of the ipv6 address command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example enables IPv6 processing on VLAN 1, configures IPv6 global address 2001:0DB8:0:1::/64 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
ZEQU0xxxxDL (config)# interface vlan 1
ZEQU0xxxxDL (config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
ZEQU0xxxxDL (config-if)# exit
```

22.6 ipv6 address link-local

Use the `ipv6 address link-local` command in Interface Configuration mode to configure an IPv6 link local address for an interface and enable IPv6 processing on the interface. To remove the manually configured link local address from the interface, use the `no` form of this command.

Syntax

```
ipv6 address ipv6-prefix link-local
```

```
no ipv6 address [link-local]
```

Parameters

- `ipv6-address`—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

Default Configuration

The default Link-local address is defined.

Command Mode

Interface Configuration mode

User Guidelines

The switch automatically generates a link local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link local address to be used by an interface, use the `ipv6 address link-local` command.

The `ipv6 address link-local` command cannot be applied to define an IPv6 address on an ISATAP interface.

Using the `no` form of the `ipv6 address` command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example enables IPv6 processing on VLAN 1 and configures FE80::260:3EFF:FE11:6770 as the link local address for VLAN 1:

```
ZEQU0xxxxDL (config)# interface vlan 1  
ZEQU0xxxxDL (config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local  
ZEQU0xxxxDL (config-if)# exit
```

22.7 ipv6 default-gateway

Use the `ipv6 default-gateway` Global Configuration mode command to define an IPv6 default gateway. To remove the IPv6 default gateway, use the `no` form of this command.

Syntax

```
ipv6 default-gateway ipv6-address | interface-id
```

```
no ipv6 default-gateway ipv6-address | interface-id
```

Parameters

- `ipv6-address`—Specifies the IPv6 address of an IPv6 router that can be used to reach a network.
- `interface-id`—Specifies the Interface Identifier of the outgoing interface that can be used to reach a network. This argument can be applied only to point-to-point interfaces (manual IPv6 over IPv4 tunnels).

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

The command is an alias of the `ipv6 route` command with the predefined (default) route: `ipv6 route ::/0 ipv6-address | interface-id`

See the definition of the `ipv6 route` command for details.

Examples

Example 1. The following example defines a default gateway with a global IPv6 address:

```
ZEQU0xxxxDL (config)# ipv6 default-gateway 5::5
```

Example 2. The following example defines a default gateway with a link-local IPv6 address:

```
ZEQU0xxxxDL (config)# ipv6 default-gateway  
FE80::260:3EFF:FE11:6770%vlan1
```

22.8 ipv6 enable

Use the `ipv6 enable` command in Interface Configuration mode to enable IPv6 processing on an interface.

To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the `no` form of this command.

Syntax

`ipv6 enable`

`no ipv6 enable`

Parameters

N/A.

Default Configuration

IPv6 interface is disabled.

Command Mode

Interface Configuration mode

User Guidelines

This command automatically configures an IPv6 link-local Unicast address on the interface while also enabling the interface for IPv6 processing. The `no ipv6 enable` command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Example

The following example enables VLAN 1 for the IPv6 addressing mode.

```
ZEQU0xxxxDL (config)# interface vlan 1  
ZEQU0xxxxDL (config-if)# ipv6 enable  
ZEQU0xxxxDL (config-if)# exit
```

22.9 ipv6 hop-limit

Use the `ipv6 hop-limit` command in Global Configuration mode to configure the maximum number of hops used in all IPv6 packets that are originated by the router.

To return the hop limit to its default value, use the `no` form of this command.

Syntax

`ipv6 hop-limit value`

`no ipv6 hop-limit`

Parameters

- `value`—Maximum number of hops. The acceptable range is from 1 to 255.

Default Configuration

The default is 64 hops.

Command Mode

Global Configuration mode

Example

The following example configures a maximum number of 15 hops for all IPv6 packets that are originated from the router:

```
ZEQU0xxxxDL (config)# ipv6 hop-limit 15
```

22.10 **ipv6 icmp error-interval**

Use the `ipv6 icmp error-interval` command in Global Configuration mode to configure the interval and bucket size for IPv6 ICMP error messages. To return the interval to its default setting, use the `no` form of this command.

Syntax

`ipv6 icmp error-interval milliseconds [bucketsize]`

`no ipv6 icmp error-interval`

Parameters

- **milliseconds**—Time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0 to 2147483647. A value of 0 disables ICMP rate limiting.
- **bucketsize**—Maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200.

Default Configuration

The default interval is 100ms and the default bucketsize is 10 i.e. 100 ICMP error messages per second.

Command Mode

Global Configuration mode

User Guidelines

Use this command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The `milliseconds` argument specifies the time interval between tokens arriving in the bucket. The optional `bucketsize` argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the `bucketsize` is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Average Packets Per Second = $(1000 / \text{milliseconds}) * \text{bucketsize}$. To disable

ICMP rate limiting, set the `milliseconds` argument to zero.

Example

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
ZEQU0xxxxDL (config)# ipv6 icmp error-interval 50 20
```

22.11 **ipv6 link-local default zone**

Use the Ipv6 link-local default zone command to configure an interface to egress a link local packet without a specified interface or with the default zone 0.

Use the no form of this command to return the default link local interface to the default value.

Syntax

Ipv6 link-local default zone interface-id

no Ipv6 link-local default zone

Parameters

- interface-id—Specifies the interface that is used as the egress interface for packets sent without a specified IPv6Z interface identifier or with the default 0 identifier.

Default

By default, link local default zone is disabled.

Command Mode

Global Configuration mode

Example

The following example defines VLAN 1 as a default zone:

```
ZEQU0xxxxDL (config)# ipv6 link-local default zone vlan1
```

22.12 **ipv6 nd advertisement-interval**

Use the `ipv6 nd advertisement-interval` in Interface Configuration mode to configure the advertisement interval option in router advertisements (RAs).

To reset the interval to the default value, use the `no` form of this command.

Syntax

`ipv6 nd advertisement-interval`

`no ipv6 nd advertisement-interval`

Parameters

N/A.

Default Configuration

Advertisement interval option is not sent.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 nd advertisement-interval` command to indicate to a visiting mobile node the interval at which that node may expect to receive RAs. The node may use this information in its movement detection algorithm.

Example

The following example enables the advertisement interval option to be sent in RAs:

```
ZEQU0xxxxDL (config) # interface vlan 1
ZEQU0xxxxDL (config-if) # ipv6 nd advertisement-interval
ZEQU0xxxxDL (config-if) # exit
```

22.13 **ipv6 nd dad attempts**

Use the `ipv6 nd dad attempts` command in Interface Configuration mode to configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the Unicast IPv6 addresses of the interface.

To return the number of messages to the default value, use the `no` form of this command.

Syntax

`ipv6 nd dad attempts value`

`no ipv6 nd dad attempts`

Parameters

- **value**—The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

Default Configuration

1

Command Mode

Interface Configuration mode

User Guidelines

Duplicate address detection verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of Unicast IPv6 addresses.

The `DupAddrDetectTransmits` node configuration variable (as specified in RFC 4862, IPv6 Stateless Address Autoconfiguration) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface, while duplicate address detection is performed on a tentative Unicast IPv6 address.

The interval between duplicate address detection, neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable `RetransTimer` (as specified in RFC 4861, Neighbor Discovery for IPv6), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the `ipv6 nd ns-interval` command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the Unicast IPv6 addresses assigned to the interface are

set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

An interface returning to administratively up, restarts duplicate address detection for all of the Unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error SYSLOG message is issued.

If the duplicate address is a global address of the interface, the address is not used and an error SYSLOG message is issued.

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Note. Since DAD is not supported on NBMA interfaces the command is allowed but does not impact on an IPv6 tunnel interface of the ISATAP type it does not impact. The configuration is saved and will impacted when the interface type is changed on another type on which DAD is supported (for example, to the IPv6 manual tunnel).

Example

The following example configures five consecutive neighbor solicitation messages to be sent on VLAN 1 while duplicate address detection is being performed on the tentative Unicast IPv6 address of the interface. The example also disables duplicate address detection processing on VLAN 2.

```
ZEQU0xxxxDL (config)# interface vlan 1
ZEQU0xxxxDL (config-if)# ipv6 nd dad attempts 5
ZEQU0xxxxDL (config-if)# exit
ZEQU0xxxxDL (config)# interface vlan 2
ZEQU0xxxxDL (config-if)# ipv6 nd dad attempts 0
ZEQU0xxxxDL (config-if)# exit
```

22.14 **ipv6 nd hop-limit**

Use the `ipv6 nd hop-limit` command in Global Configuration mode to configure the maximum number of hops used in router advertisements.

To return the hop limit to its default value, use the `no` form of this command.

Syntax

`ipv6 nd hop-limit value`

`no ipv6 nd hop-limit`

Parameters

- `value`—Maximum number of hops. The acceptable range is from 1 to 255.

Default Configuration

The default value is defined by the `ipv6 hop-limit` command, or is set to 64 hops, if the command was not configured.

Command Mode

Interface Configuration mode

User Guidelines

Use this command if you want to change the default value. The default value is defined by the `ipv6 hop-limit` command.

Example

The following example configures a maximum number of 15 hops for router advertisements on VLAN 2:

```
ZEQU0xxxxDL (config)# interface vlan 2
ZEQU0xxxxDL (config-if)# ipv6 nd hop-limit 15
ZEQU0xxxxDL (config-if)# exit
```

22.15 **ipv6 nd managed-config-flag**

Use the `ipv6 nd managed-config-flag` command in Interface Configuration mode to set the “managed address configuration flag” in IPv6 router advertisements.

To clear the flag from IPv6 router advertisements, use the `no` form of this command.

Syntax

```
ipv6 nd managed-config-flag  
no ipv6 nd managed-config-flag
```

Parameters

N/A.

Default Configuration

The “managed address configuration flag” flag is not set in IPv6 router advertisements.

Command Mode

Interface Configuration mode

User Guidelines

Setting the Managed Address Configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If this flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses, and if it is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Example

The following example configures the Managed Address Configuration flag in IPv6 router advertisements on VLAN 1:

```
ZEQU0xxxxDL(config)# interface vlan 1  
ZEQU0xxxxDL(config-if)# ipv6 nd managed-config-flag  
ZEQU0xxxxDL(config-if)# exit
```

22.16 **ipv6 nd ns-interval**

Use the `ipv6 nd ns-interval` command in Interface Configuration mode to configure the interval between IPv6 neighbor solicitation retransmissions on an interface.

To restore the default interval, use the `no` form of this command.

Syntax

`ipv6 nd ns-interval milliseconds`

`no ipv6 nd ns-interval`

Parameters

- `milliseconds`—Interval between IPv6 neighbor solicit transmissions. The acceptable range is from 1000 to 3600000 milliseconds.

Default Configuration

0 seconds (unspecified) is advertised in router advertisements and the value 1000 milliseconds is used for the neighbor discovery activity of the router itself.

Command Mode

Interface Configuration mode

User Guidelines

This value will be included in all IPv6 router advertisements sent out this interface. Very short intervals are not recommended in normal IPv6 operation. When a non-default value is configured, the configured time is both advertised and used by the router itself.

Example

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for VLAN 1:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 nd ns-interval 9000
ZEQU0xxxxDL(config-if)# exit
```

22.17 **ipv6 nd other-config-flag**

Use the `ipv6 nd other-config-flag` command in Interface Configuration mode to set the Other Stateful configuration flag in IPv6 router advertisements.

To clear the flag from IPv6 router advertisements, use the `no` form of this command.

Syntax

`ipv6 nd other-config-flag`

`no ipv6 nd other-config-flag`

Parameters

N/A.

Default Configuration

The Other Stateful configuration flag is not set in IPv6 router advertisements.

Command Mode

Interface Configuration mode

User Guidelines

The setting of the Other Stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note. If the Managed Address Configuration flag is set using the `ipv6 nd managed-config-flag` command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the Other Stateful configuration flag.

Example

The following example configures the Other Stateful configuration flag in IPv6 router advertisements on VLAN 1:

```
ZEQU0xxxxDL (config)# interface vlan 1
ZEQU0xxxxDL (config-if)# ipv6 nd other-config-flag
ZEQU0xxxxDL (config-if)# exit
```

22.18 **ipv6 nd prefix**

Use the `ipv6 nd prefix` command in Interface Configuration mode to configure which IPv6 prefixes are included in IPv6 Neighbor Discovery (ND) router advertisements.

To remove the prefixes, use the `no` form of this command.

Syntax

```
ipv6 nd prefix {ipv6-prefix/prefix-length | default} [no-advertise | {[valid-lifetime  
preferred-lifetime] [no-autoconfig] [off-link | no-onlink]}]
```

```
no ipv6 nd prefix [ipv6-prefix/prefix-length | default]
```

Parameters

- `ipv6-prefix`—IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC4293, where the address is specified in hexadecimal using 16-bit values between colons.
- `/prefix-length`—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- `default`—Default values used for automatic advertised prefixes configured as addresses on the interface using the `ipv6 address` command.
- `no-advertise`—Prefix is not advertised.
- `valid-lifetime`—Remaining length of time, in seconds, that this prefix will continue to be valid, i.e., time until invalidation. A value of 4,294,967,295 represents infinity. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.
- `preferred-lifetime`—Remaining length of time, in seconds, that this prefix will continue to be preferred, i.e., time until deprecation. A value of 4,294,967,295 represents infinity. The address generated from a deprecated prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The preferred-lifetime must not be larger than the valid-lifetime.
- `no-autoconfig`—Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration. The prefix will be advertised with the A-bit clear.
- `off-link`—Configures the specified prefix as off-link. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured using the `ipv6 address` command), then it will be removed.

- no-onlink—Configures the specified prefix as not on-link. The prefix will be advertised with the L-bit clear.

Default Configuration

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2,592,000 seconds (30 days) and a preferred lifetime of 604,800 seconds (7 days).

Note that by default:

- All prefixes are inserted in the routing table as connected prefixes.
- All prefixes are advertised as on-link (for example, the L-bit is set in the advertisement)
- All prefixes are advertised as an auto-configuration prefix (for example, the A-bit is set in the advertisement)

Command Mode

Interface Configuration mode

User Guidelines

This command enables control over the individual parameters per prefix, including whether the prefix should be advertised.

Use the `ipv6 nd prefix ipv6-prefix/prefix-length` command to add the prefix to the Prefix table.

Use the `no ipv6 nd prefix ipv6-prefix/prefix-length` command to remove the prefix from the Prefix table.

Use the `no ipv6 nd prefix` command without the `ipv6-prefix/prefix-length` argument to remove all prefixes from the Prefix Table.

Note. The `no ipv6 nd prefix` command does not return the default values to the original default values.

The switch supports the following advertisement algorithm:

- Advertise all prefixes that are configured as addresses on the interface using the parameters defined by the `ipv6 nd prefix default` command (or the default value if the command has not been configured) except prefixes that are placed in the Prefix table (changed (configured) by the `ipv6 nd prefix` command).
- Advertise all prefixes configured by the `ipv6 nd prefix` command without the `no-advertise` keyword.

Default Keyword

The default keyword can be used to set default values for automatic advertised prefixes configured as addresses on the interface using the `ipv6 address` command.

Note. These default values are not used as the default values in the `ipv6 nd prefix` command.

Use the `no ipv6 nd prefix default` command to return the default values to the original default values.

On-Link

When on-link is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. An on-link prefix is inserted into the routing table as a Connected prefix.

Auto-configuration

When auto-configuration is on (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 auto-configuration.

The configuration options affect the L-bit and A-bit settings associated with the prefix in the IPv6 ND Router Advertisement, and presence of the prefix in the routing table, as follows:

• Default	L=1 A=1, In the Routing Table
• no-onlink	L=0 A=1, In the Routing Table
• no-autoconfig	L=1 A=0, In the Routing Table
• no-onlink no-autoconfig	L=0 A=0, In the Routing Table
• off-link	L=0 A=1, Not in the Routing Table
• off-link no-autoconfig	L=0 A=0, Not in the Routing Table

Examples

Example 1. The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out VLAN 1 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds. The prefix is inserted in the Routing table:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
ZEQU0xxxxDL(config-if)# exit
```

Example 2. The following example advertises the prefix with the L-bit clear:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 address 2001::1/64
ZEQU0xxxxDL(config-if)# ipv6 nd prefix 2001::/64 3600 3600 no-onlink
ZEQU0xxxxDL(config-if)# exit
```

22.19 **ipv6 nd ra interval**

Use the `ipv6 nd ra interval` command in Interface Configuration mode to configure the interval between IPv6 router advertisement (RA) transmissions on an interface.

To restore the default interval, use the `no` form of this command.

Syntax

`ipv6 nd ra interval maximum-secs [minimum-secs]`

`no ipv6 nd ra interval`

Parameters

- `maximum-secs`—Maximum interval between IPv6 RA transmissions in seconds. The range is from 4 to 1800.
- `minimum-secs`—Minimum interval between IPv6 RA transmissions in seconds. The range is from 3 to 1350.

Default Configuration

`maximum-secs` is 600 seconds.

`minimum-secs` is $0.33 * \text{maximum-secs}$, if the value ≥ 3 seconds and is 3 seconds, if the value < 3 seconds.

Command Mode

Interface Configuration mode

User Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using this command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.

The minimum RA interval may never be more than 75% of the maximum RA interval and never less than 3 seconds.

Examples

Example 1. The following example configures an IPv6 router advertisement interval of 201 seconds for VLAN 1:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 nd ra interval 201
ZEQU0xxxxDL(config-if)# exit
```

Example 2. The following examples shows a maximum RA interval of 200 seconds and a minimum RA interval of 50 seconds:

```
ZEQU0xxxxDL (config)# interface vlan 1
ZEQU0xxxxDL (config-if)# ipv6 nd ra interval 200 50
ZEQU0xxxxDL (config-if)# exit
```

22.20 **ipv6 nd ra lifetime**

Use the `ipv6 nd ra lifetime` command in Interface Configuration mode to configure the Router Lifetime value in IPv6 router advertisements on an interface.

To restore the default lifetime, use the `no` form of this command.

Syntax

`ipv6 nd ra lifetime seconds`

`no ipv6 nd ra lifetime`

Parameters

- `seconds`—Remaining length of time, in seconds, that this router will continue to be useful as a default router (Router Lifetime value). A value of zero indicates that it is no longer useful as a default router. The acceptable range is 0 or from <Maximum RA Interval> to 9000 seconds.

Default Configuration

The default lifetime value is $3 \times \text{<Maximum RA Interval>}$ seconds.

Command Mode

Interface Configuration mode

User Guidelines

The Router Lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The Router Lifetime value can be set to a non-zero value to indicate that it should be considered a default router on this interface. The non-zero value for the Router Lifetime value should not be less than the router advertisement interval.

Example

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for VLAN 1:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 nd ra lifetime 1801
ZEQU0xxxxDL(config-if)# exit
```

22.21 **ipv6 nd suppress-ra**

Use the `ipv6 nd suppress-ra` command in Interface Configuration mode to suppress IPv6 router advertisement transmissions on an interface. To re-enable the sending of IPv6 router advertisement transmissions on an interface, use the `no` form of this command.

Syntax

`ipv6 nd suppress-ra`

`no ipv6 nd suppress-ra`

Parameters

N/A.

Default Configuration

LAN interface - IPv6 router advertisements are automatically sent.

Point-to-Point interface - IPv6 router advertisements are suppressed. NBMA

interface - IPv6 router advertisements are suppressed.

Command Mode

Interface Configuration mode

User Guidelines

Use the `no ipv6 nd suppress-ra` command to enable the sending of IPv6 router advertisement transmissions on a Point-to-Point interface (for example, manual tunnel).

NBMA interface - IPv6 router advertisements are suppressed.

Use the `no ipv6 nd suppress-ra` command to enable the sending of IPv6 router advertisement transmissions on a NBMA interface (for example, ISATAP tunnel).

Examples

Example 1. The following example suppresses IPv6 router advertisements on vlan 1:

```
ZEQU0xxxxDL (config)# interface vlan 1
ZEQU0xxxxDL (config-if)# ipv6 nd suppress-ra
ZEQU0xxxxDL (config-if)# exit
```

22.22 **ipv6 nd reachable-time**

Use the `ipv6 nd reachable-time` command in Interface Configuration mode to configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

To restore the default time, use the `no` form of this command.

Syntax

`ipv6 nd reachable-time milliseconds`

`no ipv6 nd reachable-time`

Parameters

- `milliseconds`—Amount of time that a remote IPv6 node is considered reachable (in milliseconds). The acceptable range is from 0 to 3600000 milliseconds.

Default Configuration

0 milliseconds (unspecified) is advertised in router advertisements and the value 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

Command Mode

Interface Configuration mode

User Guidelines

The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 means indicates that the configured time is unspecified by this router.

Example

The following example configures an IPv6 reachable time of 1,700,000 milliseconds for VLAN 1:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 nd reachable-time 1700000
ZEQU0xxxxDL(config-if)# exit
```

22.23 **ipv6 nd router-preference**

Use the `ipv6 nd router-preference` command in Interface Configuration mode to configure a default router preference (DRP) for the router on a specific interface.

To return to the default DRP, use the `no` form of this command.

Syntax

`ipv6 nd router-preference {high | medium | low}`

`no ipv6 nd router-preference`

Parameters

- `high`—Preference for the router specified on an interface is high.
- `medium`—Preference for the router specified on an interface is medium.
- `low`—Preference for the router specified on an interface is low.

Default Configuration

Router advertisements (RAs) are sent with the medium preference.

Command Mode

Interface Configuration mode

User Guidelines

RA messages are sent with the DRP configured by the this command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Example

The following example configures a DRP of high for the router on VLAN 1:

```
ZEQU0xxxxDL (config)# interface vlan 1
ZEQU0xxxxDL (config-if)# ipv6 nd router-preference high
ZEQU0xxxxDL (config-if)# exit
```

22.24 **ipv6 neighbor**

Use the `ipv6 neighbor` command in Global Configuration mode to configure a static entry in the IPv6 neighbor discovery cache. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the `no` form of this command.

Syntax

```
ipv6 neighbor ipv6-address interface-id mac-address
```

```
no ipv6 neighbor [[ipv6-address] interface-id]
```

Parameters

- `ipv6-address`—Specified IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- `interface-id`—Specified interface identifier.
- `mac-address`—Interface MAC address.

Default Configuration

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Mode

Global Configuration mode

User Guidelines

This command is similar to the `arp` command.

Use the `ipv6 neighbor` command to add a static entry in the IPv6 neighbor discovery cache.

If the specified IPv6 address is a global IPv6 address it must belong to one of static on-link prefixes defined in the interface. When a static on-link prefix is deleted all static entries in the IPv6 neighbor discovery cache corresponding the prefix is deleted to.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache, learned through the IPv6 neighbor discovery process, the entry is automatically converted to a static entry.

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Use the `no ipv6 neighbor ipv6-address interface-id` command to remove the one given static entry on the given interface. The command does not remove the entry from the cache, if it is a dynamic entry, learned from the IPv6 neighbor discovery process.

Use the `no ipv6 neighbor interface-id` command to delete the all static entries on the given interface.

Use the `no ipv6 neighbor` command to remove the all static entries on all interfaces.

Use the `show ipv6 neighbors` command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- **NCMP (Incomplete)**—The interface for this entry is down.
- **REACH (Reachable)**—The interface for this entry is up.

Note. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the **INCMP** and **REACH** states are different for dynamic and static cache entries.

Examples

Example 1. The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
ZEQU0xxxxDL (config)# ipv6 neighbor 2001:0DB8::45A vlan1 0002.7D1A.9472
```

Example 2. The following example deletes the static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
ZEQU0xxxxDL (config)# no ipv6 neighbor 2001:0DB8::45A vlan1
```

Example 3. The following example deletes all static entries in the IPv6 neighbor discovery cache on VLAN 1:

```
ZEQU0xxxxDL (config)# no ipv6 neighbor vlan1
```

Example 4. The following example deletes all static entries in the IPv6 neighbor discovery cache on all interfaces:

```
ZEQU0xxxxDL (config)# no ipv6 neighbor
```

22.25 **ipv6 redirects**

Use the `ipv6 redirects` command in Interface Configuration mode to enable the sending of ICMP IPv6 redirect messages to re-send a packet through the same interface on which the packet was received.

To disable the sending of redirect messages, use the `no` form of this command.

Syntax

`ipv6 redirects`

`no ipv6 redirects`

Parameters

N/A.

Default Configuration

The sending of ICMP IPv6 redirect messages is enabled.

Command Mode

Interface Configuration mode

Example

The following example disables the sending of ICMP IPv6 redirect messages on VLAN 100 and re-enables the messages on VLAN 2:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# no ipv6 redirects
ZEQU0xxxxDL(config-if)# exit
ZEQU0xxxxDL(config)# interface vlan 2
ZEQU0xxxxDL(config-if)# ipv6 redirects
ZEQU0xxxxDL(config-if)# exit
```

22.26 **ipv6 route**

Use the `ipv6 route` command in Global Configuration mode to establish static IPv6 routes.

To remove a previously configured static route, use the `no` form of this command.

Syntax

```
ipv6 route ipv6-prefix/prefix-length {next--ipv6-address | interface-id} [metric]
```

```
no ipv6 route ipv6-prefix/prefix-length {next--ipv6-address | interface-id}
```

Parameters

- `ipv6-prefix`—IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.
- `/prefix-length`—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- `next-ipv6-address`—IPv6 address of the next hop that can be used to reach the specified network.
 - If the `next--ipv6-address` argument is a link local address it must be defined in the zone format: IPv6 Zone Format> ::= IPv6-Link-Local-Address%Interface-ID
 - The `interface-id` argument must be coded without spaces.
- `interface-id`—Outgoing Interface identifier. This argument can be applied only to point-to-point interfaces (manual IPv6 over IPv4 tunnels).
- `metric`—Static route metric. Acceptable values are from 1 to 65535. The default value is 1.

Default Configuration

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Mode

Global Configuration mode

User Guidelines

If the next IPv6 address is a global IPv6 address, it should belong to a static on-link prefix. When an on-link prefix is removed or is changed to non on-link prefix, the static routes with next hop belonging to the prefix are removed from the configuration.

Examples

Example 1. The following example defines a static route with a global next hop:

```
ZEQU0xxxxDL (config)# ipv6 route 2001::/64 5::5 10
```

Example 2. The following example defines a static route with a link-local next hop:

```
ZEQU0xxxxDL (config)# ipv6 route 2001:DB8:2222::/48  
FE80::260:3EFF:FE11:6770% vlan1 12
```

22.27 **ipv6 unicast-routing**

Use the `ipv6 unicast-routing` command in Global Configuration mode to enable the forwarding of IPv6 Unicast datagrams.

To disable the forwarding of IPv6 Unicast datagrams, use the `no` form of this command.

Syntax

`ipv6 unicast-routing`

`no ipv6 unicast-routing`

Parameters

N/A.

Default Configuration

IPv6 Unicast routing is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the forwarding of IPv6 Unicast datagrams:

```
ZEQU0xxxxDL (conf ig) # ipv6 unicast-routing
```

22.28 **ipv6 unreachable**

Use the `ipv6 unreachable` command in Interface Configuration mode to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface.

To prevent the generation of unreachable messages, use the `no` form of this command.

Syntax

```
ipv6 unreachable
no ipv6 unreachable
```

Parameters

N/A.

Default Configuration

The sending of ICMP IPv6 unreachable messages is enabled.

Command Mode

Interface Configuration mode

User Guidelines

If the switch receives a Unicast packet destined for itself that uses a protocol it does not recognize, it sends an ICMPv6 unreachable message to the source.

If the switch receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

Example

The following example disables the generation of ICMPv6 unreachable messages, as appropriate, on an interface:

```
ZEQU0xxxxDL (config)# interface vlan 100
ZEQU0xxxxDL (config-if)# no ipv6 unreachable
ZEQU0xxxxDL (config-if)# exit
```

22.29 **show ipv6 interface**

Use the `show ipv6 interface` command in user EXEC or privileged EXEC mode to display the usability status of interfaces configured for IPv6.

Syntax

```
show ipv6 interface [brief] | [[interface-id] [prefix]]
```

Parameters

- `brief`—Displays a brief summary of IPv6 status and configuration for each interface where IPv6 is defined.
- `interface-id`—Interface identifier about which to display information.
 - `prefix`—Prefix generated from a local IPv6 prefix pool.

Default Configuration

Option `brief` - all IPv6 interfaces are displayed.

Command Mode User

EXEC mode Privileged

EXEC mode

User Guidelines

Use this command to validate the IPv6 status of an interface and its configured addresses. This command also displays the parameters that IPv6 uses for operation on this interface and any configured features.

If the interface's hardware is usable, the interface is marked up.

If you specify an optional interface identifier, the command displays information only about that specific interface. For a specific interface, you can enter the `prefix` keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

The keyword is supported only if IPv6 unicast routing is enabled.

Examples

Example 1. The show ipv6 interface command displays information about the specified interface:

```
ZEQU0xxxxDL# show ipv6 interface vlan 1
VLAN 1 is up/up
IPv6 is enabled, link-local address is
fe80::250:40ff:fe3b:bc42
IPv6 Forwarding is enabled
Global unicast address(es):
Ipv6 Global Address Type
3ffe:0:0:1::/64 (ANY) Autoconfig
3ffe:0:0:1::1/64 Manual
Joined group address(es):
ff02::1
ff02::2
ff02::1:ff00:0
ff02::1:ff00:1
ff02::1:ff3b:bc42
MTU is 1500 bytes
ICMP error messages limited interval is 100ms;
Bucket size is 10
tokens
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0
milliseconds
ND router maximum advertisement interval is 600
seconds
ND router minimum advertisement interval is 198
seconds (DEFAULT)
ND router advertisements live for 1800 seconds
ND advertised default router preference is
medium
Stateless autoconfiguration is disabled
MLD Version is 2
```

Field Descriptions:

- vlan 1 is up/up—Indicates the interface status: administrative/operational.
- IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked Enabled. If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked Stalled. If IPv6 is not enabled, the interface is marked Disabled.
- link-local address—Displays the link-local address assigned to the interface.

- Global unicast address(es):—Displays the global Unicast addresses assigned to the interface. The type is manual or autoconfig.
- Joined group address(es):—Indicates the Multicast groups to which this interface belongs.
- MTU is 1500 bytes—Maximum transmission unit of the interface.
- ICMP error messages—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
- ICMP redirects—State of ICMP IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
- ND DAD—The state of duplicate address detection on the interface (enabled or disabled).
- number of DAD attempts:—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
- ND reachable time—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
- ND advertised reachable time—Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
- ND advertised retransmit interval—Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
- ND router advertisements—Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire.
- ND advertised default router preference is Medium—DRP for the router on a specific interface.
- MLD Version—Version of MLD

Example 2. The following command with the brief keyword displays information about all interfaces that IPv6 is defined on:

```
ZEQU0xxxxDL# show ipv6 interface brief
```

Interface	Interface State	IPv6 State	Link Local IPv6 Address	MLD Version	Number of Global Addresses
vlan 1	up/up	enabled	fe80::250:40ff:fe3b:bc42	2	2
vlan 2	up/up	enabled	fe80::250:40ff:fe3b:bc42	2	2

Example 3. This sample output shows the characteristics of VLAN 1 that has generated a prefix from a local IPv6 prefix pool:

```

ZEQU0xxxxDL# configure terminal
ZEQU0xxxxDL(config)# interface vlan1
ZEQU0xxxxDL(config-if)# ipv6 address 2001:0DB8:1::1/64
ZEQU0xxxxDL(config-if)# ipv6 address 2001:0DB8:2::1/64
ZEQU0xxxxDL(config-if)# ipv6 address 2001:0DB8:3::1/64
ZEQU0xxxxDL(config-if)# ipv6 nd prefix 2001:0DB8:1::/64 no-advertise
ZEQU0xxxxDL(config-if)# ipv6 nd prefix 2001:0DB8:3::/64 2912000
564900 off-link
ZEQU0xxxxDL(config-if)# ipv6 nd prefix 2001:0DB8:4::/64
ZEQU0xxxxDL(config-if)# ipv6 nd prefix 2001:0DB8:5::/64 2912000
564900 off-link
ZEQU0xxxxDL(config-if)# exit
ZEQU0xxxxDL(config)# exit
ZEQU0xxxxDL# show ipv6 interface vlan 1 prefix
IPv6 Prefix Advertisements VLAN 1
Codes: A - Address, P - Prefix is advertised, R is in Routing Table
Code Prefix          Flags   Valid Lifetime Preferred Lifetime
-----
Default              LA      2592000    604800
AR  2001:0DB8:1::/64  LA      infinite   infinite
APR 2001:0DB8:2::/64  LA      infinite   infinite
AP  2001:0DB8:3::/64  A       infinite   infinite
PR  2001:0DB8:4::/64  LA      2592000    604800
P   2001:0DB8:5::/64  A       2912000    564900

```

22.30 **show ipv6 link-local default zone**

Use the show ipv6 link-local default zone command in user EXEC or privileged EXEC mode to display the IPv6 link local default zone.

Syntax

```
show ipv6 link-local default zone
```

Command Mode User

EXEC mode Privileged

EXEC mode

Examples

Example 1. The following example displays the default zone when it is defined:

```
ZEQU0xxxxDL# show ipv6 link-local default zone  
Link Local Default Zone is VLAN 1
```

Example 2. The following example displays the default zone when it is not defined:

```
ZEQU0xxxxDL# show ipv6 link-local default zone  
Link Local Default Zone is not defined
```

22.31 **show ipv6 nd prefix**

Use the `show ipv6 nd prefix` command in user EXEC or privileged EXEC mode to display IPv6 prefixes included in IPv6 Neighbor Discovery (ND) router advertisements.

Syntax

```
show ipv6 nd prefix [interface-id]
```

Parameters

- `interface-id`—Specified interface identifier on which prefixes are advertised.

Default Configuration

No prefixes are displayed.

Command Mode User

EXEC mode Privileged

EXEC mode

User Guidelines

Use the `show ipv6 nd prefix` command with the `interface-id` argument to display prefixes advertised on a single interface.

Example

The following example displays IPv6 prefixes:

```
ZEQU0xxxxDL# show ipv6 nd prefix vlan 100
vlan 100
  default

    valid-lifetime 2,592,000 secs
    preferred-lifetime 604,800 secs
    on-link
    auto-config
  prefix 2001::1/64
    valid-lifetime 3,600 secs
    preferred-lifetime 2,700 secs
  prefix 2001:2:12/64
    no advertise
  prefix 2002::1/64

    valid-lifetime 3,600 secs
    preferred-lifetime 2,700 secs
    on-link
  prefix 2011::1/64
    valid-lifetime 3,600 secs
    preferred-lifetime 2,700 secs
    off-link
    auto-config
```

22.32 show ipv6 neighbors

Use the show ipv6 neighbors command in User EXEC or Privileged EXEC mode to display IPv6 neighbor discovery (ND) cache information.

Syntax

```
show ipv6 neighbors [interface-id | ipv6-address | ipv6-hostname]
```

Parameters

- interface-id—Specifies the identifier of the interface from which IPv6 neighbor information is to be displayed.
- ipv6-address—Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- ipv6-hostname—Specifies the IPv6 host name of the remote networking device.

Default Configuration

All IPv6 ND cache entries are listed.

Command Mode User

EXEC mode Privileged

EXEC mode

User Guidelines

When the interface-id argument is not specified, cache information for all IPv6 neighbors is displayed. Specifying the interface-id argument displays only cache information about the specified interface.

Examples

Example 1. The following is sample output from the show ipv6 neighbors command when entered with an interface-id:

```
ZEQU0xxxxDL# show ipv6 neighbors vlan 1
```

IPv6 Address	Age	Link-layer Addr	State	Interface	Router
2000:0:0:4::2	0	0003. a0d6. 141e	REACH	VLAN1	Yes
3001:1::45a	–	0002. 7d1a. 9472	REACH	VLAN1	–
FE80::203:A0FF:FED6:141E	0	0003. a0d6. 141e	REACH	VLAN1	No

Example 2. The following is sample output from the show ipv6 neighbors command when entered with an IPv6 address:

```
ZEQU0xxxxDL#show ipv6 neighbors 2000:0:0:4::2
IPv6 Address           Age Link-layer Addr  State  Interface Router
2000:0:0:4::2         0  0003.a0d6.141e    REACH  VLAN1      Yes
```

Field Descriptions:

- Total number of entries—Number of entries (peers) in the cache.
- IPv6 Address—IPv6 address of neighbor or interface.
- Age—Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
- Link-layer Addr—MAC address. If the address is unknown, a hyphen (-) is displayed.
- Interface—Interface which the neighbor is connected to.
- Router—Specifies if the neighbor is a Router. A hyphen (-) is displayed for static entries.

22.33 **show ipv6 route**

Use the show ipv6 route command in user EXEC or privileged EXEC mode to display the current contents of the IPv6 routing table.

Syntax

```
show ipv6 route [ipv6-address | ipv6-prefix/prefix-length | protocol | interface interface-id]
```

Parameters

- **ipv6-address**—Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **ipv6-prefix**—Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- **protocol**—Displays routes for the specified routing protocol using any of these keywords: bgp, isis, ospf, or rip; or displays routes for the specified type of route using any of these keywords: connected, static, nd, or icmp.
- **interface interface-id**—Identifier of an interface.

Default Configuration

All IPv6 routing information for all active routing tables is displayed.

Command Mode User

EXEC mode Privileged

EXEC mode

User Guidelines

This command provides output similar to the show ip route command, except that the information is IPv6-specific.

When the ipv6-address or ipv6-prefix/prefix-length argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. When the icmp, nd, connected, local, or static keywords are specified, only that type of route is displayed. When the interface-id argument are specified, only the specified interface-specific routes are displayed.

Examples

Example 1. The following is sample output from the show ipv6 route command when IPv6 Routing is not enabled and the command is entered without an IPv6 address or prefix specified:

```
ZEQU0xxxxDL# show ipv6 route
Codes: > - Best
       S - Static, C - Connected, I - ICMP Redirect, ND - Router
Advertisement
[d/m]: d - route' s distance, m - route' s metric
IPv6 Routing Table - 6 entries
C> 3002:1:1:1:1/64 [0/0]
   via fe80::200:cff:fe4a:dfa8 VLAN 1 Lifetime 1784 sec
S> ::/0 [1/1]
   via fe80::77 VLAN 1
ND> ::/0 [11/0]
   via fe80::200:cff:fe4a:dfa8 VLAN 1 Lifetime 1784 sec
ND> 2001::/64 [2/1]
   via :: fe80::200:cff:fe4a:dfa8 VLAN 100
ND> 2002:1:1:1::/64 [2/1]
   via :: fe80::200:cff:fe4a:dfa8 VLAN 100
ND> 3001::/64 [2/1]
   via :: fe80::200:cff:fe4a:dfa8 VLAN 101
```

Example 2. The following is sample output from the show ipv6 route command when IPv6 Routing is enabled and the command is entered without an IPv6 address or prefix specified and IPv6 Routing is enabled:

```
ZEQU0xxxxDL# show ipv6 route
Codes: > - Best
       S - Static, C - Connected,
       L - Local(on-link prefixes defined by the ipv6 nd prefix command
         with on-link keyword,
[d/m]: d - route' s distance, m - route' s metric
IPv6 Routing Table - 3 entries
S> 3000::/64 [1/1]
   via FE80::A8BB:CCFF:FE02:8B00 VLAN 100
C> 4001::/64 [0/0]
   via :: VLAN 100
L> 4002::/64 [0/0]
   via :: VLAN 100 Lifetime 9000 sec
```

22.34 **show ipv6 route summary**

Use the show ipv6 route summary command in User EXEC or Privileged EXEC mode to display the current contents of the IPv6 routing table in summary format.

Syntax

```
show ipv6 route summary
```

Parameters

N/A.

Command Mode User

EXEC mode Privileged

EXEC mode

Example

The following is sample output from the show ipv6 route summary command:

```
ZEQU0xxxxDL# show ipv6 route summary
IPv6 Routing Table Summary - 97 entries
37 local, 35 connected, 25 static
Number of prefixes:
/16: 1, /28: 10, /32: 5, /35: 25, /40: 1, /64: 9
/96: 5, /112: 1, /127: 4, /128: 36
```

22.35 **show ipv6 static**

Use the show ipv6 static command in user EXEC or privileged EXEC mode to display the current static routes of the IPv6 routing table.

Syntax

```
show ipv6 static [ipv6-address | ipv6-prefix/prefix-length] [interface  
interface-id][detail]
```

Parameters

- **ipv6-address**—Provides routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **ipv6-prefix**—Provides routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- **interface interface-id**—Identifier of an interface.
- **detail**—Specifies for invalid routes, the reason why the route is not valid.

Default Configuration

All IPv6 static routing information for all active routing tables is displayed.

Command Mode User

EXEC mode Privileged

EXEC mode

User Guidelines

When the ipv6-address or ipv6-prefix/prefix-length argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the interface-id argument is specified, only the specified interface-specific routes are displayed.

When the detail keyword is specified, the reason why the route is not valid is displayed for invalid direct or fully specified routes.

Examples

Example 1. The following is sample output from the show ipv6 static command without specified options:

```
ZEQU0xxxxDL# show ipv6 static
IPv6 Static routes Code: * - installed in Routing Information Base
(RIB)
IPv6 Static routes distance is 1
* 3000::/16, interface VLAN1, metric 1
* 4000::/16, via nexthop 2001:1::1, metric 1
  5000::/16, interface VLAN2, metric 1
* 5555::/16, via nexthop 4000::1, metric 1
  5555::/16, via nexthop 9999::1, metric 1
* 5555::/16, via nexthop 4001:AF00::1, metric 1
* 6000::/16, via nexthop 2007::1, metric 1
```

Example 2. The following is sample output from the show ipv6 route command when entered with the IPv6 prefix 2001:200::/35:

```
ZEQU0xxxxDL# show ipv6 static 2001:200::/35
IPv6 Static routes Code: * - installed in Routing Information Base
(RIB)
IPv6 Static routes distance is 1
* 2001:200::/35, via nexthop 4000::1, metric 1
  2001:200::/35, via nexthop 9999::1, metric 1
* 2001:200::/35, interface VLAN1, metric 1
```

Example 3. The following is sample output from the show ipv6 route command when entered with the interface VLAN 1:

```
ZEQU0xxxxDL# show ipv6 static interface vlan 1
IPv6 Static routes Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 5000::/16, interface VLAN1, metric 1
```

Example 4. The following is sample output from the show ipv6 route command with the detail keyword:

```
ZEQU0xxxxDL# show ipv6 static detail
IPv6 Static routes Code: * - installed in Routing Information Base
(RIB)
IPv6 Static routes distance is 1
* 3000::/16, interface VLAN1, metric 1
* 4000::/16, via nexthop 2001:1::1, metric 1
  5000::/16, interface VLAN2, metric 1
Interface is down
* 5555::/16, via nexthop 4000::1, metric 1
  5555::/16, via nexthop 9999::1, metric 1
  Route does not fully resolve
* 5555::/16, via nexthop 4001:AF00::1, metric 1
* 6000::/16, via nexthop 2007::1, metric 1
```

23 IPv6 Prefix List Commands

23.1 clear ipv6 prefix-list

Use the clear ipv6 prefix-list command in privileged EXEC mode to reset the hit count of the IPv6 prefix list entries.

Syntax

clear ipv6 prefix-list [prefix-list-name [ipv6-prefix/prefix-length]]

Parameters

- prefix-list-name—The name of the prefix list from which the hit count is to be cleared.
- ipv6-prefix—The IPv6 network from which the hit count is to be cleared. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.
- /prefix-length—The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Default Configuration

The hit count is automatically cleared for all IPv6 prefix lists.

Command Mode

Privileged EXEC mode

User Guidelines

The hit count is a value indicating the number of matches to a specific prefix list entry.

Example

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35:

```
ZEQU0xxxxDL# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

23.2 ipv6 prefix-list

Use the `ipv6 prefix-list` command in Global Configuration mode to create an entry in an IPv6 prefix list. To delete the entry, use the `no` form of this command.

Syntax

```
ipv6 prefix-list list-name [seq number] { {deny|permit} ipv6-prefix/prefix-length [ge ge-length] [le le-length]} | description text
```

```
no ipv6 prefix-list list-name [seq number]
```

Parameters

- `list-name`—Name of the prefix list. The name may contain up to 32 characters.
- `seq seq-number`—Sequence number of the prefix list entry being configured. This is an integer value from 1 to 4294967294.
- `deny`—Denies networks that matches the condition.
- `permit`—Permits networks that matches the condition.
- `ipv6-prefix`—IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal—using 16-bit values between colons.
- `/prefix-length`—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value from 0 to 128. The zero prefix-length may be used only with the zero `ipv6-prefix (::)`.
- `description text`—Text that can be up to 80 characters in length.
- `ge ge-value`—Specifies a prefix length greater than or equal to the `/prefix-length` argument. It is the lowest value of a range of the length (the “from” portion of the length range).
- `le le-value`—Specifies a prefix length greater than or equal to the `/prefix-length` argument. It is the highest value of a range of the length (the “to” portion of the length range).

Default Configuration

No prefix list is created.

Command Mode

Global Configuration mode

User Guidelines

This command without the seq keyword adds the new entry after the last entry of the prefix list with the sequence number equals to the last number plus 5. For example, if the last configured sequence number is 43, the new entry will have the sequence number of 48. If the list is empty, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.

This command with the seq keyword puts the new entry into the place specified by the parameter, if an entry with the number exists it is replaced by the new one.

This command without the seq keyword removes the prefix list.

The no version of this command with the seq keyword removes the specified entry.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you might want to put the most common permits or denies near the top of the list, using the seq-number argument.

The show ipv6 prefix-list command displays the sequence numbers of entries. IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the le keyword.

A prefix length greater than, or equal to, a value is specified using the ge keyword. The ge and le keywords can be used to specify the range of the prefix length to be matched in more detail than the usual ipv6-prefix/prefix-length argument.

For a candidate prefix to match against a prefix list entry the following conditions must exist:

- The candidate prefix must match the specified prefix list and prefix length entry
- The value of the optional le keyword specifies the range of allowed prefix lengths from 0 up to the value of the le-length argument, and including, this value.
- The value of the optional ge keyword specifies the range of allowed prefix lengths from the value of the ge-length argument up to, and including, 128.

Note that the first condition must match before the other conditions take effect. An exact match is assumed when the ge or le keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The prefix-length value must be less than the ge value. The ge value must be less than, or equal to, the le value. The le value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have permit and deny condition statements, has an implicit deny any any statement as its last match condition.

Formal Specification

Checked prefix is cP and checked prefix length is cL .

Function $\text{PrefixIsEqual}(P1, P2, L)$ compares the first L bits of two addresses $P1$ and $P2$ and returns TRUE if they are equal.

Case 1. A prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is not defined
- le - is not defined

The prefix cP/cL matches the prefix-list entry if $\text{PrefixIsEqual}(cP, P, L) \ \&\& \ cL == L$ Case 2.

An prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is defined
- le - is not defined

The prefix cP/cL matches the prefix-list entry if $\text{PrefixIsEqual}(cP, P, L) \ \&\& \ cL \geq ge$

Case 3. An prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is not defined
- le - is defined

The prefix cP/cL matches to the prefix-list entry if $\text{PrefixIsEqual}(cP, P, L) \ \&\& \ cL \leq le$

Case 4. An prefix-list entry is:

- P - prefix address
- L - prefix length
- ge - is defined
- le - is defined

The prefix cP/cL matches the prefix-list entry if $\text{PrefixIsEqual}(cP, P, L) \ \&\& \ ge \leq cL \leq le$

Examples

Example 1. The following example denies all routes with a prefix of ::/0:

```
ZEQU0xxxxDL(config)# ipv6 prefix-list abc deny ::/0
```

Example 2. The following example permits the prefix 2002::/16:

```
ZEQU0xxxxDL(config)# ipv6 prefix-list abc permit 2002::/16
```

Example 3. The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64:

```
ZEQU0xxxxDL(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

Example 4. The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64:

```
ZEQU0xxxxDL(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

Example 5. The following example permits mask lengths from 32 to 64 bits in all address space:

```
ZEQU0xxxxDL(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

Example 6. The following example denies mask lengths greater than 32 bits in all address space:

```
ZEQU0xxxxDL(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

Example 7. The following example denies all routes with a prefix of 2002::/128:

```
ZEQU0xxxxDL (config)# ipv6 prefix-list abc deny 2002::/128
```

Example 8. The following example permits all routes with a prefix of ::/0:

```
ZEQU0xxxxDL (config)# ipv6 prefix-list abc permit ::/0
```

23.3 show ipv6 prefix-list

Use the show ipv6 prefix-list command in user EXEC or privileged EXEC mode. to display information about an IPv6 prefix list or IPv6 prefix list entries.

Syntax

```
show ipv6 prefix-list [detail [list-name] | summary [list-name]]
```

```
show ipv6 prefix-list list-name ipv6-prefix/prefix-length [longer | first-match]
```

```
show ipv6 prefix-list list-name seq seq-num
```

Parameters

- detail | summary—Displays detailed or summarized information about all IPv6 prefix lists.
- list-name—Name of a specific IPv6 prefix list.
- ipv6-prefix—All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.
- /prefix-length—Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
- longer—Displays all entries of an IPv6 prefix list that are more specific than the given ipv6-prefix/prefix-length values.
- first-match—Displays the entry of an IPv6 prefix list that matches the given ipv6-prefix/prefix-length values.
- seq seq-num—Sequence number of the IPv6 prefix list entry.

Command Mode User

EXEC mode Privileged

EXEC mode

User Guidelines

If the detail and summary keywords are omitted, the detail option is applied.

If the longer and first-match keywords are omitted, all entries of the specified prefix list that matches the given network/length are displayed.

Examples

Example 1. The following example shows the output of this command with the **detail** keyword:

```
ZEQU0xxxxDL# ipv6 prefix-list detail
ipv6 prefix-list abc
  count 8, range entries: 4
  seq: 5 drop ::/0 (hit count: 0)
  seq: 10 permit 2002::/16 (hit count: 0)
  seq: 15 permit 5f00::/48 le 64 (hit count: 0)
  seq: 20 permit 2001:db8::/64 le 128 (hit count: 0)
  seq: 25 permit ::/0 ge 32 le 64 (hit count: 0)
  seq: 30 drop ::/0 ge 32 (hit count: 0)
  seq: 35 drop 2002::/128 (hit count: 0)
  seq: 20 permit 2001:db8::/64 le 128 (hit count: 0)
  seq: 25 permit ::/0 ge 32 le 64 (hit count: 0)
  seq: 40 permit ::/0 (hit count: 0)
```

Field Descriptions

- **count**—Number of entries in the list.
- **range entries**—Number of entries with matching range.
- **seq**—Entry number in the list.
- **permit, deny**—Granting status.
- **description**—Comment.
- **hit count**—Number of matches for the prefix entry.

Example 2. The following example shows the output of the **show ipv6 prefix-list** command with the **summary** keyword:

```
ZEQU0xxxxDL# show ipv6 prefix-list summary
iipv6 prefix-list abc
  count 8, range entries: 4
```

Example 3. The following example shows the output of the **show ipv6 prefix-list** command with the **seq** keyword:

```
ZEQU0xxxxDL# show ipv6 prefix-list bgp-in seq 15
seq 15 deny ::/1 (hit count: 0)
```

24 Line Commands

24.1 exec-timeout

To set the session idle time interval, during which the system waits for user input before automatic logoff, use the `exec-timeout` Line Configuration mode command. To restore the default configuration, use the `no` form of this command.

Syntax

`exec-timeout minutes [seconds]`

`no exec-timeout`

Parameters

- `minutes`—Specifies the number of minutes. (Range: 0-65535)
- `seconds`—(Optional) Specifies the number of seconds. (Range: 0-59)

Default Configuration

The default idle time interval is 10 minutes.

Command Mode

Line Configuration Mode

Example

The following example sets the telnet session idle time interval before automatic logoff to 20 minutes and 10 seconds.

```
ZEQU0xxxxDL (config) # line telnet
ZEQU0xxxxDL (config-line) # exec-timeout 20 10
```

24.2 line

To identify a specific line for configuration and enter the Line Configuration command mode, use the line Global Configuration mode command.

Syntax

line {console | telnet | ssh}

Parameters

- console—Enters the terminal line mode.
- telnet—Configures the device as a virtual terminal for remote access (Telnet).
- ssh—Configures the device as a virtual terminal for secured remote access (SSH).

Command Mode

Global Configuration mode

Example

The following example configures the device as a virtual terminal for remote (Telnet) access.

```
ZEQU0xxxxDL (config)# line telnet
ZEQU0xxxxDL (config-line)#
```

24.3 speed

To set the line baud rate, use the speed command in Line Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

speed bps no

speed

Parameters

bps—Specifies the baud rate in bits per second (bps). Possible values are 9600, 19200, 38400, 57600, and 115200.

Default Configuration

The default speed is 9600 bps.

Command Mode

Line Configuration Mode

User Guidelines

The configured speed is only applied when autobaud is disabled. This configuration applies to the current session only.

Example

The following example configures the line baud rate as 9600 bits per second.

```
ZEQU0xxxxDL (config-line)# speed 9600
```

24.4 show line

To display line parameters, use the show line Privileged EXEC mode command.

Syntax

```
show line [console | telnet | ssh]
```

Parameters

- console—(Optional) Displays the console configuration.
- telnet—(Optional) Displays the Telnet configuration.
- ssh—(Optional) Displays the SSH configuration.

Default Configuration

If the line is not specified, all line configuration parameters are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the line configuration.

```
ZEQU0xxxxDL# show line
Console configuration:
Interactive timeout: 10 minute(s)
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1

Telnet configuration:
Telnet is enabled.
Interactive timeout: 10 minute(s)
History: 10

SSH configuration:
Interactive timeout: 10 minute(s)
History: 10
```

25 Link Aggregation Control Protocol (LACP)

Commands

25.1 lacp port-priority

To set the physical port priority, use the lacp port-priority Interface (Ethernet) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

lacp port-priority value

no lacp port-priority

Parameters

value—Specifies the port priority. (Range: 1–65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example sets the priority of gi1/0/6.

```
ZEQU0xxxxDL(config)# interface gi1/0/6
ZEQU0xxxxDL(config-if)# lacp port-priority 247
```

25.2 lacp system-priority

To set the system priority, use the lacp system-priority Global Configuration mode command.
To restore the default configuration, use the no form of this command.

Syntax

lacp system-priority value

no lacp system-priority

Parameters

value—Specifies the system priority value. (Range: 1–65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

Example

The following example sets the system priority to 120.

```
ZEQU0xxxxDL (config) # lacp system-priority 120
```

25.3 lacp timeout

To assign an administrative LACP timeout to an interface, use the lacp timeout Interface (Ethernet) Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

lacp timeout {long | short}

no lacp timeout

Parameters

- long—Specifies the long timeout value.
- short—Specifies the short timeout value.

Default Configuration

The default port timeout value is Long.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example assigns a long administrative LACP timeout to gi1/0/6.

```
ZEQU0xxxxDL (config)# interface gi1/0/6  
ZEQU0xxxxDL (config-if)# lacp timeout long
```

25.4 show lacp

To display LACP information for all Ethernet ports or for a specific Ethernet port, use the show lacp Privileged EXEC mode command.

Syntax

show lacp interface-id [parameters | statistics | protocol-state]

Parameters

- interface-id—Specify an interface ID. The interface ID must be an Ethernet port
- parameters—(Optional) Displays parameters only.
- statistics—(Optional) Displays statistics only.
- protocol-state—(Optional) Displays protocol state only.

Command Mode

Privileged EXEC mode

Example

The following example displays LACP information for gi1/0/1.

```
ZEQU0xxxxDL# show lacp GigabitEthernet1/0/1
gi1/0/1 LACP parameters:
  Actor
    system priority:      1
    system mac addr:     00:50:40:3b:c4:4d
    port Admin key:      1000
    port Oper key:       1000
    port Oper number:    1
    port Admin priority: 1
    port Oper priority:  1
    port Admin timeout:  LONG
    port Oper timeout:   LONG
    LACP Activity:      ACTIVE
    Aggregation:        AGGREGATABLE
    synchronization:    TRUE
    collecting:          TRUE
    distributing:       TRUE
    expired:             FALSE
  Partner
    system priority:      1
    system mac addr:     00:50:40:3b:bb:77
    port Admin key:      0
    port Oper key:       1000
    port Oper number:    1
    port Admin priority: 0
    port Oper priority:  1
    port Oper timeout:   LONG
```

```

LACP Activity: ACTIVE
Aggregation: AGGREGATABLE
dynchronization: TRUE
collecting: TRUE
distributing: TRU
expired: FALSE
gi1/0/1 LACP statistics:
  LACP Pdus sent: 32
  LACP Pdus received: 27
gi1/0/1 LACP Protocol State:
  LACP State Machines:
    Receive FSM: Current State
    Mux FSM: Collecting Distributing State
    Periodic Tx FSM: Slow Periodic Stat
  Control Variables:
    BEGIN: FALSE
    LACP_Enabled: TRUE
    Ready_N: FALSE
    Selected: SELECTED
    Port_moved: FALSE
    NNT: FALSE
    Port_enabled: TRUE
  Timer counters:
    periodic tx timer: 3
    current while timer: 63
    wait while timer: 0
Port gi1/0/1 LACP Statistics:
  LACP PDUs sent: 2
  LACP PDUs received: 2
Port gi1/0/1 LACP Protocol State:
  LACP State Machines:
    Receive FSM: Port Disabled State
    Mux FSM: Detached State
  Control Variables:
    BEGIN: FALSE
    LACP_Enabled: TRUE
    Ready_N: FALSE
    Selected: UNSELECTED
    Port_moved: FALSE
    NNT: FALSE
    Port_enabled: FALSE
  Timer counters:
    periodic tx timer: 0
    current while timer: 0
    wait while timer: 0

```

25.5 show lacp port-channel

To display LACP information for a port-channel, use the `show lacp port-channel` Privileged EXEC mode command.

Syntax

```
show lacp port-channel [port_channel_number]
```

Parameters

`port_channel_number`—(Optional) Specifies the port-channel number.

Command Mode

Privileged EXEC mode

Example

The following example displays LACP information about port-channel 1.

```
ZEQU0xxxxDL# show lacp port-channel 1
Port-Channel Po1
  Port Type Gigabit Ethernet
  Attached Lag id:
  Actor
    System Priority: 1
    MAC Address:    00:50:40:3b:c4:4d
    Admin Key:      1000
    Oper Key:       1000
  Partner
    System Priority: 1
    MAC Address:    00:50:40:3b:bb:77
    Oper Key:       1000
```

26 Loopback Detection Protocol Commands

26.1 line loopback enable (Global)

To enable the Loopback Detection (LBD) feature globally, use the line loopback enable Global Configuration mode command. To disable the Loopback Detection feature, use the no form of this command

.

Syntax

line loopback enable

no line loopback enable

Parameters

N/A

Default Configuration

Loopback Detection is enabled.

Command Mode

Privileged EXEC mode

Global Configuration mode

This command enables the Loopback Detection feature globally. Use the line loopback enable Interface Configuration mode command to enable Loopback Detection on an interface.

Example

The following example enables the Loopback Detection feature on the device.

```
ZEQU0xxxxDL# line loopback enable
```

26.2 line loopback enable (Interface)

To enable the Loopback Detection (LBD) feature on an interface, use the line loopback Interface Configuration mode command. To disable the Loopback Detection feature on the interface, use the no form of this command.

Syntax

line loopback

no line loopback

Parameters

N/A

Default Configuration

ZEQUO 5410DL

Port 1-4 :Enable

Port 5-16 :Disable

ZEQUO 4500DL

Port 1-24 :Enable

Port 25-28 :Disable

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

This command enables Loopback Detection on an interface. Use the line loopback enable Global Configuration command to enable Loopback Detection globally.

Example

The following example enables the Loopback Detection feature on port gi1/0/1:

```
ZEQUOxxxxDL (config)# interface gi1/0/1
ZEQUOxxxxDL (config-if)# line loopback
```

26.3 line loopback mode

Sets interface working mode if loop will be detected. If shutdown mode is activated then port will be suspended.

Syntax

line loopback mode [shutdown | block]

Parameters

- shutdown — The port is shutdown.
- block — The port is block.

Default Configuration

Block mode is default

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to change loop detect behavior.

Example

The following example sets shutdown mode for gi1/0/1:

```
ZEQU0xxxxDL (config)# interface gi1/0/1
ZEQU0xxxxDL (config-if)# line loopback mode shutdown
```

26.4 line loopback recovery

Sets recovery time for interface. To restore the default configuration, use the no form of this command.

Syntax

l line loopback recovery recoverytime

no line loopback recovery

Parameters

- recoverytime — Recovery time. The unit is seconds. (Range: 60-86400)

Default Configuration

60 secondst

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Use this command to tune or disable recovery mechanism.

Example

The following example disables recovery mechanism for interface gi1/0/1:

```
ZEQU0xxxxDL (config)# interface gi1/0/1
ZEQU0xxxxDL (config-if)# no line loopback recovery
```

26.5 show line loopback configuration

To display information about Loopback Detection status and configuration.

Syntax

show line loopback configuration

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to display all Loopback Detection settings.

Example

The following example displays information about the status of Loopback Detection:

ZEQU0xxxxDL# show line loopback configuration							
Global Loop Detection Status: Enabled							
Port	Link	State	Loop Detect	Mode	Recovery	Recovery Time	
-----	-----	-----	-----	-----	-----	-----	
gi1/0/1	down	forwarding	enabled	block	enabled	60	
gi1/0/2	down	forwarding	enabled	block	enabled	60	
			.				
			.				
te1/0/27	down	forwarding	enabled	block	enabled	60	
te1/0/28	down	forwarding	enabled	block	enabled	60	
Po1	down	forwarding	enabled	block	enabled	60	
Po2	down	forwarding	enabled	block	enabled	60	
			.				
			.				
Po31	down	forwarding	enabled	block	enabled	60	
Po32	down	forwarding	enabled	block	enabled	60	

26.6 show line loopback history

To display the log messages for Loopback Detection stored in the internal buffer, use the show line loopback history Privileged EXEC mode command.

Syntax

show line loopback history

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to view the log messages for Loopback Detection in the internal buffer.

Example

The following example displays the log messages for Loopback Detection stored in the internal buffer :

ZEU0xxxxDL(config)# show line loopback history		
Entry Time(YYYY/MM/DD HH:MM:SS) Event		
1	2017/01/29 13:23:10	gi1/0/23 auto recovery.
2	2017/01/29 13:22:05	loop detected on gi1/0/23
3	2017/01/29 13:21:11	loop detected between gi1/0/17 and gi1/0/18.
4	2017/01/29 13:21:11	loop detected between gi1/0/18 and gi1/0/17.

26.7 clear line loopback history

To clear the log messages for Loopback Detection stored in the internal buffer, use the clear line loopback history Privileged EXEC mode command.

Syntax

clear line loopback history

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to clear the log messages for Loopback Detection in the internal buffer.

Example

The following example clears the log messages for Loopback Detection stored in the internal buffer :

```
ZEQU0xxxxDL(config)# clear line loopback history
Clear Loopback Detection Logging Buffer ? (Y/N) [N] Y
```

27 Management ACL Commands

27.1 deny (Management)

To set permit rule (ACE) for the management access list (ACL), use the deny Management Access-list Configuration mode command.

Syntax

deny [interface-id] [service service]

deny ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]

Parameters

- interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- service service—(Optional) Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- ipv4-address—Specifies the source IPv4 address.
- ipv6-address/ipv6-prefix-length—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- mask mask—Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- mask prefix-length—Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example denies all ports in the ACL called mlist.

```
ZEQU0xxxxDL(config)# management access-list mlist  
ZEQU0xxxxDL(config-macl)# deny
```

27.2 permit (Management)

To set permit rule (ACE) for the management access list (ACL), use the permit Management Access-list Configuration mode command.

Syntax

`permit [interface-id] [service service]`

`permit ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]`

Parameters

- `interface-id` — (Optional) Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- `service service` — (Optional) Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- `ipv4-address` — Specifies the source IPv4 address.
- `ipv6-address/ipv6-prefix-length` — Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- `mask mask` — Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.
- `mask prefix-length` — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with Ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example permits all ports in the ACL called mlist.

```
ZEQU0xxxxDL (config) # management access-list mlist
ZEQU0xxxxDL (config-macl) # permit
```

27.3 management access-list

To configure a management access list (ACL) and enter the Management Access-list Configuration mode, use the management access-list Global Configuration mode command. To delete an ACL, use the no form of this command.

Syntax

management access-list name

no management access-list name

Parameters

- name — Specifies the ACL name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management access list. This command enters the Management Access-list Configuration mode, where the denied or permitted access conditions are defined with the deny and permit commands.

If no match criteria are defined, the default value is deny.

When re-entering the access-list context, the new rules are entered at the end of the access list.

Use the management access-class command to select the active access list. The active management list cannot be updated or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with the service field are ignored), and then again on the inner IPv6 header.

Examples

Example 1 - The following example creates a management access list called mlist, configures management gi1/0/1 and gi1/0/9, and makes the new access list the active list.

```
ZEQU0xxxxDL (config)# management access-list mlist  
ZEQU0xxxxDL (config-macl)# permit gi1/0/1  
ZEQU0xxxxDL (config-macl)# permit gi1/0/9  
ZEQU0xxxxDL (config-macl)# exit  
ZEQU0xxxxDL (config)#
```

Example 2 - The following example creates a management access list called 'mlist', configures all interfaces to be management interfaces except gi1/0/1 and gi1/0/9, and makes the new access list the active list.

```
ZEQU0xxxxDL (config)# management access-list mlist  
ZEQU0xxxxDL (config-macl)# deny gi1/0/1  
ZEQU0xxxxDL (config-macl)# deny gi1/0/9  
ZEQU0xxxxDL (config-macl)# permit  
ZEQU0xxxxDL (config-macl)# exit  
ZEQU0xxxxDL (config)#
```

27.4 management access-class

To restrict management connections by defining the active management access list (ACL), use the management access-class Global Configuration mode command. To disable management connection restrictions, use the no form of this command.

Syntax

```
management access-class {console-only | name}
```

```
no management access-class
```

Parameters

- console-only—Specifies that the device can be managed only from the console.
- name—Specifies the ACL name to be used. (Length: 1–32 characters)

Default Configuration

The default configuration is no management connection restrictions.

Command Mode

Global Configuration mode

Example

The following example defines an access list called mlist as the active management access list.

```
ZEQU0xxxxDL(config)# management access-class mlist
```

27.5 show management access-list

To display management access list (ACL), use the show management access-list Privileged EXEC mode command.

Syntax

```
show management access-list [name]
```

Parameters

name—(Optional) Specifies the name of a management access list to be displayed.
(Length: 1–32 characters)

Default Configuration

All management ACLs are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the mlist management ACL.

```
ZEQU0xxxxDL# show management access-list mlist
ml
--
deny service telnet
permit gi1/0/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

27.6 show management access-class

To display information about the active management access list (ACL), use the show management access-class Privileged EXEC mode command.

Syntax

```
show management access-class
```

Parameters

N/A.

Command Mode

Privileged EXEC mode

Example

The following example displays the active management ACL information.

```
ZEQU0xxxxDL# show management access-class  
Management access-class is enabled, using access list mlist
```

28 MLD Commands

28.1 clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the `clear ipv6 mld counters` command in Privileged EXEC mode.

Syntax

`clear ipv6 mld counters [interface-id]`

Parameters

- `interface-id`—(Optional) Interface Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `clear ipv6 mld counters` command to clear the MLD counters, which keep track of the number of joins and leaves received. If you omit the optional `interface-id` argument, the `clear ipv6 mld counters` command clears the counters on all interfaces.

Example

The following example clears the counters for VLAN 100:

```
ZEQU0xxxxDL# clear ipv6 mld counters vlan 100
```

28.2 ipv6 mld last-member-query-count

To configure the Multicast Listener Discovery (MLD) last member query counter, use the `ipv6 mld last-member-query-count` command in Interface Configuration mode. To restore the default value, use the `no` form of this command.

Syntax

`ipv6 mld last-member-query-count count`

`no ipv6 mld last-member-query-count`

Parameters

`count`—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default Configuration

A value of MLD Robustness variable.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the `ipv6 mld robustness` command to change the MLD last member query counter.

Example

The following example changes a value of the MLD last member query counter to 3:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config)# ipv6 mld last-member-query-count 3
```

28.3 ipv6 mld snooping last-member-queryinterval

To configure the Multicast Listener Discovery (MLD) last member query interval, use the `ipv6 mld snooping last-member-query-interval` command in Interface Configuration mode. To restore the default MLD query interval, use the `no` form of this command.

Syntax

`ipv6 mld snooping last-member-query-interval milliseconds`

`no ipv6 mld snooping last-member-query-interval`

Parameters

- `milliseconds`—Interval, in milliseconds, at which MLD group-specific host query messages are sent on the interface. (Range: 100–25500).

Default Configuration

The default MLD last member query interval is 1000 milliseconds.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the `ipv6 mld last-member-query-interval` command to configure the MLD last member query interval on an interface.

Example

The following example shows how to increase the MLD last member query interval to 1500 milliseconds:

```
ZEQU0xxxxDL (config) # interface vlan 100
ZEQU0xxxxDL (config-if) # ipv6 mld snooping last-member-query-interval 1500
ZEQU0xxxxDL (config-if) # exit
```

28.4 ipv6 mld snooping query-interval

To configure the frequency at which the switch sends Multicast Listener Discovery (MLD) host-query messages, use the `ipv6 mld snooping query-interval` command in Interface Configuration mode. To return to the default frequency, use the `no` form of this command.

Syntax

`ipv6 mld snooping query-interval seconds`

`no ipv6 mld snooping query-interval`

Parameters

- `seconds`—Frequency, in seconds, at which the switch sends MLD query messages from the interface. The range is from 30 to 18000.

Default Configuration

The default MLD query interval is 125 seconds.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the `ipv6 mld snooping query-interval` command to configure the frequency at which the MLD querier sends MLD host-query messages from an interface. The MLD querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

The query interval must be bigger than the maximum query response time.

Example

The following example shows how to increase the frequency at which the MLD querier sends MLD host-query messages to 180 seconds:

```
ZEQU0xxxxDL (config) # interface vlan 100
ZEQU0xxxxDL (config-if) # ipv6 mld snooping query-interval 180
ZEQU0xxxxDL (config-if) # exit
```

28.5 ipv6 mld snooping query-max-response-time

To configure the maximum response time advertised in Multicast Listener Discovery (MLD) queries, use the `ipv6 mld snooping query-max-response-time` command in Interface Configuration mode. To restore the default value, use the `no` form of this command.

Syntax

`ipv6 mld snooping query-max-response-time seconds`

`no ipv6 mld snooping query-max-response-time`

Parameters

- `seconds`—Maximum response time, in seconds, advertised in MLD queries. (Range: 5–20)

Default Configuration

10 seconds.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

This command controls the period during which the responder can respond to an MLD query message before the router deletes the group.

This command controls how much time the hosts have to answer an MLD query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

The maximum query response time must be less than the query interval.

Note. If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Example

The following example configures a maximum response time of 8 seconds:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ipv6 mld snooping query-max-response-time 8
ZEQU0xxxxDL(config-if)# exit
```

28.6 ipv6 mld robustness-variable

To configure the Multicast Listener Discovery (MLD) robustness variable, use the `ipv6 mld snooping robustness-variable` command in Interface Configuration mode. To restore the default value, use the `no` form of this command.

Syntax

`ipv6 mld snooping robustness-variable count`

`no ipv6 mld snooping robustness-variable`

Parameters

- `count`—The number of expected packet loss on a link. Parameter range. (Range: 1–7).

Default Configuration

The default value is 2.

Command Mode

Interface Configuration mode

User Guidelines

Use the `ipv6 mld snooping robustness -variable` command to change the MLD robustness variable.

Example

The following example changes a value of the MLD robustness variable to 3:

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ipv6 mld snooping robustness -variable 3
ZEQU0xxxxDL(config-if)# exit
```

28.7 ipv6 mld version

To configure which version of Multicast Listener Discovery Protocol (MLD) the router uses, use the `ipv6 mld version` command in Interface Configuration mode. To restore the default value, use the `no` form of this command.

Syntax

`ipv6 mld version {1 | 2}`

`no ipv6 mld version`

Parameters

- 1—MLD Version 1.
- 2—MLD Version 2.

Default Configuration

MLD Version 1.

Command Mode

Interface Configuration mode

User Guidelines

Use the command to change the default version of MLD.

Example

The following example configures the router to use MLD Version 1:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ipv6 mld version 1
ZEQU0xxxxDL(config-if)# exit
```

28.8 show ipv6 mld snooping counters

To display the Multicast Listener Discovery (MLD) traffic counters, use the `show ipv6 mld snooping counters` command in User EXEC mode.

Syntax

```
show ipv6 mld snooping counters [interface-id]
```

Parameters

- `interface-id`—(Optional) Interface Identifier.

Command Mode

User EXEC mode

User Guidelines

Use the `show ipv6 mld snooping counters` command to check if the expected number of MLD protocol messages have been received and sent.

If you omit the optional `interface-id` argument, the `show ipv6 mld snooping counters` command displays counters of all interfaces.

Example

The following example displays the MLD protocol messages received and sent:

```
ZEQU0xxxxDL# show ipv6 mld snooping counters vlan 100
VLAN 100
  Elapsed time since counters cleared:00:00:21
  Failed received Joins: 0
  Total MLDv1 received messages: 10
  Total MLDv2 received messages: 0
  Total invalid received messages: 0
  General Sent Queries: 0
  Specific Sent Queries: 0
```

28.9 show ipv6 mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the `show ipv6 mld groups` command in User EXEC mode.

Syntax

```
show ipv6 mld groups [link-local | group-name | group-address | interface-id] [detail]
```

Parameters

- `link-local`—(Optional) Displays the link-local groups.
- `group-name | group-address`—(Optional) IPv6 address or name of the multicast group.
- `interface-id`—(Optional) Interface identifier.
- `detail`—(Optional) Displays detailed information about individual sources.

Command Mode

User EXEC mode

User Guidelines

Use the `show ipv6 mld groups [detail]` command to display all directly connected groups.

Use the `show ipv6 mld groups link-local [detail]` command to display all directly connected link-local groups.

Use the `show ipv6 mld groups [group-name | group-address] [detail]` command to display one given directly connected group.

Use the `show ipv6 mld groups interface-id [detail]` command to display all groups directly connected to the given interface.

Examples

Example 1. The following is sample output from the show ipv6 mld groups command. It shows all of the groups joined by VLAN 100:

```
ZEQU0xxxxDL# show ipv6 mld groups vlan 100
MLD Connected Group Membership
Expires: never - switch itself has joined the group
Group Address          Interface  Expires
FF02::2                VLAN 100   never
FF02::1:FF00:1         VLAN      00:10:27
FF02::1:FFAF:2C39      VLAN 100   00:09:11
FF06:7777::1          VLAN 100   00:00:26
```

Example 2. The following is sample output from the show ipv6 mld groups command using the detail keyword:

```
ZEQU0xxxxDL# show ipv6 mld groups detail
Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state
Interface: VLAN 100
Group: FF33::1:1:1
Router mode: INCLUDE
Last reporter:
2009:5::12:1
Group Timer Expires: 00:20:11
Group source list:
Source Address          Expires
2004:4::6               00:00:11
2004:4::16              00:08:11
Group: FF33::1:1:2
Router mode: EXCLUDE
Last reporter: 2008:5::2A:10
Group Timer Expires: 00:20:11
Exclude Mode Expiry (Filter) Timer: 00:10:11
Group source list:
Source Address          Expires
2004:5::1               00:04:08
2004:3::1               00:04:08
2004:7::10              00:00:00
2004:50::1              00:00:00
```

28.10 **show ipv6 mld groups summary**

To display the number of (*, G) and (S, G) membership reports present in the Multicast Listener Discovery (MLD) cache, use the `show ipv6 mld groups summary` command in User EXEC mode.

Syntax

```
show ipv6 mld groups summary
```

Parameters

N/A.

Command Mode

User EXEC mode

User Guidelines

The `show ipv6 mld groups summary` command displays the number of directly connected multicast groups (including link-local groups).

Example

The following is sample output from the `show ipv6 mld groups summary` command:

```
ZEQU0xxxxDL# show ipv6 mld groups summary
```

```
MLD Route Summary
```

```
No. of (*, G) routes = 5
```

```
No. of (S, G) routes = 0
```

Field Descriptions:

No. of (*, G) routes = 5—Displays the number of groups present in the MLD cache.

No. of (S, G) routes = 0—Displays the number of include and exclude mode sources present in the MLD cache.

28.11 show ipv6 mld interface

To display multicast-related information about an interface, use the `show ipv6 mld interface` command in User EXEC mode.

Syntax

```
show ipv6 mld interface [interface-id]
```

Parameters

- `interface-id`—Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If you omit the optional `interface-id` argument, the `show ipv6 mld interface` command displays information about all interfaces.

Example

The following is sample output from the `show ipv6 mld interface` command for Ethernet interface VLAN 100:

```
ZEQU0xxxxDL# show ipv6 mld interface vlan 100
VLAN 100 is up
Administrative MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
Operational MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
Current MLD version is 3
Administrative MLD robustness variable is 2 seconds
Operational MLD robustness variable is 2 seconds
Administrative MLD query interval is 125 seconds
Operational MLD query interval is 125 seconds
Administrative MLD max query response time is 10
seconds Operational MLD max query response time is
10 seconds
Administrative Last member query response interval is 1000 milliseconds
Operational Last member query response interval is 1000 milliseconds
```

29 MLD Proxy Commands

29.1 ipv6 mld-proxy

To add downstream interfaces to a MLD proxy tree, use the `ip mld-proxy` command in Interface Configuration mode. To remove downstream from interfaces to a MLD proxy tree, use the `no` form of this command.

Syntax

`ipv6 mld-proxy upstream-interface-id`

`no ipv6 mld-proxy`

Parameters

- `upstream-interface-id`—Upstream Interface identifier.

Default Configuration

The protocol is disabled on the interface.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the `ipv6 mld-proxy` command to add a downstream interface to a MLD proxy tree. If the proxy tree does not exist it is created.

Use the `no` format of the command to remove the downstream interface. When the last downstream interface is removed from the proxy tree it is deleted too.

Examples

Example 1. The following example adds a downstream interface to a MLD Proxy process with `vlan 200` as its Upstream interface:

```
ZEQU0xxxxDL(config)# interface vlan 100
ZEQU0xxxxDL(config-if)# ipv6 mld-proxy vlan 200
ZEQU0xxxxDL(config-if)# exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
ZEQU0xxxxDL (config)# interface range vlan 100-105
ZEQU0xxxxDL (config-if)# ipv6 mld-proxy vlan 200
ZEQU0xxxxDL (config-if)# exit
```

29.2 ipv6 mld proxy downstream protected

To disable forwarding of IPv6 Multicast traffic from downstream interfaces, use the `ipv6 mldproxy downstream protected` command in Global Configuration mode. To allow forwarding from downstream interfaces, use the `no` form of this command.

Syntax

`ipv6 mld proxy downstream protected`

`no ipv6 mld proxy downstream protected`

Parameters

N/A.

Default Configuration

Forwarding from downstream interfaces is allowed.

Command Mode

Global Configuration mode

User Guidelines

Use the `pv6 mld proxy downstream protected` command to block forwarding from downstream interfaces.

Example

The following example prohibits forwarding from downstream interfaces:

```
ZEQU0xxxxDL(config)# ipv6 mld proxy downstream protected
```

29.3 ipv6 mld-proxy downstream protected interface

To disable or enable forwarding of IPv6 Multicast traffic from a given downstream interface, use the `ipv6 mld-proxy downstream protected interface` command in Interface Configuration mode. To return to default, use the `no` form of this command.

Syntax

`ipv6 mld-proxy downstream protected interface {enabled | disabled}`

`no ipv6 mld-proxy downstream protected interface`

Parameters

- **enabled**—Downstream interface protection on the interface is enabled. IPv6 Multicast traffic arriving on the interface will not be forwarded.
- **disabled**—Downstream interface protection on the interface is disabled. IPv6 Multicast traffic arriving on the interface will be forwarded.

Default Configuration

Global downstream protection configuration (see the `ipv6 mld-proxy downstream protected` command)

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the `ipv6 mld-proxy downstream protected interface disabled` command to block forwarding from the given downstream interface.

Use the `ipv6 mld-proxy downstream protected interface enabled` command to allow forwarding from the given downstream interface.

The command can be configured only for a downstream interface. When a downstream interface is removed from the MLD Proxy tree the configuration is removed too.

Example

The following example prohibits forwarding from downstream interface `vlan 100`:

```
ZEQU0xxxxDL (config) # interface vlan100
ZEQU0xxxxDL (config-if) # ipv6 mld-proxy downstream protected interface enabled
ZEQU0xxxxDL (config-if) # exit
```

29.4 ipv6 mld-proxy ssm

To define the Source Specific Multicast (SSM) range of IP Multicast addresses, use the `ipv6 mld-proxy ssm` command in Global Configuration mode. To disable the SSM range, use the `no` form of this command.

Syntax

```
ipv6 mld-proxy ssm {default | range access-list}
```

```
no ipv6 mld-proxy ssm
```

Parameters

`default`—Defines the SSM range access list to FF3x::/32 (see RFC4607).

`range access-list`—Specifies the standard IPv6 access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global Configuration mode

User Guidelines

A new `ipv6 mld-proxy ssm` command overrides the previous `ipv6 mld-proxy ssm` command. Use the `no ipv6 mld-proxy ssm` command to remove all defined ranges.

Example

The following example shows how to configure SSM service for the default IPv6 address range and the IPv6 address ranges defined by access lists `list1`:

```
ZEQU0xxxxDL(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB8::/64
ZEQU0xxxxDL(config)# ipv6 access-list list1 deny FF7E:1220:2001:DB1::1
ZEQU0xxxxDL(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB1::/64
ZEQU0xxxxDL(config)# ipv6 pim mld-proxy range list1
```

29.5 show ipv6 mldproxy interface

To display information about interfaces configured for MLD Proxy, use the `show ipv6 mldproxy interface` command in User EXEC mode or Privileged EXEC mode.

Syntax

```
show ipv6 mldproxy interface [interface-id]
```

Parameters

- `interface-id`—(Optional) Display MLD Proxy information about the interface.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

The `show ipv6 mld-proxy interface` command is used to display all interfaces where the MLD Proxy is enabled or to display the MLD Proxy configuration for a given interface.

Examples

Example 1. The following example displays MLD Proxy status on all interfaces where the MLD Proxy is enabled:

```
ZEQU0xxxxDL# show ip mld proxy interface
```

* - the switch is the Querier on the interface

IPv6 Forwarding is enabled

IPv6 Multicast Routing is enabled

MLD Proxy is enabled

Global Downstream interfaces protection is disabled

SSM Access List Name: list1

Interface Type Discarding IPv6 Multicast

vlan 100 upstream

*vlan 102 downstream enabled

*vlan 110 downstream default

vlan 113 downstream disabled

Example 2. The following is sample output from the show ipv6 mld-proxy interface command for given upstream interface:

```
ZEQU0xxxxDL# show ipv6 mldproxy interface vlan 100
```

* - the switch is the Querier on the interface

```
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downstream interfaces protection is disabled
SSM Access List Name:
vlan 100 is a Upstream interface
Downstream interfaces:
*vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the show ipv6 mld-proxy interface command for given downstream interface:

```
ZEQU0xxxxDL# show ipv6 mldproxy interface vlan 102
```

```
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downstream interfaces protection is disabled
SSM Access List Name: default
vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Upstream interface: vlan 100
```

Example 4. The following is sample output from the show ipv6 mld-proxy interface command for an interface on which IGMP Proxy is disabled:

```
ZEQU0xxxxDL# show ipv6 mldproxy interface vlan 1
```

```
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is disabled
```

30 MLD Snooping Commands

30.1 ipv6 mld snooping (Global)

To enable IPv6 Multicast Listener Discovery (MLD) snooping, use the `ipv6 mld snooping` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ipv6 mld snooping`

`no ipv6 mld snooping`

Parameters

N/A

Default Configuration

IPv6 MLD snooping is disabled.

Command Mode

Global Configuration mode

Example

The following example enables IPv6 MLD snooping.

```
ZEQU0xxxxDL (config) # ipv6 mld snooping
```

30.2 ipv6 mld snooping vlan

To enable MLD snooping on a specific VLAN, use the `ipv6 mld snooping vlan` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ipv6 mld snooping vlan vlan-id`

`no ipv6 mld snooping vlan vlan-id`

Parameters

- `vlan-id`—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

MLD snooping can only be enabled on static VLANs.

MLDv1 and MLDv2 are supported.

To activate MLD snooping, bridge multicast filtering must be enabled by the bridge multicast filtering command.

The user guidelines of the bridge multicast mode command describe the configuration that can be written into the FDB as a function of the FDB mode, and the MLD version that is used in the network.

Example

```
ZEQU0xxxxDL(config)# ipv6 mld snooping vlan 2
```

30.3 ipv6 mld snooping querier

To enable globally the MLD Snooping querier, use the `ipv6 mld snooping querier` command in Global Configuration mode. To disable the MLD Snooping querier globally, use the `no` form of this command.

Syntax

`ipv6 mld snooping querier`

`no ipv6 mld snooping querier`

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

To run the MLD Snooping querier on a VLAN, you have enable it globally and on the VLAN.

Example

The following example disables the MLD Snooping querier globally:

```
ZEQU0xxxxDL (config)# no ipv6 mld snooping querier
```

30.4 ipv6 mld snooping vlan querier

To enable the Internet MLD Snooping querier on a specific VLAN, use the `ipv6 mld snooping vlan querier` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ipv6 mld snooping vlan vlan-id querier`

`no ipv6 mld snooping vlan vlan-id querier`

Parameters

- `vlan-id`—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The MLD Snooping querier can be enabled on a VLAN only if MLD Snooping is enabled for that VLAN.

Example

The following example enables the MLD Snooping querier on VLAN 1:

```
ZEQU0xxxxDL (config)# ipv6 mld snooping vlan 1 querier
```

30.5 ipv6 mld snooping vlan querier election

To enable MLD Querier election mechanism of an MLD Snooping querier on a specific VLAN, use the `ipv6 mld snooping vlan querier election` command in Global Configuration mode. To disable Querier election mechanism, use the `no` form of this command.

Syntax

`ipv6 mld snooping vlan vlan-id querier election`

`no ipv6 mld snooping vlan vlan-id querier election`

Parameters

- `vlan-id`—Specifies the VLAN.

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

Use the `no` form of the `ipv6 mld snooping vlan querier election` command to disable MLD Querier election mechanism on a VLAN.

If the MLD Querier election mechanism is enabled, the MLD Snooping querier supports the standard MLD Querier election mechanism specified in RFC2710 and RFC3810.

If MLD Querier election mechanism is disabled, MLD Snooping Querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an IGMP query from another Querier - it starts sending General Query messages. Once the switch acts as a Querier, it will stop sending General Query messages if it detects another Querier on the VLAN. In this case, the switch will resume sending General Query messages if it does hear another Querier for Query Passive interval that equals to $\text{<Robustness>*<Query Interval> + 0.5*<Query Response Interval>}$. See the `ipv6 mld robustness`, `ipv6 mld query-interval`, and `ipv6 mld query-max-response-time` commands for configurations of these parameters.

It is recommended to disable MLD Querier election mechanism if there is an IPMv6 Multicast router on the VLAN.

Example

The following example disables MLD Snooping Querier election on VLAN 1:

```
ZEQU0xxxxDL (config)# no ipv6 mld snooping vlan 1 querier election
```

30.6 ipv6 mld snooping vlan querier version

To configure the IGMP version of an IGMP querier on a specific VLAN, use the `ipv6 mld snooping vlan querier version` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ipv6 mld snooping vlan vlan-id querier version {1 | 2}`

`no ipv6 mld snooping vlan vlan-id querier version`

Parameters

- `vlan-id`—Specifies the VLAN.
- `querier version {1 | 2}`—Specifies the MLD version.

Default Configuration

MLDv1.

Command Mode

Global Configuration mode

Example

The following example sets the version of the MLD Snooping Querier VLAN 1 to 2:

```
ZEQU0xxxxDL (config)# ipv6 mld snooping vlan 1 querier version 2
```

30.7 ipv6 mld snooping vlan mrouter

To enable automatic learning of Multicast router ports, use the `ipv6 mld snooping vlan mrouter` command in Global Configuration mode. To remove the configuration, use the no form of this command.

Syntax

```
ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp
```

```
no ipv6 mld snooping vlan vlan-id mrouter learn pim-dvmrp
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `pim-dvmrp`—Learn Multicast router port by PIM, DVMRP and MLD messages.

Default Configuration

Learning `pim-dvmrp` is enabled.

Command Mode

Global Configuration mode

User Guidelines

Multicast router ports can be configured statically with the `bridge multicast forward-all` command.

You can execute the command before the VLAN is created.

Example

```
ZEQU0xxxxDL (config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

30.8 ipv6 mld snooping vlan mrouter interface

To define a port that is connected to a Multicast router port, use the `ipv6 mld snooping mrouter interface` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ipv6 mld snooping vlan vlan-id mrouter interface interface-list
```

```
no ipv6 mld snooping vlan vlan-id mrouter interface interface-list
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies a list of interfaces. The interfaces can be from one of the following types: port or port-channel.

Default Configuration

No ports defined

Command Mode

Global Configuration mode

User Guidelines

This command may be used in conjunction with the `bridge multicast forward-all` command, which is used in older versions to statically configure a port as a Multicast router.

A port that is defined as a Multicast router port receives all MLD packets (reports and queries) as well as all Multicast data.

You can execute the command before the VLAN is created and for a range of ports as shown in the example.

Example

```
ZEQU0xxxxDL(config)# interface gi1/0/1
```

```
ZEQU0xxxxDL(config-if)# ipv6 mld snooping vlan 1 mrouter interface gi1/0/1-4
```

30.9 ipv6 mld snooping vlan forbidden mrouter

To forbid a port from being defined as a Multicast router port by static configuration or by automatic learning, use the `ipv6 mld snooping vlan forbidden mrouter` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list`

`no ipv6 mld snooping vlan vlan-id forbidden mrouter interface interface-list`

Parameters

- `vlan-id`—Specifies the VLAN.
- `interface-list`—Specifies list of interfaces. The interfaces can be of one of the following types: Ethernet port or Port-channel.

Default Configuration

No forbidden ports by default

Command Mode

Global Configuration mode

User Guidelines

A port that is forbidden to be defined as a Multicast router port (mrouter port) cannot be learned dynamically or assigned statically.

The `bridge multicast forward-all` command was used in older versions to forbid dynamic learning of Multicast router ports.

You can execute the command before the VLAN is created.

Example

```
ZEQU0xxxxDL(config)# ipv6 mld snooping vlan 1 forbidden mrouter interface gi1/0/1
```

30.10 **ipv6 mld snooping vlan static**

To register a IPv6-layer Multicast address to the bridge table, and to add statically ports to the group, use the `ipv6 mld snooping vlan static` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
ipv6 mld snooping vlan vlan-id static ipv6-address [interface interface-list]
```

```
no ipv6 mld snooping vlan vlan-id static ipv6-address [interface interface-list]
```

Parameters

- `vlan-id`—Specifies the VLAN.
- `ipv6-address`—Specifies the IP multicast address
- `interface interface-list`—(Optional) Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

Static multicast addresses can only be defined on static VLANs. You can execute the command before the VLAN is created.

You can register an entry without specifying an interface. Using the `no` command without a port-list removes the entry.

Example

```
ZEQU0xxxxDL(config)# ipv6 mld snooping vlan 1 static FF12::3 gi1/0/1
```

30.11 **ipv6 mld snooping vlan immediate-leave**

To enable MLD Snooping Immediate-Leave processing on a VLAN, use the `ipv6 mld snooping vlan immediate-leave` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

`ipv6 mld snooping vlan vlan-id immediate-leave`

`no ipv6 mld snooping vlan vlan-id immediate-leave`

Parameters

`vlan-id`—Specifies the VLAN ID value. (Range: 1–4094)

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

When an MLD Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the MLD queries from the Multicast router, it deletes entries periodically if it does not receive any MLD membership reports from the Multicast clients.

MLD snooping Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface.

You can execute the command before the VLAN is created.

Example

```
ZEQU0xxxxDL(config)# ipv6 mld snooping vlan 1 immediate-leave
```

30.12 **show ipv6 mld snooping groups**

To display the multicast groups learned by the MLD snooping, use the `show ipv6 mld snooping groups` EXEC mode command in User EXEC mode.

Syntax

```
show ipv6 mld snooping groups [vlan vlan-id] [address ipv6-multicast-address] [source ipv6-address]
```

Parameters

- `vlan vlan-id`—(Optional) Specifies the VLAN ID.
- `address ipv6-multicast-address`—(Optional) Specifies the IPv6 multicast address.
- `source ipv6-address`—(Optional) Specifies the IPv6 source address.

Command Mode

User EXEC mode

Default Configuration

Display information for all VLANs and addresses defined on them.

User Guidelines

To see the full multicast address table (including static addresses), use the `show bridge multicast address-table` command.

The Include list contains the ports which are in a forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports which have issued an explicit Exclude for that specific source in a multicast group.

The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in a multicast bridge.

Note: Under certain circumstances, the Exclude list may not contain accurate information; for example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include list

Example

The following example shows the output for show ipv6 mld snooping groups.

ZEQU0xxxxDL# **show ipv6 mld snooping groups**

VLAN	Group Address	Source Address	Include Ports	Exclude Ports	Compatibility Mode
1	FF12::3	FE80::201:C9FF:FE40:8001	gi1/0/1		1
1	FF12::3	FE80::201:C9FF:FE40:8002	gi1/0/2		1
19	FF12::8	FE80::201:C9FF:FE40:8003	gi1/0/4		2
19	FF12::8	FE80::201:C9FF:FE40:8004	gi1/0/1	gi1/0/2	2
19	FF12::8	FE80::201:C9FF:FE40:8005	gi1/0/10-11	gi1/0/3	2

MLD Reporters that are forbidden statically:

VLAN	Group Address	Source Address	Ports
1	FF12::3	FE80::201:C9FF:FE40:8001	gi1/0/3
19	FF12::8	FE80::201:C9FF:FE40:8001	gi1/0/4

30.13 show ipv6 mld snooping interface

To display the IPv6 MLD snooping configuration for a specific VLAN, use the `show ipv6 mld snooping interface EXEC` mode command in User EXEC mode.

Syntax

```
show ipv6 mld snooping interface vlan-id
```

Parameters

- `vlan-id`—Specifies the VLAN ID.

Default Configuration

Display information for all VLANs.

Command Mode

User EXEC mode

Example

The following example displays the MLD snooping configuration for VLAN 1000.

```
ZEQUOxxxxDL# show ipv6 mld snooping interface 1000
MLD Snooping is globally enabled
MLD Snooping Querier is globally enabled
VLAN 1000
  MLD Snooping is enabled
  MLD snooping last immediate leave: enable
  Automatic learning of multicast router ports is enabled
  MLD Snooping Querier is enabled
  MLD Snooping Querier operation state: is running
  MLD Snooping Querier version: 2
  MLD Snooping Querier election is enabled
  MLD snooping robustness: admin 2 oper 2
  MLD snooping query interval: admin 125 sec oper 125 sec
  MLD snooping query maximum response: admin 10 sec oper 10 sec
  MLD snooping last member query counter: admin 2 oper 2
  MLD snooping last member query interval: admin 1000 msec oper 500 msec
```

30.14 **show ipv6 mld snooping mrouter**

To display information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN, use the `show ipv6 mld snooping mrouter EXEC mode` command in User EXEC mode.

Syntax

`show ipv6 mld snooping mrouter [interface vlan-id]`

Parameters

- `interface vlan-id`—(Optional) Specifies the VLAN ID.

Default Configuration

Display information for all VLANs.

Command Mode

User EXEC mode

Example

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000:

```
ZZEQU0xxxxDL# show ipv6 mld snooping mrouter interface 1000
```

VLAN	Dynamic	Static	Forbidden
1000	gi1/0/1	gi1/0/2	gi1/0/3-4

31 Network Management Protocol (SNMP)

Commands

31.1 snmp-server community

To set the community access string (password) that permits access to SNMP commands (v1 and v2), use the snmp-server community Global Configuration mode command. This is used for SNMP commands, such as GETs and SETs.

This command configures both SNMP v1 and v2.

To remove the specified community string, use the no form of this command.

Syntax

```
snmp-server community community-string [ro | rw | su] [ip-address | ipv6-address]  
[mask mask | prefix prefix-length] [view view-name]
```

```
no snmp-server community community-string [ip-address]
```

Parameters

- community-string—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- ro—(Optional) Specifies read-only access (default)
- rw—(Optional) Specifies read-write access
- su—(Optional) Specifies SNMP administrator access
- ip-address—(Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- mask—(Optional) Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- prefix-length—(Optional) Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- view view-name—(Optional) Specifies the name of a view configured using the command snmp-server view (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for su, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables, are available. (Range: 1–30 characters)

Default Configuration

No community is defined

Command Mode

Global Configuration mode

User Guidelines

The logical key of the command is the pair (community, ip-address). If ip-address is omitted, the key is (community, All-IPs). This means that there cannot be two commands with the same community, ip address pair.

The view-name is used to restrict the access rights of a community string. When a view-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.
- Maps the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also),

Example

Defines a password for administrator access to the management station at IP address 1.1.1.121 and mask 255.0.0.0.

```
ZEQU0xxxxDL (config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
```

31.2 snmp-server community-group

To configure access rights to a user group, use `snmp-server community-group`. The group must exist in order to be able to specify the access rights. This command configures both SNMP v1 and v2.

Syntax

```
snmp-server community-group community-string group-name [ip-address |  
ipv6-address] [mask mask | prefix prefix-length]
```

Parameters

- `community-string`—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- `group-name`—This is the name of a group configured using `snmp-server group` with v1 or v2 (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)
- `ip-address`—(Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- `mask`—(Optional) Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- `prefix-length`—(Optional) Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- `type router`—(Optional) Indicates whether the IP address is on the out-of-band or in-band network.

Default Configuration

No community is defined

Command Mode

Global Configuration mode

User Guidelines

The group-name is used to restrict the access rights of a community string. When a group-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

Example

Defines a password tom for the group abcd that enables this group to access the management station 1.1.1.121 with prefix 8.

```
ZEQU0xxxxDL (config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

31.3 snmp-server server

To enable the device to be configured by the SNMP protocol, use the `snmp-server server` Global Configuration mode command. To disable this function, use the `no` form of this command.

Syntax

`snmp-server server`

`no snmp-server server`

Parameters

N/A.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

```
ZEQU0xxxxDL(config)# snmp-server server
```

31.4 snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the `snmp-server source-interface` command in Global Configuration mode. To return to the default, use the `no` form of this command.

Syntax

```
snmp-server source-interface {traps | informs} interface-id
```

```
no snmp-server source-interface [traps | informs]
```

Parameters

- `traps`—Specifies the SNMP traps interface.
- `informs`—Specifies the SNMP informs.
- `interface-id`—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

If no parameters are specified in `no snmp-server source-interface`, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the `no snmp-server source-interface traps` command to remove the source interface for SNMP traps.

Use the `no snmp-server source-interface informs` command to remove the source interface for SNMP informs.

Use the `no snmp-server source-interface` command to remove the source interface for SNMP traps and informs.

Example

The following example configures the VLAN 100 as the source interface for traps.

```
ZEQU0xxxxDL (config) # snmp-server source-interface traps vlan 100
```

31.5 snmp-server source-interface-ipv6

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the `snmp-server source-interface` command in Global Configuration mode. To returned to the default, use the `no` form of this command.

Syntax

```
snmp-server source-interface-ipv6 {traps | informs} interface-id
```

```
no snmp-server source-interface-ipv6 [traps | informs]
```

Parameters

- `traps`—Specifies the SNMP traps interface.
- `informs`—Specifies the SNMP traps informs.
- `interface-id`—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address of the outgoing interface and selected in accordance with RFC6724.

If no parameters are specified in `no snmp-server source-interface`, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces is selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the `no snmp-server source-interface-ipv6 traps` command to remove the source IPv6 interface for SNMP traps.

Use the `no snmp-server source-interface-ipv6 informs` command to remove the source IPv6 interface for SNMP informs.

Use the `no snmp-server source-interface-ipv6` command to remove the source IPv6 interface for SNMP traps and informs.

Example

The following example configures the VLAN 100 as the source interface.

```
ZEQU0xxxxDL (config) # snmp-server source-interface-ipv6 traps vlan 100
```

31.6 snmp-server view

To create or update an SNMP view, use the `snmp-server view` Global Configuration mode command. To remove an SNMP view, use the `no` form of this command.

Syntax

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

```
no snmp-server view view-name [oid-tree]
```

Parameters

- `view-name`—Specifies the name for the view that is being created or updated. (Length: 1–30 characters)
- `included`—Specifies that the view type is included.
- `excluded`—Specifies that the view type is excluded.
- `oid-tree`—(Optional) Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System and, optionally, a sequence of numbers. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. This parameter depends on the MIB being specified.

Default Configuration

The following views are created by default:

- `Default`—Contains all MIBs except for those that configure the SNMP parameters themselves.
- `DefaultSuper`—Contains all MIBs.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view.

The command's logical key is the pair (view-name, oid-tree). Therefore there cannot be two commands with the same view-name and oid-tree.

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.

Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group (this format is specified on the parameters specified in ifEntry).

```
ZEQU0xxxxDL(config)# snmp-server view user-view system included
ZEQU0xxxxDL(config)# snmp-server view user-view system.7 excluded
ZEQU0xxxxDL(config)# snmp-server view user-view ifEntry.*.1 included
```

31.7 snmp-server group

To configure an SNMP group, use the `snmp-server group` Global Configuration mode command. Groups are used to map SNMP users to SNMP views. To remove an SNMP group, use the `no` form of this command.

Syntax

```
snmp-server group groupname {v1 | v2 | v3 {noauth | auth | priv} [notify notifyview]}  
[read readview] [write writeview]
```

```
no snmp-server group groupname {v1 | v2 | v3 [noauth | auth | priv]}
```

Parameters

- `group groupname`—Specifies the group name. (Length: 1–30 characters)
- `v1`—Specifies the SNMP Version 1 security model.
- `v2`—Specifies the SNMP Version 2 security model.
- `v3`—Specifies the SNMP Version 3 security model.
- `noauth`—Specifies that no packet authentication will be performed.
Applicable only to the SNMP version 3 security model.
- `auth`—Specifies that packet authentication without encryption will be performed.
Applicable only to the SNMP version 3 security model.
- `priv`—Specifies that packet authentication with encryption will be performed.
Applicable only to the SNMP version 3 security model. Note that creation of SNMPv3 users with both authentication and privacy must be done in the GUI. All other users may be created in the CLI.
- `notify notifyview`—(Optional) Specifies the view name that enables generating informs or a traps. An inform is a trap that requires acknowledgement. Applicable only to the SNMP version 3 security model. (Length: 1–32 characters)
- `read readview`—(Optional) Specifies the view name that enables viewing only. (Length: 1–32 characters)
- `write writeview`—(Optional) Specifies the view name that enables configuring the agent. (Length: 1–32 characters)

Default Configuration

No group entry exists.

If notifyview is not specified, the notify view is not defined.

If readview is not specified, all objects except for the community-table and SNMPv3 user and access tables are available for retrieval. If

writeview is not specified, the write view is not defined.

Command Mode

Global Configuration mode

User Guidelines

The group defined in this command is used in the snmp-server user command to map users to the group. These users are then automatically mapped to the views defined in this command.

The command logical key is (groupname, snmp-version, security-level). For snmp-version v1/v2 the security-level is always noauth.

Example

The following example attaches a group called user-group to SNMPv3, assigns the encrypted security level to the group, and limits the access rights of a view called user-view to read-only. User tom is then assigned to user-group. So that user tom has the rights assigned in user-view.

```
ZEQU0xxxxDL(config)# snmp-server group user-group v3 priv read user-view
ZEQU0xxxxDL(config)# snmp-server user tom user-group v3
```

31.8 show snmp views

To display SNMP views, use the show snmp views Privileged EXEC mode command.

Syntax

show snmp views [viewname]

Parameters

viewname—(Optional) Specifies the view name. (Length: 1–30 characters)

Default Configuration

If viewname is not specified, all views are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP views.

ZEUQ0xxxxDL# show snmp views		
Name	OID Tree	Type
Default	iso	included
Default	snmpNotificationMIB	excluded
Default	snmpVacmMIB	excluded
Default	snmpCommunityMIB	excluded
Default	rlSNMPv3	excluded
Default	snmpTargetAddrTable	excluded
Default	snmpTargetParamsTable	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
Default	Super iso	included

31.9 show snmp groups

To display the configured SNMP groups, use the show snmp groups Privileged EXEC mode command.

Syntax

show snmp groups [groupname]

Parameters

groupname—(Optional) Specifies the group name. (Length: 1–30 characters)

Default Configuration

Display all groups.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP groups.:

ZEQU0xxxxDL# show snmp groups					
Name	Security		Views		
	Model	Level	Read	Write	Notify
-----	-----	-----	-----	-----	-----
user-group	V2	no_auth	Default	""	""
managers-group	V2	no_auth	Default	Default	""

The following table describes significant fields shown above.

Field		Description
Name		Group name.
Security	Model	SNMP model in use (v1, v2 or v3).
Security	Level	Packet security. Applicable to SNMP v3 security only
Views	Read	View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	View name enabling data entry and managing the agent contents.
	Notify	View name enabling specifying an inform or a trap.

31.10 snmp-server user

To configure a new SNMP Version user, use the `snmp-server user` Global Configuration mode command. To remove a user, use the `no` form of the command.

Syntax

```
snmp-server user username groupname {v1 | v2c | [remote host] v3[auth {md5 | sha}
auth-password [priv priv-password] ]}
```

```
no snmp-server user username {v1 | v2c | [remote host] v3[auth {md5 | sha}
```

Parameters

- `username`—Define the name of the user on the host that connects to the agent. (Range: Up to 20 characters).
- `groupname`—The name of the group to which the user belongs. The group should be configured using the command `snmp-server group` with `v1` or `v2c` parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
- `v1`—Specifies that the user is a v1 user.
- `v2c`—Specifies that the user is a v2c user..
- `v3`—Specifies that the user is a v3 user..
- `remote host`—(Optional) IP address (IPv4, IPv6 or IPv6z) or host name of the remote SNMP host. See IPv6z Address Conventions.
- `auth`—(Optional) Specifies which authentication level is to be used.
- `md5`—(Optional) Specifies the HMAC-MD5-96 authentication level.
- `Sha`—(Optional) Specifies the HMAC-SHA-96 authentication level.
- `auth-password`—(Optional) Specifies the authentication password. Range: Up to 32 characters.
- `priv-password`—(Optional) Specifies the privacy password (The encryption algorithm used is data encryption standard - DES). Range: Up to 64 characters.

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

For SNMP v1 and v2, this command performs the same actions as `snmp-server community-group`, except that `snmp-server community-group` configures both v1 and v2 at the same time. With this command, you must perform it once for v1 and once for v2.

When you enter the `show running-config` command, you do not see a line for the SNMP user defined by this command. To see if this user has been added to the configuration, type the `show snmp user` command.

A local SNMP EngineID must be defined in order to add SNMPv3 users to the device (use the `snmp-server engineID remote` command). For remote hosts users a remote SNMP EngineID is also required (use the `snmp-server engineID remote` command).

Changing or removing the value of `snmpEngineID` deletes the SNMPv3 users' database.

The logical key of the command is `username`.

Configuring a remote host is required in order to send informs to that host, because an inform is a trap that requires acknowledgement. A configured remote host is also able to manage the device (besides getting the informs)

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID remote` command. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command fails.

Since the same group may be defined several times, each time with different version or different access level (noauth, auth or auth & priv), when defining a user it is not sufficient to specify the group name, rather you must specify group name, version and access level for complete determination of how to handle packets from this user.

Example

This example assigns user `tom` to group `abcd` using SNMP v1 and v2c. The default is assigned as the engineID. User `tom` is assigned to group `abcd` using SNMP v1 and v2c

```
ZEQU0xxxxDL(config)# snmp-server user tom acbd v1
ZEQU0xxxxDL(config)# snmp-server user tom acbd v2c
ZEQU0xxxxDL(config)# snmp-server user tom acbd v3
```

31.11 **show snmp users**

To display the configured SNMP users, use the show snmp users Privileged EXEC mode command.

Syntax

```
show snmp users [username]
```

Parameters

username—(Optional) Specifies the user name. (Length: 1–30 characters)

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Example

The following examples displays the configured SNMP users:

ZEQU0xxxxDL# **show snmp users**

```
User name          :ulrem
  Group name       :group1
  Authentication Algorithm : None
  Privacy Algorithm : None
  Remote          :11223344556677
  Auth Password   :
  Priv Password   :
User name          : qqg
  Group name       : www
  Authentication Algorithm : MD5
  Privacy Algorithm : None
  Remote          :
  Auth Password   : helloworld1234567890987665
  Priv Password   :
User name          : hello Group
  name            : world
  Authentication Algorithm : MD5
  Privacy Algorithm : DES
  Remote          :
  Auth Password (encrypted): Z/tC3UF5j0pYfmXm8xeMvcIOQ6LQ4GOACCGYLrdAgOE6XQKTC
                                qMlrnpWuHraRIZj
  Priv Password (encrypted) : kN1ZHzSL06WWxIkuZVzhL0o1gI5waaNf7Vq6yLBpJdS4N68tL
                                1tbTRSz2H4c4Q4o
User name          : u1noAuth
  Group name       : group1
  Authentication Algorithm : None
  Privacy Algorithm : None
  Remote          :
  Auth Password (encrypted):
  Priv Password (encrypted):
User name          : u1onlyAuth
  Group name       : group1
  Authentication Algorithm : SHA
  Privacy Algorithm : None
  Remote          :
  Auth Password (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9W0RFRM= Priv
  Password (encrypted) :
```

31.12 snmp-server filter

To create or update an SNMP server notification filter, use the snmp-server filter Global Configuration mode command. To remove a notification filter, use the no form of this command.

Syntax

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

```
no snmp-server filter filter-name [oid-tree]
```

Parameters

- **filter-name**—Specifies the label for the filter record that is being updated or created. The name is used to reference the filter in other commands. (Length: 1–30 characters)
- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included**—Specifies that the filter type is included.
- **excluded**—Specifies that the filter type is excluded.

Default Configuration

No view entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter. If an object identifier is included in two or more lines, later lines take precedence. The command's logical key is the pair (filter-name, oid-tree).

Example

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group (this format depends on the parameters defined in ifEntry).

```
ZEQU0xxxxDL(config)# snmp-server filter f1 system included
ZEQU0xxxxDL(config)# snmp-server filter f2 system.7 excluded
ZEQU0xxxxDL(config)# snmp-server filter f3 ifEntry.*.1 included
```

31.13 show snmp filters

To display the defined SNMP filters, use the show snmp filters Privileged EXEC mode command.

Syntax

show snmp filters [filtername]

Parameters

filtername—Specifies the filter name. (Length: 1–30 characters)

Default Configuration

If filtername is not defined, all filters are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP filters.

ZEUQ0xxxxDL# show snmp filters user-filter		
Name	OID Tree	Type
-----	-----	-----
user-filter	1.3.6.1.2.1.1	Included
user-filter	1.3.6.1.2.1.1.7	Excluded
user-filter	1.3.6.1.2.1.2.2.1.*.1	Included

31.14 snmp-server host

To configure the host for SNMP notifications: (traps/informs), use the `snmp-server host` Global Configuration mode command. To remove the specified host, use the `no` form of this command.

Syntax

```
snmp-server host {host-ip | hostname} [traps | informs] [version {1 | 2c | 3 [auth |  
noauth | priv]]] community-string [udp-port port] [filter filtername] [timeout  
seconds] [retries retries]
```

```
no snmp-server host {ip-address | hostname} [traps | informs] [version {1 | 2c | 3}]
```

Parameters

- `host-ip`—IP address of the host (the targeted recipient). The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- `hostname`—Hostname of the host (the targeted recipient). (Range: 1–158 characters. Maximum label size of each part of the host name: 63)
- `trap`—(Optional) Sends SNMP traps to this host (default).
- `informs`—(Optional) Sends SNMP informs to this host. An inform is a trap that requires acknowledgement. Not applicable to SNMPv1.
- `version 1`—(Optional) SNMPv1 traps are used.
- `version 2c`—(Optional) SNMPv2 traps or informs are used
- `version 3`—(Optional) SNMPv2 traps or informs are used
- Authentication options are available for SNMP v3 only. The following options are available:
 - `noauth`—(Optional) Specifies no authentication of a packet.
 - `auth`—(Optional) Specifies authentication of a packet without encryption.
 - `priv`—(Optional) Specifies authentication of a packet with encryption.
- `community-string`—Password-like community string sent with the notification operation. (Range: 1–20 characters). For v1 and v2, any community string can be entered here. For v3, the community string must match the user name defined in `snmp-server user` (ISCLI) command for v3.
- `udp-port port`—(Optional) UDP port of the host to use. The default is 162. (Range: 1–65535)

- **filter filtername**—(Optional) Filter for this host. If unspecified, nothing is filtered. The filter is defined using `snmp-server filter` (no specific order of commands is imposed on the user). (Range: Up to 30 characters)
- **timeout seconds**—(Optional) (For informs only) Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1–300)
- **retries retries**—(Optional) (For informs only) Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. (Range: 0–255)

Default Configuration

Version: SNMP V1

Type of notification: Traps

udp-port: 162

If informs are specified, the default for retries: 3

Timeout: 15

Command Mode

Global Configuration mode

User Guidelines

The logical key of the command is the list (ip-address/hostname, traps/informs, version).

When configuring SNMP v1 or v2 notifications recipient, the software automatically generates a notification view for that recipient for all MIBs.

For SNMPv3 the software does not automatically create a user or a notify view.

, use the commands `snmp-server user` (ISCLI) and `snmp-server group` to create a user or a group.

Example

The following defines a host at the IP address displayed.

```
ZEQU0xxxxDL (config)# snmp-server host 1.1.1.121 abc
```

31.15 snmp-server engineID local

To specify the SNMP engineID on the local device for SNMP v3, use the `snmp-server engineID local` Global Configuration mode command. To remove this engine ID, use the `no` form of this command.

Syntax

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

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

Parameters

- `engineid-string`—Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)
- `default`—Specifies that the engine ID is created automatically based on the device MAC address.

Default Configuration

The default engine ID is defined per standard as:

- First 4 octets: First bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet: Set to 3 to indicate the MAC address that follows.
- Last 6 octets: The device MAC address.

Command Mode

Global Configuration mode

User Guidelines

To use SNMPv3, an engine ID must be specified for the device. Any ID can be specified or the default string, which is generated using the device MAC address, can be used.

As the engineID should be unique within an administrative domain, the following guidelines are recommended:

- Configure a non-default EngineID, and verify that it is unique within the administrative domain.
- Changing or removing the value of `snmpEngineID` deletes the SNMPv3 users database.
- The SNMP EngineID cannot be all 0x0 or all 0xF or 0x000000001.

Example

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
ZEQU0xxxxDL(config)# snmp-server engineid local default
```

The engine-id must be unique within your administrative domain. Do you wish to continue?

[Y/N]Y

The SNMPv3 database will be erased. Do you wish to continue? [Y/N]Y

31.16 snmp-server engineID remote

To specify the SNMP engine ID of a remote SNMP device, use the `snmp-server engineID remote` Global Configuration mode command. To remove the configured engine ID, use the `no` form of this command.

Syntax

`snmp-server engineID remote ip-address engineid-string`

`no snmp-server engineID remote ip-address`

Parameters

- `ip-address` —IPv4, IPv6 or IPv6z address of the remote device. See IPv6z Address Conventions.
- `engineid-string`—The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. If the user enters an odd number of hexadecimal digits, the system automatically prefixes the hexadecimal string with a zero. (Range: `engineid-string` 5–32 characters. 9–64 hexadecimal digits)

Default Configuration

The remote engineID is not configured by default.

Command Mode

Global Configuration mode

User Guidelines

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Example

```
ZEQU0xxxxDL(config)# snmp-server engineID remote 1.1.1.1 11:AB:01:CD:23:44
```

31.17 **show snmp engineID**

To display the local SNMP engine ID, use the show snmp engineID Privileged EXEC mode command.

Syntax

show snmp engineID

Parameters

N/A

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP engine ID.

```
ZEQU0xxxxDL# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
IP address           Remote SNMP engineID
-----
172. 16. 1. 1       08009009020C0B099C075879
```

31.18 **snmp-server enable traps**

To enable the device to send SNMP traps, use the `snmp-server enable traps` Global Configuration mode command. To disable all SNMP traps, use the `no` form of the command.

Syntax

`snmp-server enable traps`

`no snmp-server enable traps`

Default Configuration

SNMP traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

If no `snmp-server enable traps` has been entered, you can enable failure traps by using `snmp-server trap authentication` as shown in the example.

Example

The following example enables SNMP traps except for SNMP failure traps.

```
ZEQU0xxxxDL (config) # snmp-server enable traps
ZEQU0xxxxDL (config) # no snmp-server trap authentication
```

31.19 snmp-server trap authentication

To enable the device to send SNMP traps when authentication fails, use the `snmp-server trap authentication` Global Configuration mode command. To disable SNMP failed authentication traps, use the `no snmp-server trap authentication` command.

Syntax

`snmp-server trap authentication`

`no snmp-server trap authentication`

Parameters

N/A

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

The command `snmp-server enable traps` enables all traps including failure traps. Therefore, if that command is enabled (it is enabled by default), this command is not necessary.

Example

The following example disables all SNMP traps and enables only failed authentication traps.

```
ZEQU0xxxxDL (config) # no snmp-server enable traps
ZEQU0xxxxDL (config) # snmp-server trap authentication
```

31.20 **snmp-server contact**

To set the value of the system contact (sysContact) string, use the `snmp-server contact` Global Configuration mode command. To remove the system contact information, use the `no snmp-server contact` command.

Syntax

`snmp-server contact text`

`no snmp-server contact`

Parameters

`text`—Specifies system contact information. (Length: 1–160 characters)

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the system contact information to `Technical_Support`.

```
ZEQU0xxxxDL (config)# snmp-server contact Technical_Support
```

31.21 **snmp-server location**

To set the value of the system location string, use the snmp-server location Global Configuration mode command. To remove the location string, use the no form of this command.

Syntax

snmp-server location text

no snmp-server location

Parameters

text—Specifies the system location information. (Length: 1–160 characters)

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the device location to New_York.

```
ZEQU0xxxxDL (config) # snmp-server location New_York
```

31.22 snmp-server set

To define SNMP MIB commands in the configuration file if a MIB performs an action for which there is no corresponding CLI command, use the `snmp-server set` Global Configuration mode command.

Syntax

```
snmp-server set variable-name name value [name2 value2...]
```

Parameters

- `variable-name`—Specifies an SNMP MIB variable name, which must be a valid string.
- `name value`—Specifies a list of names and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

Default Configuration

None

Command Mode

Global Configuration mode

User Guidelines

Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent CLI command. To generate configuration files that support those situations, the system uses `snmp-server set`. This command is not intended for the end user.

Example

The following example configures the scalar MIB `sysName` with the value `TechSupp`.

```
ZEQU0xxxxDL(config)# snmp-server set sysName sysname TechSupp
```

31.23 **snmp trap link-status**

To enable link-status generation of SNMP traps, use the `snmp trap link-status` Interface Configuration mode command. To disable generation of link-status SNMP traps, use the `no` form of this command.

Syntax

`snmp trap link-status`

`no snmp trap link-status`

Parameters

N/A.

Default Configuration

Generation of SNMP link-status traps is enabled

Command Mode

Interface Configuration mode

Example

The following example disables generation of SNMP link-status traps.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# no snmp trap link-status
```

31.24 **show snmp**

To display the SNMP status, use the show snmp Privileged EXEC mode command.

Syntax

show snmp

Parameters

N/A

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP communications status.

```
ZEQU0xxxxDL# show snmp
```

SNMP is enabled.

SNMP traps Source IPv4 interface: vlan 1
SNMP informs Source IPv4 interface: vlan 11
SNMP traps Source IPv6 interface: vlan 10
SNMP informs Source IPv6 interface:

Community-String	Community-Access	View name	IP Address	Mask
public	read only	user-view	All	
private	read write	Default	172.16.1.1/10	
private	su	DefaultSuper	172.16.1.1	

Community-string	Group name	IP Address	Mask	Type
public	user-group	All		Router

Traps are enabled.

Authentication trap is enabled.

Version 1,2 notifications

Target Address	Type	Community	Version	UDP Port	Filter Name	T0 Sec	Retries
192.122.173.42	Trap	public	2	162		15	3
192.122.173.42	Inform	public	2	162		15	3

Version 3 notifications

Target Address	Type	Username	Security Level	UDP Port	Filter name	T0 Sec	Retries
192.122.173.42	Inform	Bob	Priv	162		15	3

System Contact: Robert

System Location: Marketing

The following table describes the significant fields shown in the display.

Field	Description
Community-string	The community access string permitting access to SNMP.
Community-access	The permitted access type—read-only, read-write, super access.
IP Address	The management station IP Address.
Target Address	The IP address of the targeted recipient.
Version	The SNMP version for the sent trap.

32 PHY Diagnostics Commands

32.1 test cable-diagnostics tdr

To use Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port, use the test cable-diagnostics tdr Privileged EXEC mode command.

Syntax

test cable-diagnostics tdr interface interface-id

Parameters

interface-id—(Optional) Specifies an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

This command does not work on fiber ports (if they exist on the device). The port to be tested should be shut down during the test, unless it is a combination port with fiber port active. In this case, it does not need to be shut down, because the test does not work on fiber ports.

The maximum length of cable for the TDR test is 120 meters.

Examples

Example 1 - Test the copper cables attached to port gi1/0/1 (a copper port).

```
ZEQU0xxxxDL# test cable-diagnostics tdr interface gi1/0/1
Cable is open at 64 meters
```

Example 2 - Test the copper cables attached to port 2 (a combo port with fiber active).

```
ZEQU0xxxxDL# test cable-diagnostics tdr interface gi1/0/2
Fiber ports are not supported
```

32.2 show cable-diagnostics tdr

To display information on the last Time Domain Reflectometry (TDR) test performed on all copper ports or on a specific copper port, use the `show cable-diagnostics tdr` Privileged EXEC mode command.

Syntax

```
show cable-diagnostics tdr [interface interface-id]
```

Parameters

- `interface-id`—(Optional) Specify an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

The maximum length of cable for the TDR test is 120 meters.

Example

The following example displays information on the last TDR test performed on all copper ports.

```
ZEQU0xxxxDL# show cable-diagnostics tdr
```

Port	Result	Length [meters]	Date
----	-----	-----	-----
gi1/0/1	OK		
gi1/0/2	Short	50	13:32:00 23 July 2017
gi1/0/3	Test has not been performed		
gi1/0/4	Open	64	13:32:00 23 July 2017

32.3 show cable-diagnostics cable-length

To display the estimated copper cable length attached to all ports or to a specific port, use the show cable-diagnostics cable-length Privileged EXEC mode command.

Syntax

show cable-diagnostics cable-length [interface interface-id]

Parameters

- interface-id—(Optional) Specify an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

The port must be active and working at 100 M or 1000 M.

Example

The following example displays the estimated copper cable length attached to all ports.

ZEUQ0xxxxDL# show cable-diagnostics tdr			
Port	Result	Length [meters]	Date
----	-----	-----	-----
gi1/0/1	OK		
gi1/0/2	Short	50	13:32:00 23 July 2017
gi1/0/3	Test has not been performed		
gi1/0/4	Open	64	13:32:00 23 July 2017

33 Port Channel Commands

33.1 channel-group

To associate a port with a port-channel, use the channel-group Interface (Ethernet) Configuration mode command. To remove a port from a port-channel, use the no form of this command.

Syntax

channel-group CHANNEL-NO mode {on | auto}

no channel-group

Parameters

- CHANNEL-NO—Specifies the port channel number for the current port to join. (Range: 1–32)
- mode—Specifies the mode of joining the port channel. The possible values are:
 - on—Forces the port to join a channel without an LACP operation.
 - auto— In an active negotiating state and the port initiates negotiations with other ports by sending LACP packets.
 - In a passive negotiation state and the port responds to LACP packets that it receives but does not initiate LACP negotiation.

Default Configuration

The port is not assigned to a port-channel.

Command Mode

Interface (Ethernet) Configuration mode

Default mode is on.

User Guidelines

LACP starts to manage port joining.

Example

The following example forces port gi1/0/25 to join port-channel 1 without an LACP operation.

```
ZEQU0xxxxDL(config)# interface gi1/0/25
ZEQU0xxxxDL(config-if)# channel-group 1 mode on
```

33.2 port-channel load-balance

To configure the load balancing policy of the port channeling, use the port-channel load-balance Global Configuration mode command. To reset to default, use the no form of this command.

Syntax

port-channel load-balance {src-dst-mac | src-dst-mac-ip}

no port-channel load-balance

Parameters

- src-dst-mac—Port channel load balancing is based on the source and destination MAC addresses.
- src-dst-mac-ip—Port channel load balancing is based on the source and destination of MAC and IP addresses.

Default Configuration

src-dst-mac is the default option.

Command Mode

Global Configuration mode

Example

```
ZEQU0xxxxDL (config) # port-channel load-balance src-dst-mac
```

33.3 show channel-group

To display port-channel information for all port channels or for a specific port channel, use the show channel-group Privileged EXEC mode command.

Syntax

```
show channel-group [channel [CHANNEL-NO]]
```

Parameters

CHANNEL-NO—(Optional) Specify a port channel number.

Command Mode

Privileged EXEC mode

Examples

The following example displays information on all port-channels.

```
ZEQU0xxxxDL# show channel-group
```

```
Load balancing: src-dst-mac.
```

```
Gathering information...
```

```
Channel  Ports
```

```
-----  -
```

```
Po1      Active: gi1/0/1-3
```

```
Po2
```

34 Quality of Service (QoS) Commands

34.1 mls qos

Use the qos Global Configuration mode command to enable QoS on the device and set its mode. Use the no form of this command to disable QoS on the device.

Syntax

```
mls qos [basic | {advanced [ports-not-trusted | ports-trusted]}]
```

```
no mls qos
```

Parameters

- **basic**—QoS basic mode. If no option is specified, the QoS mode defaults to the basic mode.
- **advanced**—Specifies the QoS advanced mode, which enables the full range of QoS configuration.
- **ports-not-trusted**—Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to egress queue 0. This is the default setting in advanced mode.
- **ports-trusted**—Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to an egress queue based on the packet's fields. Use the mls qos advanced-mode trust command to specify the trust mode.

Default Configuration

QoS basic mode

Command Mode

Global Configuration mode

Examples

Example 1—The following example disables QoS on the device.

```
ZEQU0xxxxDL (config)# no mls qos
```

Example 2—The following example enables QoS advanced mode on the device with the **ports-not-trusted** option.

```
ZEQU0xxxxDL (config)# mls qos advanced
```

34.2 mls qos advanced-mode trust

Use the mls qos advanced-mode trust Global Configuration mode command to configure the trust mode in advanced mode. Use the no form of this command to return to default.

Syntax

```
mls qos advanced-mode trust {cos | dscp | cos-dscp}
```

```
no mls qos advanced-mode trust
```

Parameters

- cos—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- dscp—Classifies ingress packets with the packet DSCP values.
- cos-dscp—Classifies ingress packets with the packet DSCP values for IP packets. For other packet types, use the packet CoS values.

Default Configuration

cos-dscp

Command Mode

Global Configuration mode

User Guidelines

The configuration is relevant for advanced mode in the following cases:

- ports-not-trusted mode: For packets that are classified to the QoS action trust.
- ports-trusted mode: For packets that are not classified by to any QoS action or classified to the QoS action trust.

Example

The following example sets cos as the trust mode for QoS on the device.

```
ZEQU0xxxxDL(config)# mls qos advanced-mode trust cos
```

34.3 show mls qos

Use the show mls qos Privileged EXEC mode command to display the QoS information for the device. The trust mode is displayed for the QoS basic mode.

Syntax

show mls qos

Parameters

N/A

Default Configuration

Disabled Command Mode

Command Mode

Privileged EXEC mode

User Guidelines

Trust mode is displayed if QoS is enabled in basic mode.

Examples

```
ZEQU0xxxxDL(config)# show mls qos
Qos: Disabled
ZEQU0xxxxDL(config)# show mls qos
Qos: Basic mode
Basic trust: dscp
ZEQU0xxxxDL(config)# show mls qos
Qos: Advanced mode
Advanced mode trust type: cos
Advanced mode ports state: Trusted
```

34.4 class-map

Use the class-map Global Configuration mode command to create or modify a class map and enter the Class-map Configuration mode (only possible when QoS is in the advanced mode). Use the no form of this command to delete a class map.

Syntax

```
class-map class-map-name [match-all | match-any]
```

```
no class-map class-map-name
```

Parameters

- class-map-name—Specifies the class map name. (Length: 1–32 characters)
- match-all—Performs a logical AND of all the criteria of the ACLs belonging to this class map. All match criteria in this class map must be matched. If neither match-all nor match-any is specified, the match-all parameter is selected by default.
- match-any—Performs a logical OR of the criteria of the ACLs belonging to this class map. Only a single match criteria in this class map must be matched.

Default Configuration

No class map.

Command Mode

Global Configuration mode

User Guidelines

The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally-named service policy applied on a per-interface basis.

A class map consists of one or more ACLs. It defines a traffic flow by determining which packets match some or all of the criteria specified in the ACLs.

All class map commands are only available when QoS is in advanced mode. The

class-map enters Class-map Configuration mode. In this mode, up to two match commands can be entered to configure the criteria for this class. Each match specifies an ACL.

When using a few match commands, each must point to a different type of ACL, such as: one IP ACL, one IPv6 ACL, and one MAC ACL. The classification is by first match, therefore, the order of the ACLs is important.

Error messages are generated in the following cases:

- There is more than one match command in a match-all class map
- There is a repetitive classification field in the participating ACLs.

After entering the Class-map Configuration mode, the following configuration commands are available:

- `exit`: Exits the Class-map Configuration mode.
- `match`: Configures classification criteria.
- `no`: Removes a match statement from a class map.

Example

The following example creates a class map called Class1 and configures it to check that packets match all classification criteria in the ACL specified.

```
ZEQU0xxxxDL(config)# class-map class1 match-all  
ZEQU0xxxxDL(config-cmap)# match access-group acl-name
```

34.5 show class-map

The show class-map Privileged EXEC mode command displays all class maps when QoS is in advanced mode.

Syntax

```
show class-map [class-map-name]
```

Parameters

class-map-name—Specifies the name of the class map to be displayed. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

Example

The following example displays the class map for Class1.

```
ZEQU0xxxxDL (config)# show class-map  
Class Map matchAll c1  
  Match access-group a1
```

34.6 match

Use the match Class-map Configuration mode. command to bind the ACLs that belong to the class-map being configured. Use the no form of this command to delete the ACLs.

Syntax

match access-group acl-name

no match access-group acl-name

Parameters

acl-name—Specifies the MAC, IP ACL name, or IPv6 ACL name. (Length: 1–32 characters)

Default Configuration

No match criterion is supported.

User Guidelines

This command is available only when the device is in QoS advanced mode.

Command Mode

Class-map Configuration mode.

Example

The following example defines a class map called Class1. Class1 contains an ACL called enterprise. Only traffic matching all criteria in enterprise belong to the class map.

```
ZEQU0xxxxDL(config)# class-map class1
ZEQU0xxxxDL(config-cmap)# match access-group enterprise
```

34.7 policy-map

Use the policy-map Global Configuration mode command to creates a policy map and enter the Policy-map Configuration mode. Use the no form of this command to delete a policy map.

Syntax

```
policy-map policy-map-name  
no policy-map policy-map-name
```

Parameters

policy-map-name—Specifies the policy map name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

This command is only available when QoS is in advanced mode.

Use the policy-map Global Configuration mode command to specify the name of the policy map to be created, added to, or modified before configuring policies for classes whose match criteria are defined in a class map.

A policy map contains one or more class maps and an action that is taken if the packet matches the class map. Policy maps may be bound to ports/port-channels.

Entering the policy-map Global Configuration mode command also enables configuring or modifying the class policies for that policy map. Class policies in a policy map can be configured only if the classes have match criteria defined for them.

Policy map is applied on the ingress path.

The match criteria is for a class map. Only one policy map per interface is supported. The same policy map can be applied to multiple interfaces and directions.

The service-policy command binds a policy map to a port/port-channel.

Example

The following example creates a policy map called Policy1 and enters the Policy-map Configuration mode.

```
ZEQU0xxxxDL (config)# policy-map policy1  
ZEQU0xxxxDL (config-pmap)#
```

34.8 class

Use the class Policy-map Configuration mode. command after the policy-map command to attach ACLs to a policy-map. Use the no form of this command to detach a class map from a policy map.

Syntax

class class-map-name [access-group acl-name]

no class class-map-name

Parameters

- class-map-name—Specifies the name of an existing class map. If the class map does not exist, a new class map is created under the specified name. (Length: 1–32 characters)
- access-group acl-name—Specifies the name of an IP, IPv6, or MAC Access Control List (ACL). (Length: 1–32 characters)

Default Configuration

No class map is defined for the policy map.

Command Mode

Policy-map Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

This is the same as creating a class map and then binding it to the policy map. You can specify an existing class map in this command, or you can use the access-group parameter to create a new class map.

After the policy-map is defined, use the service-policy command to attach it to a port/port-channel.

Example

The following example defines a traffic classification (class map) called class1 containing an ACL called enterprise. The class is in a policy map called policy1. The policy-map policy1 now contains the ACL enterprise.

```
ZEQU0xxxxDL (config)# policy-map policy1
ZEQU0xxxxDL (config-pmap)# class class1 access-group enterprise
```

34.9 show policy-map

Use the show policy-map Privileged EXEC mode command to display all policy maps or a specific policy map.

This command is only available when QoS is in advanced mode.

Syntax

show policy-map [policy-map-name]

Parameters

policy-map-name—Specifies the policy map name. (Length: 1–32 characters)

Default Configuration

All policy-maps are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays all policy maps.

```
ZEQU0xxxxDL (config)# show policy-map
Policy Map policy1
  class class1
  set dscp 7
Policy Map policy2
  class class 2
  police 96000 4800 exceed-action drop class
  class2
  redirect gi1/0/2
  class class 3
  police 96000 4800 exceed-action policed-dscp-transmit peak 128000 9600 violate-action
  policed-dscp-transmit
```

34.10 **trust**

Use the trust Policy-map Class Configuration mode. command to configure the trust state. Use the no form of this command to return to the default trust state.

Syntax

trust

no trust

Parameters

N/A

Default Configuration

The default state is according to the mode selected in the qos command (advanced mode). The type of trust is determined in mls qos advanced-mode trust.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is relevant only when QoS is in advanced, ports-not-trusted mode. Trust indicates that traffic is sent to the queue according to the packet's QoS parameters (UP or DSCP).

Use this command to distinguish the QoS trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class map can be configured to match and trust the DSCP values in the incoming traffic.

The type of trust is determined in mls qos advanced-mode trust.

Trust values set with this command supersede trust values set on specific interfaces with the qos trust (Interface) Interface Configuration mode command.

The trust and set commands are mutually exclusive within the same policy map. The set command is not supported into egress policies.

If specifying trust cos, QoS maps a packet to a queue, the received or default port CoS value, and the CoS-to-queue map.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and configures the trust state.

```
ZEQU0xxxxDL(config)# ip access-list extended ip1
ZEQU0xxxxDL(config-ip-a1)#permit ip any any
ZEQU0xxxxDL(config-ip-a1)#exit
ZEQU0xxxxDL(config)# class-map c1
ZEQU0xxxxDL(config-cmap)# match access-group ip1
ZEQU0xxxxDL(config-cmap)# exit
ZEQU0xxxxDL(config)# policy-map p1
ZEQU0xxxxDL(config-pmap)# class c1
ZEQU0xxxxDL(config-pmap-c)#trust
```

34.11 set

Use the set Policy-map Class Configuration mode. command to select the value that QoS uses as the DSCP value, the egress queue or to set user priority values.

Syntax

```
set {dscp new-dscp | queue queue-id | cos new-cos}
```

```
no set
```

Parameters

- dscp new-dscp—Specifies the new DSCP value for the classified traffic. (Range: 0–63)
- queue queue-id—Specifies the egress queue. (Range: 1-8)
- cos new-cos—Specifies the new user priority to be marked in the packet. (Range: 0–7)

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

The set and trust commands are mutually exclusive within the same policy map. To return to the Configuration mode, use the exit command. To return to the Privileged EXEC mode, use the end command.

The queue keyword is not supported into egress policies.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and sets the DSCP value in the packet to 56 for classes in the policy map called p1.

```
ZEQU0xxxxDL(config)# ip access-list extended ip1
ZEQU0xxxxDL(config-ip-acl)# permit ip any any
ZEQU0xxxxDL(config-ip-acl)# exit
ZEQU0xxxxDL(config)# class-map c1
ZEQU0xxxxDL(config-cmap)# match access-group ip1
ZEQU0xxxxDL(config-cmap)# exit
ZEQU0xxxxDL(config)# policy-map p1
ZEQU0xxxxDL(config-pmap)# class c1
ZEQU0xxxxDL(config-pmap-c)# set dscp 56
```

34.12 redirect

Use the redirect Policy-map Class Configuration mode. command to redirect a traffic flow to a given Ethernet port or port channel.

Syntax

redirect interface-id

no redirect

Parameters

- interface-id—Specifies an Ethernet port or port channel to which the flow is redirected.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

Use the redirect command to redirect a frame into the VLAN the frame was assigned to.

This command is only available when QoS is in advanced mode.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and redirects the flow to Ethernet port gi1/0/2:

```
ZEQU0xxxxDL (config)# ip access-list extended ip1
ZEQU0xxxxDL (config-ip-al)# permit ip any any
ZEQU0xxxxDL (config-ip-al)# exit
ZEQU0xxxxDL (config)# class-map c1
ZEQU0xxxxDL (config-cmap)# match access-group ip1
ZEQU0xxxxDL (config-cmap)# exit
ZEQU0xxxxDL (config)# policy-map p1
ZEQU0xxxxDL (config-pmap)# class c1
ZEQU0xxxxDL (config-pmap-c)# redirect gi1/0/2
ZEQU0xxxxDL (config-pmap-c)# exit
ZEQU0xxxxDL (config-pmap)# exit
ZEQU0xxxxDL (config)#
```

34.13 mirror

Use the mirror Policy-map Class Configuration mode. command to mirror a traffic flow to an analyzer Ethernet port.

Syntax

mirror session_number

no mirror

Parameters

- session_number—Specify the session number identified with the SPAN or RSPAN session. Only a value of 1 is allowed.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

A frame is mirrored in the same format if it matches to one of the class ACLs regardless the command of this ACL: permit or deny.

Only one source session from VLAN and flow mirroring is supported.

The analyzer Ethernet port is configured by the monitor session destination command with the same session number.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and mirrors the flow to an analyzer Ethernet port defined by session 2:

```
ZEQU0xxxxDL(config)# ip access-list extended ip1
ZEQU0xxxxDL(config-ip-acl)# permit ip any any
ZEQU0xxxxDL(config-ip-acl)# exit
ZEQU0xxxxDL(config)# class-map c1
ZEQU0xxxxDL(config-cmap)# match access-group ip1
ZEQU0xxxxDL(config-cmap)# exit
ZEQU0xxxxDL(config)# policy-map p1
ZEQU0xxxxDL(config-pmap)# class c1
ZEQU0xxxxDL(config-pmap-c)# mirror 2
ZEQU0xxxxDL(config-pmap-c)# exit
ZEQU0xxxxDL(config-pmap)# exit
ZEQU0xxxxDL(config)#
```

34.14 police

Use the police Policy-map Class Configuration mode. command to define the policer for classified traffic. This defines another group of actions for the policy map (per class map). Use the no form of this command to remove a policer.

Syntax

```
police committed-rate-kbps committed-burst-byte [exceed-action action] [peak  
peak-rate-kbps peak-burst-byte [violate-action action]]
```

```
no police
```

Parameters

- committed-rate-kbps—Specifies the average traffic rate (CIR) in kbits per second (bps). (Range: 3–57982058)
- committed-burst-byte—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- exceed-action—Specifies the action taken when the committed rate is exceeded and the peak rate is not exceeded. If the keyword is not configured then the following action is applied:
 - drop, if peak the keyword is not configured.
 - policed-dscp-transmit, if peak the keyword is configured.
- peak—Specifies the Two-rate Three-color policer. If the peak rate is exceeded the packet is dropped.
- peak-rate-kbps—Specifies the average traffic rate (CIR) in kbits per second (bps). (Range: 3–57982058)
- peak-burst-byte—Specifies the peak burst size (PBS) in bytes. (Range: 3000–19173960)
- violate-action—Specifies the action taken when the peak rate is exceeded. If the keyword is not configured then the drop action is applied.
- action—Specifies the taken action. The possible values are:
 - drop—Drops the packet.
 - policed-dscp-transmit—Remarks the packet DSCP of IP traffic. The DSCP remarking is configured by the qos map policed-dscp command with the violation keyword for the violation action and without this keyword for the exceed action. DSCP remarking will have effect only if the mode is trust dscp.

Default Usage

No policer

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is used after the policy-map and class commands. This command is only available when QoS is in advanced mode. Policing uses a token bucket algorithm.

Examples

Example 1. The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 kbps and the normal burst size exceeds 9600 bytes, the packet is dropped. The class is called class1 and is in a policy map called policy1.

```
ZEQU0xxxxDL(config)# policy-map policy1
ZEQU0xxxxDL(config-pmap)# class cls1
ZEQU0xxxxDL(config-pmap-c)# police 124000 9600 exceed-action drop
```

Example 2. The following example defines a Two-rate Three-color policer for classified traffic. When the committed traffic rate exceeds 124,000 kbps and the committed burst size exceeds 9600 bytes, the packet is marked. When the peak traffic rate exceeds 200,000 kbps and the peak burst size exceeds 19200 bytes, the packet is marked. The class is called class1 and is in a policy map called policy1.

```
ZEQU0xxxxDL(config)# policy-map policy1
ZEQU0xxxxDL(config-pmap)# class cls1
ZEQU0xxxxDL(config-pmap-c)# police 124000 9600 exceed-action
policed-dscp-transmit peak 200000 19200 violate-action policed-dscp-transmit
```

34.15 service-policy

Use the service-policy Interface (Ethernet, Port Channel) Configuration mode mode command to bind a policy map to an interface. Use the no form of this command to detach a policy map from an interface.

Syntax

```
service-policy {input | output} policy-map-name [default-action {permit-any | deny-any}]
```

```
no service-policy input | output
```

```
service-policy {input | output} policy-map-name
```

Parameters

- input—Specifies an ingress policy.
- output—Specifies an egress policy.
- policy-map-name—Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)
- default-action—Specifies the default action. If the keyword is not configured then the deny-any default action is applied.
- deny-any—Deny all the packets (which were ingress of the port) that do not meet the rules in a policy.
- permit-any—Forward all the packets (which were ingress of the port) that do not meet the rules in a policy.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Default

Policy map is not bound.

User Guidelines

This command is only available in QoS advanced mode.

Only one policy map per interface per direction is supported.

If the policy map includes the police command a separate copy of the policy map rules is created in TCAM for each Ethernet port.

An egress policy cannot support the following actions:

- set with the queue keyword
- trust
- redirect
- mirror
- police

The service-policy output command fails if the bound policy contains actions not supported by egress policies.

A policy map cannot be bound as input and output at the same time.

Example

The following example attaches a policy map called Policy1 to the input interface.

```
ZEQU0xxxxDL(config-if)# service-policy input policy1
```

The following example attaches a policy map called Policy1 to the input interface and forwards all packets that do not meet the rules of the policy.

```
ZEQU0xxxxDL(config-if)# service-policy input policy1 permit-any
```

The following example attaches a policy map called Policy2 to the output interface.

```
ZEQU0xxxxDL(config-if)# service-policy output policy2
```

34.16 mls qos aggregate-policer

Use the mls qos aggregate-policer Global Configuration mode command to define the policer parameters that can be applied to multiple traffic classes. Use the no form of this command to remove an existing aggregate policer.

Syntax

```
mls qos aggregate-policer aggregate-policer-name committed-rate-kbps  
committed-burst-byte [exceed-action action] [peak peak-rate-kbps  
peak-burst-byte [violate-action action]]
```

```
no qos aggregate-policer aggregate-policer-name
```

Parameters

- aggregate-policer-name—Specifies the aggregate policer name. (Length: 1–32 characters)
- committed-rate-kbps—Specifies the average traffic rate (CIR) in kbits per second (bps). (Range: 3–57982058)
- committed-burst-byte—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- exceed-action—Specifies the action taken when the committed rate is exceeded and the peak rate is not exceeded. If the keyword is not configured then the following action is applied:
 - drop, if peak the keyword is not configured.
 - policed-dscp-transmit, if peak the keyword is configured.
- peak—Specifies the Two-rate Three-color policer. If the peak rate is exceeded the packet is dropped.
- peak-rate-kbps—Specifies the average traffic rate (CIR) in kbits per second (bps). (Range: 3–57982058)
- peak-burst-byte—Specifies the peak burst size (PBS) in bytes. (Range: 3000–19173960)
- violate-action—Specifies the action taken when the peak rate is exceeded. If the keyword is not configured then the drop action is applied.
- action—Specifies the taken action. The possible values are:
 - drop—Drops the packet.
 - policed-dscp-transmit—Remarks the packet DSCP of IP traffic. The DSCP remarking is configured by the qos map policed-dscp command with the violation keyword for the violation action and without this keyword for the exceed action. DSCP remarking will have effect only if the mode is trust dscp.

Default Configuration
No aggregate policer is defined.

Command Mode
Global Configuration mode

User Guidelines

This command is only available when QoS is in advanced mode.

Use the `mls qos aggregate-policer` command to define a policer that aggregates traffic from multiple class maps.

Aggregate policers cannot aggregate traffic from multiple devices. If the aggregate policer is applied to more than one device, the traffic on each device is counted separately and is limited per device.

Traffic from two different ports on the same device can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be deleted if it is being used in a policy map. The `no police aggregate Policy-map Class Configuration mode` command must first be used to delete the aggregate policer from all policy maps before using the `no qos aggregate-policer` command.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket. CBS represents the depth of the bucket.

Examples

Example 1. The following example defines the parameters of a policer called `policer1` that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
ZEQU0xxxxDL(config)# mls qos aggregate-policer policer1 124000 9600 exceed-action drop
```

Example 2. The following example defines the parameters of a Two-rate Three-color policer called `policer2` that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is remarked. When the average traffic rate exceeds 200,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
ZEQU0xxxxDL(config)# mls qos aggregate-policer policer2 124000 9600 exceed-action  
policed-dscp-transmit peak 200000 19200 violate-action policed-dscp-transmit
```

34.17 **show mls qos aggregate-policer**

Use the show mls qos aggregate-policer Privileged EXEC mode command to display aggregate policers

This command is only available in QoS advanced mode.

Syntax

show mls qos aggregate-policer [aggregate-policer-name]

Parameters

aggregate-policer-name—Specifies the aggregate policer name. (Length: 1–32 characters)

Default Configuration

All policers are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the parameters of the aggregate Two-rate Three-color policer called Policer1.

```
ZEQU0xxxxDL# show mls qos aggregate-policer policer1
```

```
aggregate-policer policer1 124000 9600 exceed-action policed-dscp-transmit peak 200000 19200  
violate-action policed-dscp-transmit not used by any policy map.
```

34.18 police aggregate

Use the police aggregate Policy-map Class Configuration mode. command to apply an aggregate policer to multiple class maps within the same policy map. Use the no form of this command to remove an existing aggregate policer from a policy map.

This command is only available in QoS advanced mode.

Syntax

police aggregate aggregate-policer-name

no police aggregate aggregate-policer-name

Parameters

aggregate-policer-name—Specifies the aggregate policer name. (Length: 1–32 characters)

Command Mode

Policy-map Class Configuration mode.

User Guidelines

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps or interfaces.

Use the exit command to return to the Configuration mode. Use the end command to return to the Privileged EXEC mode.

Example

The following example applies the aggregate policer called Policer1 to a class called class1 in a policy map called policy1 and class2 in policy map policy2.

```
ZEQU0xxxxDL(config)# qos aggregate-policer policer1 124000 9600 exceed-action drop
ZEQU0xxxxDL(config)# policy-map policy1
ZEQU0xxxxDL(config-pmap)# class class1
ZEQU0xxxxDL(config-pmap-c)# police aggregate policer1
ZEQU0xxxxDL(config-pmap-c)# exit
ZEQU0xxxxDL(config-pmap)# exit
ZEQU0xxxxDL(config)# policy-map policy2
ZEQU0xxxxDL(config-pmap)# class class2
ZEQU0xxxxDL(config-pmap-c)# police aggregate policer1
```

34.19 **wrr-queue cos-map**

Use the `wrr-queue cos-map` Global Configuration mode command to map Class of Service (CoS) values to a specific egress queue. Use the `no` form of this command to restore the default configuration.

Syntax

```
wrr-queue cos-map queue-id cos0... cos7
```

```
no wrr-queue cos-map [queue-id]
```

Parameters

- `queue-id`—Specifies the queue number to which the CoS values are mapped.
- `cos0... cos7`—Specifies up to 8 CoS values to map to the specified queue number. (Range: 0–7)

Default Configuration

The default CoS value mapping to 8 queues is as follows:

CoS value 0 is mapped to queue 1.

CoS value 1 is mapped to queue 1.

CoS value 2 is mapped to queue 2.

CoS value 3 is mapped to queue 5.

CoS value 4 is mapped to queue 4.

CoS value 5 is mapped to queue 7.

CoS value 6 is mapped to queue 7

CoS value 7 is mapped to queue 6

Command Mode

Global Configuration mode

User Guidelines

Use this command to distribute traffic to different queues.

Example

The following example maps CoS value 4 and 6 to queue 2.

```
ZEQU0xxxxDL (config)# wrr-queue cos-map 2 4 6
```

34.20 wrr-queue bandwidth

Use the wrr-queue bandwidth Global Configuration mode command to assign Weighted Round Robin (WRR) weights to egress queues. The weight ratio determines the frequency at which the packet scheduler removes packets from each queue. Use the no form of this command to restore the default configuration.

Syntax

wrr-queue bandwidth weight1 weight2... weighting

no wrr-queue bandwidth

Parameters

weight1 weight1... weighting the ratio of bandwidth assigned by the WRR packet scheduler to the packet queues. See explanation in the User Guidelines. Separate each value by a space. (Range for each weight: 0–255)

Default Configuration

wrr is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue.

A weight of 0 indicates that no bandwidth is allocated for the same queue, and the shared bandwidth is divided among the remaining queues. It is not recommended to set the weight of a queue to a 0 as it might stop transmission of control-protocols packets generated by the device.

All queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

An expedite queue is a priority queue, which is serviced until empty before the other queues are serviced. The expedite queues are designated by the priority-queue out num-of-queues command.

Example

The following assigns WRR values to the queues.

```
ZEQU0xxxxDL(config)# priority-queue out num-of-queues 0
ZEQU0xxxxDL(config)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

34.21 **priority-queue out num-of-queues**

Use the `priority-queue out num-of-queues` Global Configuration mode command to configure the number of expedite queues. Use the `no` form of this command to restore the default configuration.

Syntax

`priority-queue out num-of-queues number-of-queues`

`no priority-queue out num-of-queues`

Parameters

- `number-of-queues`—Specifies the number of expedite (strict priority) queues. Expedite queues are assigned to the queues with the higher indexes. (Range: 0–8 .There must be either 0 `wrr` queues or more than one.

If `number-of-queues = 0`, all queues are assured forwarding (according to `wrr` weights) If the `number-of-queues = 8` , all the queues are expedited (strict priority queues).

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

An expedite queue is a strict priority queue, which is serviced until empty before the other lower priority queues are serviced.

the weighted round robin (WRR) weight ratios are affected by the number of expedited queues, because there are fewer queues participating in WRR. This indicates that the corresponding weight in the `wrr-queue bandwidth` Interface Configuration mode command is ignored (not used in the ratio calculation).

Example

The following example configures the number of expedite queues as 2.

```
ZEQU0xxxxDL (config)# priority-queue out num-of-queues 2
```

34.22 traffic-shape

Use the traffic-shape Interface (Ethernet, Port Channel) Configuration mode command to configure the egress port shaper. Use the no form of this command to disable the shaper.

Syntax

traffic-shape committed-rate [committed-burst]

no traffic-shape

Parameters

- committed-rate—Specifies the maximum average traffic rate (CIR) in kbits per second (kbps). (Range: FE, GE: 64kbps–maximum port speed ,10GE: 64Kbps–maximum port speed))
- committed-burst—Specifies the maximum permitted excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The egress port shaper controls the traffic transmit rate (Tx rate) on a port.

Example

The following example sets a traffic shaper on gi1/0/1 when the average traffic rate exceeds 64 kbps or the normal burst size exceeds 4096 bytes.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# traffic-shape 64 4096
```

34.23 traffic-shape queue

Use the traffic-shape queue Interface (Ethernet, Port Channel) Configuration mode command to configure the egress queue shaper. Use the no form of this command to disable the shaper.

Syntax

traffic-shape queue queue-id committed-rate [committed-burst]

no traffic-shape queue queue-id

Parameters

queue-id—Specifies the queue number to which the shaper is assigned. (Range: 1-8).

- committed-rate—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 64 kbps–maximum port speed)
- committed-burst—Specifies the excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The egress port shaper controls the traffic transmit rate (Tx rate) on a queue on a port.

Example

The following example sets a shaper on queue 1 on gi1/0/1 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# traffic-shape queue 1 64 4096
```

34.24 mls qos wrr-queue wrtd

Use the mls qos wrr-queue wrtd Global Configuration mode command to enable Weighted Random Tail Drop (WRTD). Use the no form of this command to disable WRTD.

Syntax

mls qos wrr-queue wrtd

no mls qos wrr-queue wrtd

Parameters

N/A

Default

Disabled

Command Mode

Global Configuration mode

User Guidelines

The command is effective after reset.

Example

```
ZEQU0xxxxDL(config)# mls qos wrr-queue wrtd
```

This setting will take effect only after copying running configuration to startup configuration and resetting the device

```
ZEQU0xxxxDL(config)#
```

34.25 **show mls qos wrr-queue wrtd**

Use the show mls qos wrr-queue wrtd Privileged EXEC mode command to display the Weighted Random Tail Drop (WRTD) configuration.

Syntax

```
show mls qos wrr-queue wrtd
```

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
ZEQU0xxxxDL (config)# show mls qos wrr-queue wrtd  
Weighted Random Tail Drop is disabled  
Weighted Random Tail Drop will be enabled after reset
```

34.26 **show mls qos interface**

Use the show mls qos interface Privileged EXEC mode command to display Quality of Service (QoS) information on the interface.

Syntax

```
show mls qos interface [buffers | queueing | policers | shapers] [interface-id]
```

Parameters

- **buffers**—Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the queues. For FE ports, displays the minimum reserved setting.
- **queueing**—Displays the queue's strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- **policers**—Displays all the policers configured for this interface, their settings, and the number of policers currently unused (on a VLAN).
- **shapers**—Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, or Port-channel.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

If no parameter is specified with the show mls qos interface command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so on), default CoS value, DSCP-to-DSCP- map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

In case of Policers, Shapers and Rate Limit - only the ports which are not in the default configuration will be showed.

Examples

Example 1—The following is an example of the output from the show mls qos interface command.

```
ZEQU0xxxxDL(config)# show mls qos interface gi1/0/1
Ethernet gi1/0/1
Default CoS: 0
Default ACE ingress action: deny-all
Default ACE egress action: deny-all
```

Example 2—The following is an example of the output from the show mls qos interface queueing command for 4 queues.

```
ZEQU0xxxxDL(config)# show mls qos interface queueing gi1/0/1
Ethernet gi1/0/0/1
wrr bandwidth weights and EF priority:
qid-weights      Ef - Priority
1 - N/A          ena- 1
2 - N/A          ena- 2
3 - N/A          ena- 3
4 - N/A          ena- 4
5 - N/A          ena- 5
6 - N/A          ena- 6
7 - N/A          ena- 7
8 - N/A          ena- 8
Cos-queue map:
cos-qid
0 - 1
1 - 1
2 - 2
3 - 5
4 - 4
5 - 7
6 - 7
7 - 6
```

Example 3 —The following an example of the output from the show mls qos interface buffers command for 8 queues

```
ZEQU0xxxxDL (config)# show mls qos interface buffers gi1/0/1
```

```
Ethernet gi1/0/1
```

qid	thresh0	thresh1	thresh2
1	100	100	80
2	100	100	80
3	100	100	80
4	100	100	80
5	100	100	80
6	100	100	80
7	100	100	80
8	100	100	80

Example 4—This is an example of the output from the show mls qos interface shapers command.

```
ZEQU0xxxxDL (config)# show mls qos interface shapers gi1/0/1
```

```
Ethernet gi1/0/1
```

```
Port shaper: enable
```

```
Committed rate: 192000 bps
```

```
Committed burst: 9600 bytes
```

qid	Status	Target Committed Rate [bps]	Target Committed Burst [bytes]
1	Enable	100000	17000
2	Disable	N/A	N/A
3	Enable	200000	19000
4	Disable	N/A	N/A
5	Disable	N/A	N/A
6	Disable	N/A	N/A
7	Enable	178000	8000
8	Enable	23000	1000

Example 5—This is an example of the output from show mls qos interface policer

```
ZEQU0xxxxDL(config)# show mls qos interface policer gi1/0/1
Ethernet gi1/0/1
Ingress Policers:
Class map: A
Policer type: aggregate
Committed rate: 19200 bps
Committed burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Class map: B
Policer type: single
Committed rate: 19200 bps
Committed burst: 9600 bytes
Peak rate: 25600 bps
Peak burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Violate-action: drop
Class map: C
Policer type: none
Egress Policers:
Class map: D
```

34.27 mls qos map policed-dscp

Use the qos map policed-dscp Global Configuration mode command to configure the policed-DSCP map for remarking purposes. Use the no form of this command to restore the default configuration.

Syntax

mls qos map policed-dscp [violation] dscp-list to dscp-mark-down

no mls qos map policed-dscp [violation] [dscp-list]

Parameters

- violation—Specifies the DSCP remapping in the violate action. If the keyword is not configured the the command specifies the DSCP remapping in the exceed action.
- dscp-list—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- dscp-mark-down—Specifies the DSCP value to mark down. (Range: 0–63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode

User Guidelines

The original DSCP value and policed-DSCP value must be mapped to the same queue in order to prevent reordering.

Example

The following example marks incoming DSCP value 3 as DSCP value 5 on the policed-DSCP map.

```
ZEQU0xxxxDL(config)# mls qos map policed-dscp 3 to 5
```

34.28 mls qos map dscp-queue

Use the qos map dscp-queue Global Configuration mode command to configure the DSCP to queue map. Use the no form of this command to restore the default configuration.

Syntax

mls qos map dscp-queue dscp-list to queue-id

no mls qos map dscp-queue [dscp-list]

Parameters

- dscp-list—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- queue-id—Specifies the queue number to which the DSCP values are mapped.

Default Configuration

The default map for 8 queues is as follows.

DSCP value	9-15	0-8	17 - 23	32,41-47	25-31	33-39	16,24,40,48-63	None
Queue-I D	2	1	3	7	4	5	6	8

Command Mode

Global Configuration mode

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
ZEQU0xxxxDL(config)# mls qos map dscp-queue 33 40 41 to 1
```

34.29 mls qos trust (Global)

Use the `mls qos trust` Global Configuration mode command to configure the system to the basic mode and trust state. Use the `no` form of this command to return to the default configuration.

Syntax

```
mls qos trust {cos | dscp}  
no mls qos trust
```

Parameters

- `cos`— Specifies that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- `dscp`— Specifies that ingress packets are classified with packet DSCP values.

Default Configuration

`dscp`

Command Mode

Global Configuration mode

User Guidelines

This command can be used only in QoS basic mode.

Packets entering a QoS domain are classified at its edge. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-queue map.

When the system is configured with trust CoS, the traffic is mapped to the queue by the CoS-queue map.

For an inter-QoS domain boundary, configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different in the QoS domains.

Example

The following example configures the system to the DSCP trust state.

```
ZEQU0xxxxDL(config)# mls qos trust dscp
```

34.30 mls qos trust (Interface)

Use the mls qos trust Interface (Ethernet, Port Channel) Configuration mode command to enable port trust state while the system is in the basic QoS mode. Use the no form of this command to disable the trust state on each port.

Syntax

mls qos trust

no mls qos trust

Parameters

N/A

Default Configuration

Each port is enabled while the system is in basic mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures gi1/0/1 to the default trust state.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# mls qos trust
```

34.31 mls qos cos

Use the qos cos Interface (Ethernet, Port Channel) Configuration mode command to define the default CoS value of a port. Use the no form of this command to restore the default configuration.

Syntax

mls qos cos default-cos

no mls qos cos

Parameters

default-cos—Specifies the default CoS value (VPT value) of the port. If the port is trusted and the packet is untagged, then the default CoS value become the CoS value. (Range: 0–7)

Default Configuration

The default CoS value of a port is 0.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the default CoS value to assign a CoS value to all untagged packets entering the interface.

Example

The following example defines the port gi1/0/1 default CoS value as 3.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# mls qos cos 3
```

34.32 mls qos dscp-mutation

Use the mls qos dscp-mutation Global Configuration mode command to apply the DSCP Mutation map to system DSCP trusted ports. Use the no form of this command to restore the trusted port with no DSCP mutation.

Syntax

mls qos dscp-mutation

no mls qos dscp-mutation

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

Apply the DSCP-to-DSCP-mutation map to a port at the boundary of a Quality of Service (QoS) administrative domain. If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. Apply the map to ingress and to DSCP-trusted ports only. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports. If applying the DSCP mutation map to an untrusted port, to class of service (CoS), or to an IP-precedence trusted port.

Global trust mode must be DSCP or CoS-DSCP. In advanced CoS mode, ports must be trusted.

Example

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
ZEQU0xxxxDL(config)# mls qos dscp-mutation
```

34.33 mls qos map dscp-mutation

Use the `mls qos map dscp-mutation` Global Configuration mode command to configure the DSCP to DSCP Mutation table. Use the `no` form of this command to restore the default configuration.

Syntax

`mls qos map dscp-mutation in-dscp to out-dscp`

`no mls qos map dscp-mutation [in-dscp]`

Parameters

- `in-dscp`—Specifies up to 8 DSCP values to map, separated by spaces. (Range: 0–63)
- `out-dscp`—Specifies up to 8 DSCP mapped values, separated by spaces. (Range: 0–63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode

User Guidelines

This is the only map that is not globally configured. It is possible to have several maps and assign each one to a different port.

Example

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
ZEQU0xxxxDL(config)# mls qos map dscp-mutation 1 2 4 5 6 to 63
```

34.34 show mls qos map

Use the `show mls qos map` Privileged EXEC mode command to display the various types of QoS mapping.

Syntax

```
show mls qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]
```

Parameters

- `dscp-queue`—Displays the DSCP to queue map.
- `dscp-dp`—Displays the DSCP to Drop Precedence map.
- `policed-dscp`—Displays the DSCP to DSCP remark table.
- `dscp-mutation`—Displays the DSCP-DSCP mutation table.

Default Configuration

Display all maps.

Command Mode

Privileged EXEC mode

Examples

Example 1. The following example displays the QoS mapping information:

```
ZEQU0xxxxDL (conf ig)# show mls qos map dscp-queue
```

Dscp-queue map:

```

d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   01 01 01 01 01 01 01 01 01 01
1 :   01 01 01 01 01 01 02 02 02 02
2 :   02 02 02 02 02 02 02 02 02 02
3 :   02 02 03 03 03 03 03 03 03 03
4 :   03 03 03 03 03 03 03 03 04 04
5 :   04 04 04 04 04 04 04 04 04 04
6 :   04 04 04 04
```

Example 2. The following example displays the dscp remapping information:

ZEQU0xxxxDL (config) # show mls qos map policed-dscp

Policed-dscp (Exceed) map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

0 : 00 01 02 03 04 05 06 07 08 09

1 : 10 11 12 13 14 15 16 17 18 19

2 : 20 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

6 : 21 21 21

Policed-dscp (Violate) map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

0 : 00 01 02 03 04 05 06 07 08 09

1 : 10 11 12 13 14 15 16 17 18 19

2 : 20 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

6 : 11 11 11

34.35 clear mls qos statistics

Use the clear mls qos statistics Privileged EXEC mode command to clear the QoS statistics counters.

Syntax

clear mls qos statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example clears the QoS statistics counters.

```
ZEQU0xxxxDL (config)# clear mls qos statistics
```

34.36 mls qos statistics policer

Use the mls qos statistics policer Interface (Ethernet, Port Channel) Configuration mode mode command to enable counting in-profile and out-of-profile. Use the no form of this command to disable counting.

This command is relevant only when policers are defined.

Syntax

mls qos statistics policer policy-map-name class-map-name

no mls qos statistics policer policy-map-name class-map-name

Parameters

- policy-map-name—Specifies the policy map name. (Length: 1–32 characters)
- class-map-name—Specifies the class map name. (Length: 1–32 characters)

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# mls qos statistics policer policy1 class1
```

34.37 **mls qos statistics aggregate-policer**

Use the `mls qos statistics aggregate-policer` Global Configuration mode command to enable counting in-profile and out-of-profile. Use the `no` form of this command to disable counting.

Syntax

`mls qos statistics aggregate-policer aggregate-policer-name`

`no mls qos statistics aggregate-policer aggregate-policer-name`

Parameters

`aggregate-policer-name`—Specifies the aggregate policer name. (Length: 1–32 characters)

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Global Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
ZEQU0xxxxDL(config)# mls qos statistics aggregate-policer policer1
```

34.38 **clear queue statistics**

Use the clear queue statistics Privileged EXEC mode command to clear the queue statistics.

Syntax

clear queue statistics [interface-id]

Parameters

- interface-id—Specifies an Ethernet port which queue statistics are cleared.

Command Mode

Privileged EXEC mode

User Guidelines

Use the clear queue statistics interface-id command to clear the queue statistics of the given port.

Use the clear queue statistics command to clear the queue statistics of all ports.

Example

The following example clears queue statistics of Ethernet port gi1/0/2:

```
ZEQU0xxxxDL# clear queue statistics gi1/0/2
```

34.39 show queue statistics

Use the show queue statistics Privileged EXEC mode command to display the queue statistics.

Syntax

show queue statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use the show queue statistics interface-id command to display the queue statistics of the given port.

Use the show queue statistics command to display the queue statistics of all ports.

Example

The following example displays queue statistics of Ethernet port gi1/0/2:

ZEQU0xxxxDL# show queue statistics

Policers

Interface	Policy map	Class Map	In-profile bytes	Out-of-profile bytes
gi1/0/1	Policy1	Class1	756457	12
gi1/0/1	Policy1	Class2	87591	12
gi1/0/2	Policy1	Class1	75457	2
gi1/0/2	Policy1	Class2	5326	12

Aggregate Policers

Name	In-profile bytes	Out-of-profile bytes
Policer	756457	12

34.40 show mls qos statistics

Use the show mls qos statistics Privileged EXEC mode command to display Quality of Service statistical information.

Syntax

show mls qos statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use the show mls qos statistics command to display QoS statistics.

Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Example

The following example displays Quality of Service statistical information.

```
ZEQU0xxxxDL (config)# show mls qos statistics
```

Policers

Interface	Policy map	Class Map	In-profile bytes	Out-of-profile bytes

gi1/0/1	Policy1	Class1	756457	12
gi1/0/1	Policy1	Class2	87591	12
gi1/0/2	Policy1	Class1	75457	2
gi1/0/2	Policy1	Class2	5326	12

Aggregate Policers

Name	In-profile bytes	Out-of-profile bytes
Policer	756457	12

35 RADIUS Commands

35.1 radius-server host

Use the radius-server host Global Configuration mode command to configure a RADIUS server host. Use the no form of the command to delete the specified RADIUS server host.

Syntax

```
radius-server host {ip-address | hostname} [auth-port auth-port-number] [acct-port  
acct-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key  
key-string] [priority priority] [usage login]
```

```
no radius-server host {ip-address | hostname}
```

Parameters

- ip-address—Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.
- hostname—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length of each part of the hostname: 63 characters)
- auth-port auth-port-number—Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- acct-port acct-port-number—Port number for accounting requests. The host is not used for accountings if set to 0. If unspecified, the port number defaults to 1813.
 - timeout timeout—Specifies the timeout value in seconds. (Range: 1–30)
- retransmit retries—Specifies the number of retry retransmissions (Range: 1–15)
 - deadtime deadtime—Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)
- key key-string—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters). If this parameter is omitted, the globally-configured radius key will be used.
- priority priority—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)
- usage login— login—Specifies that the RADIUS server is used for user login parameters authentication.

Default Configuration

The default authentication port number is 1812.

If timeout is not specified, the global value (set in the radius-server timeout command) is used.

If retransmit is not specified, the global value (set in the radius-server retransmit command) is used.

If key-string is not specified, the global value (set in the radius-server key command) is used.

If the usage keyword is not specified, the all argument is applied.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, this command is used for each host.

Example

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
ZEQU0xxxxDL (config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

35.2 radius-server key

Use the radius-server key Global Configuration mode command to set the authentication key for RADIUS communications between the device and the RADIUS daemon. Use the no form of this command to restore the default configuration.

Syntax

radius-server key [key-string]

no radius-server key

Parameters

- key-string—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0–128 characters)

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

Example

The following example defines the authentication key for all RADIUS communications between the device and the RADIUS daemon.

```
ZEQU0xxxxDL (config)# radius-server key enterprise-server
```

35.3 radius-server retransmit

Use the radius-server retransmit Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.

Syntax

radius-server retransmit retries

no radius-server retransmit

Parameters

- retransmit retries—Specifies the number of retry retransmissions (Range: 1–15).

Default Configuration

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

Example

The following example configures the number of times the software searches all RADIUS server hosts as 5.

```
ZEQU0xxxxDL (config) # radius-server retransmit 5
```

35.4 radius-server host source-interface

Use the radius-server host source-interface Global Configuration mode command to specify the source interface whose IPv4 address will be used as the Source IPv4 address for communication with IPv4 RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax

radius-server host source-interface interface-id

no radius-server host source-interface

Parameters

- interface-id—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 RADIUS server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 100 as the source interface.

```
ZEQU0xxxxDL (config) # radius-server host source-interface vlan 100
```

35.5 radius-server host source-interface-ipv6

Use the radius-server host source-interface-ipv6 Global Configuration mode command to specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax

radius-server host source-interface-ipv6 interface-id

no radius-server host source-interface-ipv6

Parameters

- interface-id—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 RADIUS server.

Example

The following example configures the VLAN 100 as the source interface.

```
ZEQU0xxxxDL (config)# radius-server host source-interface-ipv6 vlan 100
```

35.6 radius-server timeout

Use the radius-server timeout Global Configuration mode command to set how long the device waits for a server host to reply. Use the no form of this command to restore the default configuration.

Syntax

radius-server timeout timeout-seconds

no radius-server timeout

Parameters

- timeout timeout-seconds—Specifies the timeout value in seconds. (Range: 1–30).

Default Configuration

The default timeout value is 3 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout interval on all RADIUS servers to 5 seconds.

```
ZEQU0xxxxDL (config) # radius-server timeout 5
```

35.7 radius-server deadtime

Use the radius-server deadtime Global Configuration mode command to configure how long unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the no form of this command to restore the default configuration.

Syntax

radius-server deadtime deadtime

no radius-server deadtime

Parameters

- **deadtime**—Specifies the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000).

Default Configuration

The default deadtime interval is 0.

Command Mode

Global Configuration mode

Example

The following example sets all RADIUS server deadtimes to 10 minutes.

```
ZEQU0xxxxDL(config)# radius-server deadtime 10
```

35.8 show radius-servers

Use the show radius-servers Privileged EXEC mode command to display the RADIUS server settings.

Syntax

show radius-servers

Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server settings:

ZEQU0xxxxDL# show radius-servers								
IP address	Port	Port	Time-	Ret-	Dead-	Prio. Usage		
	Auth	Acc	Out	rans	time			
-----	----	----	----	-----	-----	-----	-----	-----
172. 16. 1. 1	1812	1813	125	Global	Global	1	All	
172. 16. 1. 2	1812	1813	102	8	Global	2	All	
Global values								

TimeOut: 3								
Retransmit: 3								
Deadtime: 0								
Source IPv4 interface: vlan 120								
Source IPv6 interface: vlan 10								

35.9 show radius-servers key

Use the show radius-servers key Privileged EXEC mode command to display the RADIUS server key settings.

Syntax

show radius-servers key

Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server key settings.

```
ZEQU0xxxxDL# show radius-servers key
```

IP address	Key
172.16.1.1	Sharon123
172.16.1.2	Bruce123
Alice456	

36 Rate Limit and Storm Control Commands

36.1 clear storm-control counters

To clear storm control counters, use the clear storm-control counters command in Privileged EXEC mode.

Syntax

clear storm-control counters [broadcast | multicast | unicast] [interface interface-id]

Parameters

- broadcast—(Optional) Clear Broadcast storm control counters.
- multicast—(Optional) Clear Multicast storm control counters.
- unicast—(Optional) Clear Unicast Unknown storm control counters.
- interface interface-id—(Optional) Clear storm control counters for the specified Ethernet port.

Command Mode

Privileged EXEC mode

User Guidelines

The switch clears the port counter of a given traffic type when storm control for this traffic type on this port is enabled.

Use this command to clear the storm control counters when storm control is running.

Use the clear storm-control counters command to clear all the storm control counters of all Ethernet ports.

Use the clear storm-control counters interface interface-id command to clear all the storm control counters of a given port.

Use the clear storm-control counters broadcast | multicast | unicast command to clear all storm control counters of a given traffic type of all Ethernet ports.

Use the clear storm-control counters broadcast | multicast | unicast interface interface-id command to clear one storm control counter of a given traffic type and of a given port.

Example

Example 1. The following example clears all storm control counters of all ports:

```
ZEQU0xxxxDL# clear storm-control counters
```

Example 2. The following example clears all storm control counters of port gi1/0/1:

```
ZEQU0xxxxDL# clear storm-control counters interface gi1/0/1
```

Example 3. The following example clears broadcast storm control counter of all ports:

```
ZEQU0xxxxDL# clear storm-control counters broascat
```

Example 4. The following example clears multicast storm control counter of port gi1/0/1:

```
ZEQU0xxxxDL# clear storm-control counters multicast interface gi1/0/1
```

36.2 rate-limit (Ethernet)

To limit the incoming traffic rate on a port, use the rate-limit command in Interface (Ethernet) Configuration mode. To disable the rate limit, use the no form of this command.

Syntax

rate-limit committed-rate-kbps [burst committed-burst-bytes]

no rate-limit

Parameters

- committed-rate-kbps—Specifies the maximum number of kilobits per second of ingress traffic on a port. The range is 3–maximal port speed.
- burst committed-burst-bytes—(Optional) The burst size in bytes. (Range: 3000–19173960). If unspecified, defaults to 128K.

Default Configuration

Rate limiting is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

The Rate Limit does not calculate traffic controlled by Storm control. The real allowed rate will be sum of the rate specified by the command and the rates specified by the Storm control commands for particular traffic types.

Example

The following example limits the incoming traffic rate on gi1/0/1 to 150,000 kbps.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# rate-limit 150000
```

36.3 rate-limit vlan

To limit the incoming traffic rate for a VLAN in, use the rate-limit vlan command in Global Configuration mode. To disable the rate limit, use the no form of this command.

Syntax

rate-limit vlan vlan-id committed-rate [burst committed-burst-bytes]

no rate-limit vlan vlan-id

Parameters

- vlan-id—Specifies the VLAN ID.
- committed-rate—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3-57982058)
- burst committed-burst—(Optional) Specifies the maximum burst size (CBS) in bytes. (Range: 3000–19173960). If unspecified, defaults to 128K.

Default Configuration

Rate limiting is disabled.

Command Mode

Global Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Traffic policing in a policy map takes precedence over VLAN rate limiting. If a packet is subject to traffic policing in a policy map and is associated with a VLAN that is rate limited, the packet is counted only in the traffic policing of the policy map.

It does not work in conjunction with IP Source Guard.

Example

The following example limits the rate on VLAN 11 to 150000 kbps or the normal burst size to 9600 bytes.

```
ZEQU0xxxxDL(config)# rate-limit vlan 11 150000 burst 9600
```

36.4 storm-control

To enable broadcast, multicast, or unicast storm control on a port, use the storm-control command in Interface (Ethernet) Configuration mode. To return to default, use the no form of this command.

Syntax

storm-control broadcast {level level | kbps kbps} [trap] [shutdown]

no storm-control broadcast

storm-control multicast [registered | unregistered] {level level | kbps kbps} [trap] [shutdown]

no storm-control multicast

storm-control unicast {level level | kbps kbps} [trap] [shutdown]

no storm-control unicast

no storm-control

Parameters

- broadcast—Enables broadcast storm control on the port.
- multicast [registered | unregistered]—Enables ether all multicast, only registered multicast, or only unregistered multicast storm control on the port.
- unicast—Enables unicast unknown storm control on the port.
- level level—Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1-100)
- kbps kbps—Maximum of kilobits per second of Broadcast traffic on a port. (Range 1–10000000)
- trap—(Optional) Sends a trap when a storm occurs on a port. If the keyword is not specified the trap is not sent.
- shutdown—(Optional) Shut down a port when a storm occurs on the port. If the keyword is not specified extra traffic is discarded.

Default Configuration

Storm control is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead

(preamble+SFD+IPG).

The rate limit on a port does not calculate traffic controlled by storm control on this port.

Use the no storm-control command to disable storm control of all traffic type on the port.

You can use the following commands to reset an interface shut down by Storm Control:

- The errdisable recovery reset command with the interface interface-id parameter to reset a given interface.
- The errdisable recovery cause with the storm-control parameter to automatically recover from the Storm Control error-disabled state.

Example

The following example enables broadcast, multicast, and unicast unknown storm control on port gi1/0/1 and multicast unregistered and unicast unknown on port gi1/0/2:

Enable group 1 for registered and unregistered multicast traffic on interface gi1/0/1. Extra traffic is discarded.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# storm-control broadcast kbps 10000 shutdown
ZEQU0xxxxDL(config-if)# storm-control multicast level 20 trap
ZEQU0xxxxDL(config-if)# storm-control unicast level 5 trap shutdown
ZEQU0xxxxDL(config-if)# exit
ZEQU0xxxxDL(config)# interface gi1/0/2
ZEQU0xxxxDL(config-if)# storm-control multicast unregistered level 5 trap shutdown
ZEQU0xxxxDL(config-if)# storm-control unicast level 5 trap
ZEQU0xxxxDL(config-if)# exit
```

36.5 show mls qos rate-limit interface

To display mls qos rate limit configuration on an interface, use the show mls qos rate-limit interface command in Privileged EXEC mode.

Syntax

show mls qos rate-limit interface [interface-id]

Parameters

- interface-id—(Optional) Specifies an Ethernet port. If the argument is not configured rate limit configuration of all Ethernet ports is displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the show mls qos rate-limit interface:

ZEQU0xxxxDL> show mls qos rate-limit interface		
Interface	Rate Limit (kbps)	Burst (Bytes)
gi1/0/1	N/A	128000
gi1/0/2	N/A	128000
	.	
	.	
	.	
te1/0/27	N/A	128000
te1/0/28	N/A	128000

36.6 show mls qos rate-limit vlan

To display mls qos rate limit configuration on a VLAN, use the show rate-limit vlan command in Privileged EXEC mode.

Syntax

show mls qos rate-limit vlan [vlan-id]

Parameters

- vlan-id—(Optional) Specifies a VLAN ID If the argument is not configured rate limit configuration of all VLANs is displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the show rate-limit vlan:

ZEU0xxxxDL> show mls qos rate-limit vlan 1075		
VLAN	rate-limit [kbps]	burst [Bytes]
1075	100000	1024

36.7 show storm-control interface

To display storm control information of an interface, use the show storm-control interface command in Privileged EXEC mode.

Syntax

```
show storm-control interface [interface-id]
```

Parameters

- interface-id—(Optional) Specifies an Ethernet port. If the argument is not configured storm control information of all Ethernet ports is displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the show storm-control interface:

```
ZEQU0xxxxDL> show storm-control interface
```

```
gi1/0/1
```

```
  Broadacst
```

```
    Rate: 5%
```

```
    Action: Shutdown
```

```
    Passed Counter (Bytes): 124997
```

```
    Dropped Counter (Bytes): 10
```

```
    Last drop time: 27-Jan-2019, 09:00:01
```

```
  Multicast
```

```
    Rate: 1000 kbps
```

```
    Action: Drop, Trap
```

```
    Passed Counter (Bytes):112876
```

```
    Dropped Counter (Bytes):1272
```

```
    Last drop time: 20-Jan-2019, 11:00:01
```

```
  Unicast
```

```
    Rate: 10%
```

```
    Action: drop
```

```
    Passed Counter (Bytes): 27653
```

```
    Dropped Counter (Bytes):1
```

```
    Last drop time: 27-Feb-2019, 09:00:01
```

```
gi1/0/2
```

```
  Broadacst
```

```
    Rate: 5%
```

```
    Action: Shutdown
```

```
    Passed Counter (Bytes): 124997
```

```
    Dropped Counter (Bytes): 0
```

```
    Last drop time:
```

```
  Multicast Unregistred
```

```
    Rate: 5%
```

```
    Action: Shutdown
```

```
    Traffic Type:Broadcast
```

```
    Passed Counter (Bytes): 124997
```

```
    Dropped Counter (Bytes): 3
```

```
    Last drop time: 26-Jan-2019, 10:00:01
```

37 Remote Network Monitoring (RMON)

Commands

37.1 rmon alarm

To configure alarm conditions, use the rmon alarm Global Configuration modecommand. To remove an alarm, use the no form of this command.

Syntax

```
rmon alarm index mib-object-id interval rising-threshold falling-threshold  
rising-event falling-event [type {absolute | delta}] [startup {rising | rising-falling |  
falling}] [owner name]
```

```
no rmon alarm index
```

Parameters

- index—Specifies the alarm index. (Range: 1–65535)
- mib-object-id—Specifies the object identifier of the variable to be sampled. (Valid OID)
- interval—Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1–2147483647)
- rising-threshold—Specifies the rising threshold value. (Range: 0–2147483647)
- falling-threshold—Specifies the falling threshold value. (Range: 0–2147483647)
- rising-event—Specifies the index of the event triggered when a rising threshold is crossed. (Range: 0–65535)
- falling-event—Specifies the index of the event triggered when a falling threshold is crossed. (Range: 0–65535)
- type {absolute | delta}—(Optional) Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. The possible values are:
 - absolute—Specifies that the selected variable value is compared directly with the thresholds at the end of the sampling interval.
 - delta—Specifies that the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.

- startup {rising | rising-falling | falling}—(Optional) Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
 - rising—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to rising-threshold, a single rising alarm is generated.
 - rising-falling—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to rising-threshold, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to falling-threshold, a single falling alarm is generated.
 - falling —Specifies that if the first sample (after this entry becomes valid) is less than or equal to falling-threshold, a single falling alarm is generated.
- owner name—(Optional) Specifies the name of the person who configured this alarm. (Valid string)

Default Configuration

The default method type is absolute.

The default startup direction is rising-falling.

If the owner name is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an alarm with index 1000, MIB object ID D-Link, sampling interval 360000 seconds (100 hours), rising threshold value 1000000, falling threshold value 1000000, rising threshold event index 10, falling threshold event index 10, absolute method type and rising-falling alarm.

```
ZEQU0xxxxDL(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20
```

37.2 show rmon alarm-table

To display a summary of the alarms table, use the show rmon alarm-table Privileged EXEC mode command.

Syntax

show rmon alarm-table

Parameters

N/A.

Command Mode

Privileged EXEC mode

Example

The following example displays the alarms table.

```
ZEQU0xxxxDL# show rmon alarm-table
Index      OID                               Owner
-----
1           1. 3. 6. 1. 2. 1. 2. 2. 1. 10. 1  CLI
2           1. 3. 6. 1. 2. 1. 2. 2. 1. 10. 1  Manager
3           1. 3. 6. 1. 2. 1. 2. 2. 1. 10. 9  CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

37.3 show rmon alarm

To display alarm configuration, use the show rmon alarm Privileged EXEC mode command.

Syntax

show rmon alarm number

Parameters

alarm number—Specifies the alarm index. (Range: 1–65535)

Command Mode

Privileged EXEC mode

Example

The following example displays RMON 1 alarms.

```
ZEQU0xxxxDL# show rmon alarm 1
```

Alarm 1

OID: 1.3.6.1.2.1.2.2.1.10.1

Last sample Value: 878128

Interval: 30

Sample Type: delta Startup Alarm:

rising Rising Threshold: 8700000

Falling Threshold: 78

Rising Event: 1

Falling Event: 1

Owner: CLI

The following table describes the significant fields shown in the display:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	Value of the statistic during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.
Interval	Interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	Method of sampling the variable and calculating the value compared against the thresholds. If the value is absolute, the variable value is compared directly with the thresholds at the end of the sampling interval. If the value is delta, the variable value at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
Startup Alarm	Alarm that is sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising-falling, then a single falling alarm is generated.
Rising Threshold	Sampled statistic rising threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	Sampled statistic falling threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	Event index used when a rising threshold is crossed.
Falling Event	Event index used when a falling threshold is crossed.
Owner	Entity that configured this entry.

37.4 rmon event

To configure an event, use the `rmon event` Global Configuration mode command. To remove an event, use the `no` form of this command.

Syntax

```
rmon event index {none | log | trap | log-trap} [community text] [description text]
[owner name]
```

```
no rmon event index
```

Parameters

- `index`—Specifies the event index. (Range: 1–65535)
- `none`— Specifies that no notification is generated by the device for this event.
- `log`—Specifies that a notification entry is generated in the log table by the device for this event.
- `trap`—Specifies that an SNMP trap is sent to one or more management stations by the device for this event.
- `log-trap`—Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the device for this event.
- `community text`—(Optional) Specifies the SNMP community (password) used when an SNMP trap is sent. (Octet string; length: 0–127 characters). Note this must be a community used in the definition of an SNMP host using the “`snmp-server host`” command.
- `description text`—(Optional) Specifies a comment describing this event. (Length: 0–127 characters)
- `owner name`—(Optional) Specifies the name of the person who configured this event. (Valid string)

Default Configuration

If the owner name is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an event identified as index 10, for which the device generates a notification in the log table.

```
ZEQU0xxxxDL(config)# rmon event 10 log
```

37.5 show rmon events

To display the RMON event table, use the show rmon events Privileged EXEC mode command.

Syntax

```
show rmon events
```

Parameters

N/A.

Command Mode

Privileged EXEC mode

Example

The following example displays the RMON event table.

```
ZEQU0xxxxDL# show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
----	-----	-----	-----	-----	-----
	Errors	Log			
1	High	Log	router	CLI	Jan 18 2006 23:58:17
2	Broadcast	Trap		Manager	Jan 18 2006 23:59:48

The following table describes significant fields shown in the display:

Field	Description
Index	Unique index that identifies this event.
Description	Comment describing this event.
Type	Type of notification that the device generates about this event. Can have the following values: none, log, trap, log-trap. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent with the SNMP community string specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

37.6 show rmon log

To display the RMON log table, use the show rmon log Privileged EXEC mode command.

Syntax

show rmon log [event]

Parameters

event—(Optional) Specifies the event index. (Range: 0–65535)

Command Mode

Privileged EXEC mode

Example

The following example displays event 1 in the RMON log table.

ZEQU0xxxxDL# show rmon log 1		
Maximum table size: 500 (800 after reset)		
Event	Description	Time
-----	-----	-----
1	MIB Var. : 1.3.6.1.2.1.2.1.10. 53, Delta, Rising, Actual Val: 800, Thres.Set: 100, Interval (sec):1	Jan 18 2017 23:48:19

37.7 mon table-size

To configure the maximum size of RMON tables, use the `rmon table-size` Global Configuration mode command. To return to the default size, use the `no` form of this command.

Syntax

```
rmon table-size {history entries | log entries}
```

```
no rmon table-size {history | log}
```

Parameters

- `history entries`—Specifies the maximum number of history table entries. (Range: 20–32767)
- `log entries`—Specifies the maximum number of log table entries. (Range: 20–32767)

Default Configuration

The default history table size is 270 entries. The default log table size is 200 entries.

Command Mode

Global Configuration mode

User Guidelines

The configured table size takes effect after the device is rebooted.

Example

The following example configures the maximum size of RMON history tables to 100 entries.

```
ZEQU0xxxxDL (config)# rmon table-size history 100
```

37.8 show rmon statistics

To display RMON Ethernet statistics, use the show rmon statistics Privileged EXEC mode command.

Syntax

show rmon statistics {interface-id}

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

Privileged EXEC mode

Example

The following example displays RMON Ethernet statistics for port gi1/0/1.

```
ZEQU0xxxxDL# show rmon statistics gi1/0/1
Port gi1/0/1

Dropped: 0
Octets: 0
Broadcast: 0
CRC Align Errors: 0
Undersize Pkts: 0
Fragments: 0
64 Octets: 0
128 to 255 Octets: 1
512 to 1023 Octets: 0

Packets: 0
Multicast: 0
Collisions: 0
Oversize Pkts: 0
Jabbers: 0
65 to 127 Octets: 1
256 to 511 Octets: 1
1024 to max Octets: 0
```

The following table describes the significant fields displayed.

Field	Description
Dropped	Total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	Total number of good packets received and directed to the broadcast address. This does not include multicast packets.

Multicast	Total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	Total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	Best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	Total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	Total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
64 Octets	Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	Total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	Total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	Total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to max	Total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).

37.9 rmon collection stats

To enable RMON MIB collecting history statistics (in groups) on an interface, use the rmon collection stats Interface Configuration mode command. To remove a specified RMON history group of statistics, use the no form of this command.

Syntax

```
rmon collection stats index [owner ownername] [buckets bucket-number] [interval seconds]
```

```
no rmon collection stats index
```

Parameters

- index—The requested group of statistics index.(Range: 1–65535)
- owner ownername—(Optional) Records the name of the owner of the RMON group of statistics. If unspecified, the name is an empty string. (Range: Valid string)
- buckets bucket-number—(Optional) A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50.(Range: 1–50)
- interval seconds—(Optional) The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: 1–3600).

Command Mode

Interface Configuration mode.

37.10 show rmon collection stats

To display the requested RMON history group statistics, use the show rmon collection stats Privileged EXEC mode command.

Syntax

show rmon collection stats [interface-id]

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

Privileged EXEC mode

Example

The following example displays all RMON history group statistics.

```
ZEQU0xxxxDL# show rmon collection stats
```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner
-----	-----	-----	-----	-----	-----
1	gi1/0/1	30	50	50	CLI
2	gi1/0/1	1800	50	50	Manager

The following table describes the significant fields shown in the display.

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

37.11 show rmon history

To display RMON Ethernet history statistics, use the show rmon history Privileged EXEC mode command.

Syntax

```
show rmon history index {throughput | errors | other} [period seconds]
```

Parameters

- index—Specifies the set of samples to display. (Range: 1–65535)
- throughput—Displays throughput counters.
- errors—Displays error counters.
- other—Displays drop and collision counters.
- period seconds—(Optional) Specifies the period of time in seconds to display. (Range: 1–2147483647)

Command Mode

Privileged EXEC mode

Example

The following examples display RMON Ethernet history statistics for index 1:

ZEQUOxxxxDL# show rmon history 1 throughput					
Sample Set: 1	Owner: CLI				
Interface: gi1/0/1	Interval: 1800				
Requested samples: 50	Granted samples: 50				
Maximum table size: 500					
Time	Octets	Packets	Broadcast	Multicast	Util
-----	-----	-----	-----	-----	-----
Jan 18 2017 21:57:00	303595962	357568	3289	7287	19%
Jan 18 2017 21:57:30	287696304	275686	2789	5878	20%

ZEQUOxxxxDL# show rmon history 1 errors					
Sample Set: 1	Owner: Me				
Interface: gi1/0/1	Interval: 1800				
Requested samples: 50	Granted samples: 50				
Maximum table size: 500 (800 after reset)					
Time	CRC	Under	Oversize		Jabbers
	Align	size	Fragments		
-----	-----	-----	-----		-----
Jan 18 2017 21:57:00	1	1	49		0
Jan 18 2017 21:57:30	1	1	27		0

```

ZEQU0xxxxDL# show rmon history 1 other
Sample Set: 1          Owner: Me
Interface: gi1/0/1     Interval: 1800
Requested samples: 50   Granted samples: 50
Maximum table size: 500
Time                  Dropped   Collisions
-----
Jan 18 2017 21:57:00   3         0
Jan 18 2017 21:57:30   3         0

```

The following table describes significant fields shown in the display:

Field	Description
Time	Date and Time the entry is recorded.
Octets	Total number of octets of data (including those in bad packets and excluding framing bits but including FCS octets) received on the network.
Packets	Number of packets (including bad packets) received during this sampling interval.
Broadcast	Number of good packets received during this sampling interval that were directed to the broadcast address.
Multicast	Number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
Utilization	Best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	Total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.

Field	Description

Jabbers	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	Total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is the number of times this condition has been detected.
Collisions	Best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

38 RIP Commands

38.1 clear rip statistics

The clear rip statistics Privileged EXEC mode command clears statistics counters of all interfaces and all peers.

Syntax

clear rip statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

The following example shows how to clear all counters:

```
ZEQU0xxxxDL# clear rip statistics
```

38.2 default-information originate

To generate a default route into Routing Information Protocol (RIP), use the `default-information originate` command in Router Configuration mode. To disable this feature, use the `no default-information originate` command.

Syntax

`default-information originate`

`no default-information originate`

Parameters

N/A

Default Configuration

Default route is not generated by RIP.

Command Mode

Router RIP Configuration mode

User Guidelines

Use the command to enable generation of a default route.

Examples

Example 1 - The following example shows how to originate a default route:

```
ZEQU0xxxxDL (config) # router rip
ZEQU0xxxxDL (config-rip) # default-information originate
ZEQU0xxxxDL (config-rip) # exit
```

38.3 default-metric

The default-metric Router RIP configuration mode command sets the default metric value when RIP advertises routes derived by other protocols (for example, by static configuration). The no format of the command sets the default value.

Syntax

default-metric [metric-value]

no default-metric

Parameters

- metric-value—Default metric value. (Range 1-15)

Default Configuration

metric-value—1.

Command Mode

Router RIP Configuration mode

Example

The following example shows how to set the default metric to 2:

```
ZEQU0xxxxDL(config)# router rip
ZEQU0xxxxDL(config-rip)# default-metric 2
ZEQU0xxxxDL(config-rip)# exit
```

38.4 ip rip authentication key-chain

The ip rip authentication key-chain IP Interface Configuration mode command specifies the set of keys that can be used for and specifies the type of authentication. The no format of the command returns to default.

Syntax

ip rip authentication key-chain name-of-chain

no ip rip authentication key-chain

Parameters

- name-of-chain—Specifies the name of key set. The name-change parameter points to list of keys specified by the key chain CLI command.

Default Configuration

No defined key chain.

Command Mode

IP Configuration mode

User Guidelines

Use the ip rip authentication key-chain IP Interface Configuration mode command to define a key chain name. Only one key chain may be defined per an IP interface. Each the ip rip authentication key-chain command overrides the previous definition.

In order to have a smooth rollover of keys in a key chain, a key should be configured with a lifetime that starts several minutes before the lifetime of the previous key expires.

Example

The following example shows how to define a chain name:

```
ZEQU0xxxxDL (config) # interface ip 1.1.1.1
ZEQU0xxxxDL (config-route-map) # ip rip authentication key-chain alpha
ZEQU0xxxxDL (config-route-map) # exit
```

38.5 ip rip authentication mode

The ip rip authentication mode IP Interface Configuration mode command enables authentication. The no format of the command returns to default.

Syntax

ip rip authentication mode {text | md5}

no ip rip authentication mode

Parameters

- text—Specifies the clear text authentication.
- md5—Specifies the MD5 authentication.

Default Configuration

No authentication.

Command Mode

IP Configuration mode

User Guidelines

If you enable the MD5 authentication, you must configure a key chain name with the ip rip authentication key-chain interface command. If a key chain is not defined for the IP interface or there is not a valid key then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

If you enable the clear text authentication, you must configure a password with the ip rip authentication-key interface command. If a password is not defined for the IP interface then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

Example

The following example shows how to set the md5 mode:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1
ZEQU0xxxxDL(config-route-map)# ip rip authentication mode md5
ZEQU0xxxxDL(config-route-map)# exit
```

38.6 ip rip authentication-key

To assign a password to be used by neighboring routers that are using the RIP clear text authentication, use the `ip rip authentication-key` command in interface configuration mode. To remove the RIP password, use the `no` form of this command.

Syntax

`ip rip authentication-key password`

`no ip rip authentication-key`

Parameters

- `password`—Any continuous string of characters that can be entered from the keyboard up to 16 characters in length.

Default Configuration

No password is specified.

Command Mode

IP Configuration mode

User Guidelines

The password created by this command is used as a "key" that is inserted directly into the RIP header when the switch software originates routing protocol packets.

A separate password can be assigned to each subnetwork. All neighboring routers on the same subnetwork must have the same password to be able to exchange RIP information.

Only one password may be defined per IP interface. Each `ip rip authentication-key` command overrides the previous definition.

Example

The following example shows how to define a password:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1
ZEQU0xxxxDL(config-route-map)# ip rip authentication mode text
ZEQU0xxxxDL(config-route-map)# ip rip authentication-key alph$$12
ZEQU0xxxxDL(config-route-map)# exit
```

38.7 ip rip default-information originate

The ip rip default-information originate IP Interface generates a metric for a default route in RIP. The no format of the command disables the feature.

Syntax

```
ip rip default-information originate {disable | metric}
```

```
no ip rip default-information originate
```

Parameters ranges

- disable—Do not send the default route.
- metric—Default route metric value.(Range: 1-15)

Default Configuration

The RIP behavior is specified by the default-information originate command.

Command Mode

IP Configuration mode

User Guidelines

Use the command to override the RIP behavior specified by the default-information originate command on a given IP interface.

Example

The following example shows how to enable sending of default route with metric 3:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1  
ZEQU0xxxxDL(config-route-map)# ip rip default-information originate 3  
ZEQU0xxxxDL(config-route-map)# exit
```

38.8 ip rip distribute-list in

The `ip rip distribute-list in` IP configuration mode command enables filtering of routes in incoming RIP update messages. The `no` format of the command disables the filtering.

Syntax

```
ip rip distribute-list access access-list-name in no ip
```

```
rip distribute-list in
```

Parameters

- `access-list-name`—Standard IP access list name, up to 32 characters. The list defines which routes in incoming RIP update messages are to be accepted and which are to be suppressed.

Default Configuration

No filtering

Command Mode

IP Configuration mode

User Guidelines

Each network from a received RIP update message is evaluated by the access list and it is accepted only if it is permitted by the list. See the `ip access-list (IP standard)` and `ip prefix-list` commands for details.

Example

The following example shows how to define input filtering:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1  
ZEQU0xxxxDL(config-route-map)# ip rip distribute-list access 5 in  
ZEQU0xxxxDL(config-route-map)# exit
```

38.9 ip rip distribute-list out

The `ip rip distribute-list out` IP configuration mode command enables filtering of routes in outgoing RIP update messages. The `no` format of the command disables the filtering.

Syntax

```
ip rip distribute-list access access-list-name out no ip
```

```
rip distribute-list out
```

Parameters

- `access-list-name`—Standard IP access list name, up to 32 characters. The list defines which routes in outgoing RIP update messages are to be sent and which are to be suppressed.

Default Configuration

No filtering

Command Mode

IP Configuration mode

User Guidelines

Each network from the IP Forwarding table is evaluated by the list and it is included in the RIP update message only if it is permitted by the list. See the `ip access-list (IP standard)` and `ip prefix-list` commands.

Example

The following example shows how to define outgoing filtering:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1  
ZEQU0xxxxDL(config-route-map)# ip rip distribute-list access 5 out  
ZEQU0xxxxDL(config-route-map)# exit
```

38.10 ip rip offset

The ip rip offset IP configuration mode command defines a metric added to incoming routes. The no format of the command returns to default.

Syntax

ip rip offset offset

no ip rip offset

Parameters

- offset—Specifies the offset to be applied to received routes. Range: 1-15.

Default Configuration

offset—1.

Command Mode

IP Configuration mode

User Guidelines

Example

The following example shows how to set offset to 2:

```
ZEQU0xxxxDL (config)# interface ip 1.1.1.1  
ZEQU0xxxxDL (config-route-map)# ip rip offset 2  
ZEQU0xxxxDL (config-route-map)# exit
```

38.11 ip rip passive-interface

The ip rip passive-interface IP Interface Configuration mode command disables sending RIP packets on an IP interface. The no format of the command re-enables the sending RIP packets.

Syntax

ip rip passive-interface

no ip rip passive-interface

Parameters

N/A.

Default Configuration

RIP messages are sent.

Command Mode

IP Configuration mode

User Guidelines

Use the ip rip passive-interface command to stop sending RIP messages on the giving IP interface. To stop RIP messages being sent on all interfaces, use the passive-interface command.

Note. The no ip rip passive-interface command does not override the passive-interface command.

Example

The following example shows how to stop the sending of RIP messages:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1
ZEQU0xxxxDL(config-route-map)# ip rip passive-interface
ZEQU0xxxxDL(config-route-map)# exit
```

38.12 ip rip shutdown

The ip rip shutdown IP Interface configuration mode command changes the RIP interface state from enabled to disabled. The no ip rip shutdown command returns the state to a value of enabled.

Syntax

ip rip shutdown

no ip rip shutdown

Parameters

N/A

Default Configuration

Enabled

Command Mode

IP Configuration mode

User Guidelines

Use the ip rip shutdown CLI command to disable RIP on an IP interface without removing its configuration. The ip rip shutdown CLI command may be applied only to RIP interfaces created by the network CLI command. The ip rip shutdown CLI command does not remove the RIP interface configuration.

Example

The following example shows how to disable RIP on the 1.1.1.1 IP interface:

```
ZEQU0xxxxDL(config)# interface ip 1.1.1.1
ZEQU0xxxxDL(config-route-map)# ip rip shutdown
ZEQU0xxxxDL(config-route-map)# exit
```

38.13 network

The network Router RIP configuration mode command enables RIP on the given IP interfaces. The no format of the command disables RIP on the given IP interfaces and removes its interface configuration.

Syntax

network ip-address [shutdown]

no network ip-address

Parameters

- ip-address—An IP address of a switch IP interface.
- shutdown—RIP is enabled on the interface in the shutdown state.

Default Configuration

N/A

Command Mode

Router RIP Configuration mode

User Guidelines

RIP can be defined only on manually-configured IP interfaces, meaning that RIP cannot be defined on an IP address defined by DHCP or on a default IP address.

Use the network CLI command with the shutdown keyword to create RIP on an interface if you are going to change the default values of RIP configuration and the use the no ip rip shutdown CLI command.

Use the no network CLI command to remove RIP on an IP interface and remove its interface configuration.

Examples

Example 1. The following example shows how to enable RIP on IP interface 1.1.1.1 with the default interface configuration:

```
ZEQU0xxxxDL(config)# router rip
ZEQU0xxxxDL(config-rip)# network 1.1.1.1
ZEQU0xxxxDL(config-rip)# exit
```

Example 2. The following example enables RIP on 1.1.1.1 in the shutdown state, configures metric and starts RIP:

```
ZEQU0xxxxDL (config)# router rip
ZEQU0xxxxDL (config-rip)# network 1.1.1.1 shutdown
ZEQU0xxxxDL (config-rip)# exit
ZEQU0xxxxDL (config)# interface ip 1.1.1.1
ZEQU0xxxxDL (config-route-map)# ip rip offset 2
ZEQU0xxxxDL (config-route-map)# no ip rip shutdown
ZEQU0xxxxDL (config-route-map)# exit
```

38.14 **passive-interface (RIP)**

To disable sending routing updates on all RIP IP interfaces, use the `passive-interface` command in Router RIP Configuration mode. To re-enable the sending of RIP routing updates, use the `no` form of this command.

Syntax

`passive-interface`

`no passive-interface`

Parameters

N/A

Default Configuration

Routing updates are sent on all IP RIP interfaces.

Command Mode

Router RIP Configuration mode

User Guidelines

After using the `passive-interface` command, you can then configure individual interfaces where adjacencies are desired using the `no ip rip passive-interface` command.

Example

The following example sets all IP interfaces as passive and then excludes the IP interface 1.1.1.1:

```
ZEQU0xxxxDL (config)# router rip
ZEQU0xxxxDL (config-rip)# passive-interface
ZEQU0xxxxDL (config-rip)# network 1.1.1.1
ZEQU0xxxxDL (config-rip)# network 2.2.2.2
ZEQU0xxxxDL (config-rip)# network 3.3.3.3
ZEQU0xxxxDL (config-rip)# exit
ZEQU0xxxxDL (config)# interface ip 1.1.1.1
ZEQU0xxxxDL (config-route-map)# no ip rip passive-interface
ZEQU0xxxxDL (config-route-map)# exit
```

38.15 redistribute (RIP)

To redistribute routes from one routing domain into a RIP routing domain, use the redistribute command in the Router RIP configuration mode. To disable redistribution, use the no form of this command.

Syntax

```
redistribute protocol [metric {metric-value | transparent}] [match {internal | external 1 | external 2}]
```

```
no redistribute protocol [match {internal | external 1 | external 2}]
```

Parameters

- **protocol**—Source protocol from which routes are being redistributed. It can be one of the following keywords: connected or static.
 - **metric transparent**—Causes RIP to use the source protocol metric for redistributed routes as the RIP metric. Only routes with metric less than 16 are redistributed.
 - **metric metric-value**—Specifies the metric assigned to the redistributed routes. The value supersedes the metric value specified using the default-metric command.
 - **match {internal | external 1 | external 2}**—Use the match keyword only with the ospf keyword to specify the conditions under which OSPF routes are redistributed into RIP. You can specify one of the following:
 - **internal**—Internal route to a specific autonomous system.
 - **external 1**—External route to a specific autonomous system.
However, it is imported into OSPF as a external route of Type 1.
 - **external 2**—External route to a specific autonomous system.
However, it is imported into OSPF as a external route of Type 2.
By default, the internal route and the external 1 route are redistributed.
- Note: You can define multiple redistribute commands with different values of the match keyword.

Default Configuration

Route redistribution is disabled

Command Mode

Router RIP Configuration mode

User Guidelines

Routes distributed to the source protocol are never redistributed by it

The `connected` keyword is used to redistribute to RIP routes that correspond to defined IP interfaces on which RIP is not enabled. By default, the RIP Routing Table includes only routes that correspond only to IP interfaces on which it is enabled.

The `static` keyword is used to redistribute to RIP static routes. By default, static routes are not redistributed to RIP.

If the metric value is set by the route map (by the `set metric` command) then the value will supersede the metric value specified by the `metric-value` argument.

If the `metric` keyword is not defined, then the metric is specified by the `default-metric` CLI command is assigned to the redistributed routes. If metric value set by the route map is equal or bigger than 16 the route is not redistributed.

Changing or disabling any keyword will not affect the state of other keywords. Removing options that you have configured for the `redistribute` command requires careful use of the `no` form of the `redistribute` command to ensure that you obtain the result that you are expecting.

Examples

Example 1. The following example enables redistribution of static routes by RIP with transparent metric:

```
ZEQU0xxxxDL (config) # router rip
ZEQU0xxxxDL (config-rip) # redistribute static metric transparent
ZEQU0xxxxDL (config-rip) # exit
```

Example 2. The following example enables redistribution of static routes by RIP with transparent metric and then changes the metric to default:

```
ZEQU0xxxxDL (config) # router rip
ZEQU0xxxxDL (config-rip) # redistribute static metric transparent
ZEQU0xxxxDL (config-rip) # no redistribute static metric transparent
ZEQU0xxxxDL (config-rip) # exit
```

Example 3. The following example enables redistribution of static routes by RIP with default metric and then changes the metric to transparent:

```
ZEQU0xxxxDL (config) # router rip
ZEQU0xxxxDL (config-rip) # redistribute static
ZEQU0xxxxDL (config-rip) # redistribute static metric transparent
ZEQU0xxxxDL (config-rip) # exit
```

Example 4. The following example enables redistribution of static routes by RIP with transparent metric. The second redistribute command does not affect:

```
ZEQU0xxxxDL (config) # router rip  
ZEQU0xxxxDL (config-rip) # redistribute static metric transparent  
ZEQU0xxxxDL (config-rip) # redistribute static  
ZEQU0xxxxDL (config-rip) # exit
```

Example 5. The following example disables redistribution of static routes by RIP:

```
ZEQU0xxxxDL (config) # router rip  
ZEQU0xxxxDL (config-rip) # no redistribute static  
ZEQU0xxxxDL (config-rip) # exit
```

38.16 router rip

The router rip Global Configuration mode command specifies the Router RIP mode and enables it if it was disabled. The no format of the command disables RIP globally and removes its configuration.

Syntax

router rip

no router rip

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

RIP supports the following global states:

- disabled
- enabled
- shutdown

If a value of the RIP global state is disabled (default value), RIP is not operational and cannot be configured. When this state is set, the RIP configuration is removed. The state may be set by the no router rip CLI command from any RIP global state.

If a value of the RIP global state is shutdown, RIP is not operational, but can be configured. When the state is set the RIP configuration is not changed. The state may be set by the shutdown CLI command from the enabled RIP global state.

If the value of the RIP global state is enabled, RIP is operational, and can be configured. The state can be set by the router rip CLI command from the disabled RIP global state and by the no shutdown CLI command from the shutdown RIP global state.

Example

The following example shows how to enable RIP globally:

```
ZEQU0xxxxDL(config)# router rip
```

38.17 show ip rip database

The show ip rip database Privileged EXEC mode command displays information about the RIP Database.

Syntax

show ip rip database [all | brief | ip-address]

Parameters

- all—Provides the full RIP database information about all RIP interfaces. The option is assumed if the parameter is omitted.
- brief—Provides a summary view of the RIP database information.
- ip-address—Provides the full RIP database information about the given IP Address.

Command Mode

Privileged EXEC mode

Default Configuration

N/A

Examples

Example 1—The following example shows the full RIP database information about all RIP interfaces is displayed:

```
ZEQU0xxxxDL# show ip rip database
```

```
RIP is enabled
```

```
RIP Administrative state is UP
```

```
Default metric value is 1
```

```
Redistributing is enabled from
```

```
    Connected:
```

```
        Metric is default-metric
```

```
    Static:
```

```
        Metric is transparent
```

```
IP Interface: 1.1.1.1
```

```
Administrative State is enabled
```

```
IP Interface Offset is 10
```

```
Default Originate Metric is 12
```

```
Authentication Type is text
```

```
Password is afGRwiteW%3
```

```
IN Filtering Type is Access List
```

```
Access List Name is 10
```

```
OUT Filtering Type is Access List
```

```
Access List Name is List12
```

```
IP Interface: 2.2.2.2
```

```
Administrative State is enabled
```

```
IP Interface Offset is 2
```

```
No Default Originate Metric
```

```
Authentication Type is MD5
```

```
Key Chain Name is chain1
```

```
IN Filtering Type is Access List
```

```
Access List Name is 10
```

```
OUT Filtering Type is Access List
```

```
Access List Name is 12
```

```
IP Interface: 3.3.3.3
```

```
Administrative State is enabled
```

```
IP Interface Offset is 1
```

```
IP Interface is passive
```

```
Default Originate Metric 3, on passive too
```

```
No Authentication
```

```
No IN Filtering
```

```
No OUT Filtering
```

```
IP Interface: 4.4.4.4
```

```
Administrative State is shutdown
```

```
IP Interface Offset is 1
```

```
No Authentication
```

```
No IN Filtering
```

```
No OUT Filtering
```

Example 2—The following example shows the full RIP database information about a given IP address is displayed:

```
ZEQU0xxxxDL# show ip rip database 1.1.1.1
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: on passive only
Default metric value is 1
Redistributing is enabled from
    Connected
        Metric is default-metric
    Static
        Metric is transparent

IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwiteW%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
```

Example 3—The following example shows the brief RIP database information about all RIP interfaces is displayed:

```
ZEQU0xxxxDL# show ip rip database brief
```

```
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: route-map is condition
Default metric value is 1
Redistributing is enabled from
Connected
Metric is default-metric
Static
Metric is transparent
OSPF:
from metric type:
metric value is 2
external 1
metric value is 4
external 2
metric value is 6
with subnets
```

IP Interface	Admin State	Offset	Passive Interface	Default Metric	Auth. Type	IN Filt. Type	OUT Filt. Type
100.100.100.100	enabled	10	No	12	Text	Access	Access
2.2.2.2	enabled	2	No		MD5	Access	Access
3.3.3.3	enabled	1	Yes				
4.4.4.4	shutdow	1	No				

Example 4—The following example shows the output when RIP is disabled:

```
ZEQU0xxxxDL# show ip rip database
RIP is disabled
```

38.18 show ip rip peers

The show ip rip peers Privileged EXEC mode command displays information about RIP Peers.

Syntax

show ip rip peers

Parameters

N/A

Command Mode

Privileged EXEC mode

Default Configuration

N/A

Example

ZEQU0xxxxDL# **show ip rip peers**

RIP is enabled
Static redistributing is enabled with Default metric
Default redistributing metric is 1

Address	Last Update	Received Bad Packets	Received Bad Route
-----	-----	-----	-----
1. 1. 12	00:10:17	-	1
2. 2. 2. 3	00:10:01	-	-

38.19 show ip rip statistics

The show ip rip statistics Privileged EXEC mode command displays RIP statistics.

Syntax

show ip rip statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Default Configuration

N/A

Example

ZEQU0xxxxDL# show ip rip statistics

RIP is enabled
Static redistributing is enabled with transparent metric
Default redistributing metric is 1

Interface	Received Bad Pakets	Received Bad Routes	Sent Triggered Packets
-----	-----	-----	-----
1. 1. 1. 1	-	1	8
2. 2. 2. 2	-	-	7

38.20 shutdown

The shutdown Router RIP configuration mode command sets the RIP global state to shutdown. The no format of the command sets the RIP global state to enabled.

Syntax

shutdown

no shutdown

Parameters

N/A

Default Configuration

Enabled

Command Mode

Router RIP Configuration mode

User Guidelines

Use the shutdown CLI command to stop RIP globally without removing its configuration

Example

The following example shows how to shutdown RIP globally:

```
ZEQU0xxxxDL (config)# router rip  
ZEQU0xxxxDL (config-rip)# shutdown  
ZEQU0xxxxDL (config-rip)# exit
```

39 Router Resources Commands

39.1 system router resources

To configure the system router resources, use the system router resources command in Global Configuration mode. To return to the default, use the no form of this command.

Syntax

```
system router resources [ip-entries max-number] [ipv6-entries max-number]  
[ipm-entries max-number] [ipmv6-entries max-number]
```

```
no system router resources
```

Parameters

- ip-entries max-number—(Optional) The maximum number of IPv4 entries.
- ipv6-entries max-number—(Optional) The maximum number of IPv6 entries.
- ipm-entries max-number—(Optional) The maximum number of IPv4 multicast entries.
- ipmv6-entries max-number—(Optional) The maximum number of IPv6 multicast entries.

Default Configuration

- ip-entries— 4094.
- ipv6-entries— 4094.
- ipm-entries— 1024.
- ipmv6-entries— 1024.

Command Mode

Global Configuration mode

User Guidelines

Use the `system router resources` command to enter new settings for routing entries. After entering the command, the current routing entries configuration will be displayed, and the user will be required to confirm saving the new setting to the startup-configuration and to reboot the system.

When this command is included in a configuration file that is downloaded to the device, if it is downloaded to the running configuration file, the command will be rejected. If it is downloaded to the startup configuration file, the device will not be automatically rebooted. The new settings will be used after the device is rebooted manually.

Data Validation:

If the new settings exceed the maximum number of routing entries, the command is rejected and a message is displayed to the user.

If the new settings are fewer than the currently in-use routing entries, a confirmation message is displayed to the user (before the save confirmation message).

Use the `no system router resources` command to restore the default settings. The

following table displays the conversion between logical entities to HW entries:

Logical Entity	IPv4
IP Neighbor	1 entry
IP Address	2 entries
IP Remote Route	1 entry
IPM Group (*,G) or (S,G)	2 entries

Logical Entity	IPv6 (Router TCAM)
IP Neighbor	4 Entries
IP Address	8 entries
IP Remote Route	4 Entries
On-Link-Prefix	4 Entries
IPM Group (*,G) or (S,G)	8 entries

Examples

Example 1

The following example defines the supported number of IPv4 routing entries.

```
ZEQU0xxxxDL(config)# system router resources ip-entries 128 ipv6-entries 32
```

	In-Use	Reserved (Current)	Reserved (New)
IPv4 Entries	4	3072	128
Number of Routes	0		
Number of Neighbors		0	
Number of Interfaces		1	
IPv6 Entries	0	3072	3072
Number of Routes	0		
Number of Neighbors		0	
Number of Interfaces		0	
Number of Prefixes		0	
IPv4 Policy-Based-Routes	0	64	64
IPv6 Policy-Based-Routes	0	64	64
VLAN mapping entries	0	64	64

Setting the new configuration of route entries requires saving the running-configuration file to startup-configuration file and rebooting the system, do you want to continue?
(Y/N) [N]

Example 2

The following example defines the supported number of IPv4 and IPv6 routing entries. In the example, the configured router entries are less than the router entries which are currently in use. Using this configurations means that the system will not have enough resources for the running again in the existing network:

ZEQU0xxxxDL (config) # **system router resources ip-enries 256**

	In-Use	Reserved (Current)	Reserved (New)
IPv4 Entries	4	3072	128
Number of Routes	0		
Number of Neighbors		0	
Number of Interfaces		1	
IPv6 Entries	0	3072	3072
Number of Routes	0		
Number of Neighbors		0	
Number of Interfaces		0	
Number of Prefixes		0	
IPv4 Policy-Based-Routes	0	64	64
IPv6 Policy-Based-Routes	0	64	64
VLAN mapping entries	0	64	64

Setting the new configuration of route entries requires saving the running-configuration file to startup-configuration file and rebooting the system, do you want to continue?
(Y/N) [N]

39.2 show system router resources

To display router resources, use the show system router resources command in User EXEC mode.

Syntax

show system router resources

Parameters

N/A.

Command Mode

User EXEC mode

Example

In the following example, the configured router entries are displayed:

ZEQU0xxxxDL (config) # show system router resources			
	In-Use	Reserved (Current)	Reserved (New)
	-----	-----	-----
IPv4 Entries	4	3072	128
Number of Routes	0		
Number of Neighbors		0	
Number of Interfaces		1	
IPv6 Entries	0	3072	3072
Number of Routes	0		
Number of Neighbors		0	
Number of Interfaces		0	
Number of Prefixes		0	
IPv4 Policy-Based-Routes	0	64	64
IPv6 Policy-Based-Routes	0	64	64
VLAN mapping entries	0	64	64

Setting the new configuration of route entries requires saving the running-configuration file to startup-configuration file and rebooting the system, do you want to continue? (Y/N) [N]

40 RSA and Certificate Commands

Keys and Certificates

The device automatically generates default RSA/DSA keys and certificates at following times:

- When the device is booted following a software upgrade.
- When the device is booted with an empty configuration.
- When user-defined keys/certificates are deleted.

Some commands in this section are used to generate user-defined RSA/DSA keys and certificates that replace the default keys and are used by SSL and SSH server commands. Other commands can be used to import these keys from an external source.

These keys and certificates are stored in the configuration files.

The following table describes when these keys/certificates are displayed..

File Type Being Displayed	What is Displayed in a Show Command Without Detailed	What is Displayed in a Show Command With Detailed
Startup Config	Only user-defined keys/certificates.	Option is not supported.
Running Config	Keys are not displayed.	All keys (default and user-defined)
Text-based CLI (local backup config. file, or remote backup config. file)	Keys are displayed as they were copied. There is no distinction here between default and user-defined keys.	Option is not supported.

The following table describes how keys/certificates can be copied from one type of configuration file to another (using the copy command)..

Destination File Type	Copy from Running Config.	Copy from Startup Config.	Copy from Remote/Local Backup Config. File
Startup Config.	All keys/certificate s are copied (but only user-defined ones can be displayed	Option is not supporte d.	All keys/certificates present in this file are copied (*, **).
Running Config	N/A	Only user defined.	All keys/certificates present in this file are copied (*).
Text-based CLI (local backup config. file, or remote backup config. file)	All keys (default and user)	Only user defined.	All keys/certificates present in this file are copied (**)

* If the Running Configuration file on the device contains default keys (not user-defined ones), the same default keys remain after reboot.

** In a text-based configuration file, there is no distinction between automatically-defined, default keys and user-defined keys.

Lists of Commands

40.1 crypto key generate dsa

The crypto key generate dsa Global Configuration mode command generates a public and private DSA key (DSA key pair).

Syntax

crypto key generate dsa

Parameters

N/A

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs - one public DSA key and one private DSA key.

If the device already has DSA keys default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

This command is not saved in the Running configuration file. However, the keys generated by this command are saved in a private configuration (which is never displayed to the user or backed up to another device).

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example generates a DSA key pair.

```
ZEQUOxxxxDL (config)# crypto key generate dsa
```

```
The SSH service is generating a private DSA key.
```

```
This may take a few minutes, depending on the key size.
```

```
.....
```

40.2 crypto key generate rsa

The crypto key generate rsa Global Configuration mode command generates RSA key pairs.

Syntax

crypto key generate rsa

Parameters

N/A

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs - one public RSA key and one private RSA key. If the device already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example generates RSA key pairs where a RSA key already exists.

```
ZEQU0xxxxDL(config)# cryptokey generate rsa
Replace Existing RSA Key [y/n]? N
ZEQU0xxxxDL(config)#
```

40.3 crypto key import

The crypto key import Global Configuration mode command imports the DSA/RSA key pair.

Use the no form of the command to remove the user key and generate a new default in its place.

Syntax

```
crypto key import {dsa | rsa} no crypto key {dsa | rsa}
```

Parameters

N/A

Default Configuration

DSA and RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA/RSA keys are imported in pairs - one public DSA/RSA key and one private DSA/RSA key.

If the device already has DSA/RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is saved in the Running Configuration file.

When using the encrypted key-word, the private key is imported in its encrypted form.

Example

ZEQU0xxxxDL (config) # crypto key import rsa

Please paste the input now, add a period (.) on a separate line after the input

----- BEGIN SSH2 PRIVATE KEY -----

ZEQU0xxxxDL (config) # encrypted crypto key import rsa

----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----

Comment: RSA Private Key

```
84et9C2XUfCRlpemuGINAygnLwfkKJcDM6m20ReALHScqqLhi0wMSSYNI T1 IWFZP1kEV
HHFpt1aECZi7HfGLcp1pMZwjnl+HaXBtQjPDiEtbpScXqrg6m1/0EnwpFK2TrmUyOIi
fwk8E/mMfX3i/2rRZLkEBea5jrA6Q62gl5naRw1Zk0ges+GNeibtvZYSk1jzr56LUR6f
T7Xu5iKMcU2b2NsuSD5yW8R/x0CW2elqDDz/biA2gSgd6FfnW2HV48bTC55eCKrs1d2M
mjbExUdz+RQRhzjcGMBYp6HzkD66z8HmSh0U+hKd7M1K9U4Sr+Pr1vyWUJIEk0gz906a
ZoIGp4tgm4VDy/K/G/sI5nVLO+bR8LFUXU0/U5hohBcyRUF02fHYKZrhTiPT5Rw+PHt6
/+EXKG9E+Trs IUADMI tCRvs+lsB33IBdvoRDdI98YaA2htZay1TkMqCUBdfIO+74UO
qa/b+bp67wCYKe9 yen418MaYKtcHJBQmF7sUQZQGP34VPmOMyZzon68S/ZoT77cy0ih
RZx9wcI1yYhJnDiYxP dgXHYhW6kCTcTj6LrUSQuxCJ9su89Z1WNn50wdgonLSpvfnab
v2GHmmeIaveL7JJ/7Ucf061q5D4PJ67Vk2xL7PqyHXN931rseTzPuJpIkSLCFZ5uqTmb
WwYQEKmHDIOx35vIGou5tky9LgIwG4d+9edctZZaggeq5cgjnsZWJgUoB4Bn4hIreyOd
HDiFUPPRxkoyhG0GnJuvxC9T9K6BF1wBTdDQS+Gu47/0/gRoD/50q4sGkzqHsRJJ53W0
TOQ1bHMTMLPpwn2nXzvfGxWL/bu QhZZSqRonG6MX1cP7KT7i4TPq2w2k3TGTNBnVYHx
60oNcaTHmg1N2s50gRsyXD9tF++6nY RfMN8CsV+9jQKQP7ZaGc8Ju+d72jvSwppSr03
2HY+IpzZ4ujkK+/X5oawZL5NnkaEQTKKX RSL55S405NP0jS/pC9hg7GaVjoY2mQ7Hdp
SUBeTIDTlv0wC2kSkA9C6aF/Axj2dXLweQd5 lXk7m0/mMNAiJsNk6y33LcuKjIxpNNj
K9n9KzRPkGNMF0bprfenWKteDftjQ==
```

----- END SSH2 PRIVATE KEY -----

----- BEGIN SSH2 PUBLIC KEY -----

Comment: RSA Public Key

```
AAAAB3NzaC1yc2EAAAABIwAAAIEAvRHsKry6NKMkYmb+yWEp9042vupLvYVq3ngt1sB9
JH 0cdK/2nw7lCQguy1mLsX8/bKMYXSk/3aBEvaoJQ82+r/nRf0y3HTy4Wp9zV0SiVC8
jLD+77t0aHejzfUhr0FRhWWcLnvYwr+nmrYDpS6FADMC2hVA85KZRYe9ifxT7otE=
```

----- END SSH2 PUBLIC KEY -----

40.4 show crypto key

The show crypto key Privileged EXEC mode command displays the device's SSH private and public keys for both default and user-defined keys.

Syntax

```
show crypto key [mypubkey] [rsa | dsa]
```

Parameters

- mypubkey—Displays only the public key.
- rsa—Displays the RSA key.
- dsa—Displays the DSA key.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example displays the SSH public DSA keys on the device.

```
ZEQU0xxxxDL# show crypto key mypubkey dsa
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: DSA Public Key
```

```
AAAAB3NzaC1kc3MAAACBALzTTQZBE6yBqs47QXq3VqzMmvRw+SCdT62hCGEH  
4dZY41k8a18H/hBrv32W+13Tncr5A0wNEL0iXmlox823Q7nJYtfwx0BCK/dR  
wvE1uxeZRp0A1/ZyliunqNqyF0YLL+lfHIWr8VbFiUbc+Xy/XIveK5JISK8N  
o9LzLCnE+oM3AAAAFQDbPRINEoeFnusoHCeu0/obb+ybJwAAAIeAJEuCfT8I  
TyjqHXAKJonyDgIeKxor9QbpYCYBTiX+pHxcTnLomFo0e3bD7BnmngwA1CDH  
/d0Gmruv3oixdm/+YUfcF1jfhBUcQA2FcFQuMOH4jllS+qVEX041i8npIAtb  
JZE/nmqWBSMvKzSLfN2aXBaqOMR6Nmjb3gFeXQmwfzIAAACATvnVjhYyUK49  
PaNQ7RKsJlJ2y2rc9G3V0sHwGfEMaoR4pjGPKVJiyu206g3Dub+krFvGjU1D  
JuXNBCn2x4c/78E80h0AQs4dsiKkK2ve/bM+cSon+l1StK9SGuRua0tCtQRc  
gBADpRI3ACyEkrdldShSxQ9TRnNueYHKw0zddnw=
```

```
---- END SSH2 PUBLIC KEY ----
```

```
Public Key Fingerprint:
```

```
b4:73:1a:b8:c3:f0:33:ae:05:ef:03:31:57:79:d9:45
```

```
This key is a default key
```

40.5 crypto certificate generate

The crypto certificate generate Global Configuration mode command generates a self-signed certificate for HTTPS.

Syntax

crypto certificate number generate [key-generate [length]] [cn common- name] [ou organization-unit] [or organization] [loc location] [st state] [cu country] [duration days]

Parameters

- number—Specifies the certificate number. (Range: 1–2)
- key-generate length—Regenerates SSL RSA key and specifies the SSL's RSA key length. (Range: 512–2048)

The following elements can be associated with the key. When the key is displayed, they are also displayed.

- cn common- name—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
- ou organization-unit—Specifies the organization-unit or department name. (Length: 1–64 characters)
- or organization—Specifies the organization name. (Length: 1–64 characters)
- loc location—Specifies the location or city name. (Length: 1–64 characters)
- st state—Specifies the state or province name. (Length: 1–64 characters)
- cu country—Specifies the country name. (Length: 2 characters)
- duration days—Specifies the number of days a certification is valid. (Range: 30–3650)

Default Configuration

The default SSL's RSA key length is 1024.

If cn common- name is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If duration days is not specified, it defaults to 365 days.

Command Mode

Global Configuration mode

User Guidelines

If the RSA key does not exist, you must use the parameter `key-generate`.

If both certificates 1 and 2 have been generated, use the `ip https certificate` command to activate one of them.

See [Keys and Certificates](#) for information on how to display and copy this key pair.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

Example

The following example generates a self-signed certificate for HTTPS whose length is 2048 bytes.

```
ZEQU0xxxxDL (config)# crypto certificate 1 generate key-generate 2048
```

40.6 crypto certificate request

The crypto certificate request Privileged EXEC mode command generates and displays a certificate request for HTTPS.

Syntax

crypto certificate number request [cn common- name] [ou organization-unit] [or organization] [loc location] [st state] [cu country]

Parameters

- number—Specifies the certificate number. (Range: 1–2)
- The following elements can be associated with the key. When the key is displayed, they are also displayed.
 - cn common- name—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
 - ou organization-unit—Specifies the organization-unit or department name. (Length: 1–64 characters)
 - or organization—Specifies the organization name. (Length: 1–64 characters)
 - loc location—Specifies the location or city name. (Length: 1–64 characters)
 - st state—Specifies the state or province name. (Length: 1–64 characters)
 - cu country—Specifies the country name. (Length: 2 characters)

Default Configuration

If cn common-name is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the `crypto certificate generate` command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the `crypto certificate import` command to import the certificate into the device. This certificate replaces the self-signed certificate.

Example

The following example displays the certificate request for HTTPS.

ZEQU0xxxxDL# crypto certificate 1 request

-----BEGIN CERTIFICATE REQUEST-----

```
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAXCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZiIhvcNAQkBFgFsMIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/FOMV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTdekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
```

```
MRDjEyMwgICCAgICAICAglMAOGCSqGSIb3DQEBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwI8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
```

-----END CERTIFICATE REQUEST-----

40.7 crypto certificate import

The crypto certificate import Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS. In addition, the RSA key-pair can also be imported.

Use the no form of the command to delete the user-defined keys and certificate.

Syntax

crypto certificate number import

encrypted crypto certificate number import no

crypto certificate number

Parameters

- number—Specifies the certificate number. (Range: 1–2).

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

To end the session (return to the command line to enter the next command), enter a blank line.

The imported certificate must be based on a certificate request created by the crypto certificate request command.

If only the certificate is imported, and the public key found in the certificate does not match the device's SSL RSA key, the command fails. If both the public key and the certificate are imported, and the public key found in the certificate does not match the imported RSA key, the command fails.

This command is saved in the Running configuration file.

When using the encrypted form of the command, only the private key must be in encrypted format.

See Keys and Certificates for information on how to display and copy this key pair.

Examples

Example 1 - The following example imports a certificate signed by the Certification Authority for HTTPS.

```
ZEQU0xxxxDL(config)# crypto certificate 1 import
```

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.

```
-----BEGIN CERTIFICATE-----
```

```
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB  
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg  
MIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY  
0Og9XM1Axf0iqLIQJHd4xP+BHGZWwfkjKjUDBPZn52LxdDu1KrpB/h0+TZPOFv38  
7mIDqtnoF1NLsWxkVKRM5LPkaOL/ha1pYxp7EWAt5iDBzSw5s04lv0bSN7oaGjFA  
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQinJst6hI  
XFDxe7I80d3Uyt3Dmf7KE/AmUVOPif2yUluy/RuxRwKhDp/lGrK12tzLQz+s50x7  
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW  
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
```

```
.  
-----END CERTIFICATE-----
```

Certificate imported successfully.

Issued by : C=, ST=, L=, CN=0.0.0.0, O=, OU=

Valid From: Jan 24 18:41:24 2017 GMT

Valid to: Jan 24 18:41:24 2017 GMT

Subject: C=US, ST=, L=, CN=router.gm.com, O= General Motors, OU=

SHA1 Finger print: DC789788 DC88A988 127897BC BB789788

Example 2: The following example imports a certificate signed by the Certification Authority for HTTPS, and the RSA key-pair.

```
ZEQU0xxxxDL(config)# crypto certificate 1 import
```

```
Please paste the input now, add a period (.) on a separate line after  
the input, and press Enter.
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
ACnrqImEgIXkwxBuZUIA09nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cV  
Xh20wrBhJgB69vLUIJuJM9p1IXFpMk8qR3NS7JzIInYAWjHKKbEZBMsKSA6+t/UzVxev  
KK6HTGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6Nj0/ZOAgvNAMKNr2Wa+tGU0oA  
glOb/C11EoqzpCq5mT7+V0FhPS04dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGpOpX0vDA9  
ENY17qsZMWmCfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGxKn  
IUs6uTzhW dKWWc0e/vwMgPtLIWyxWynnaPOfAJ+PawOAdsK75bo79NBim3HcNVXhWN  
zqfg2s3AYCRBx WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhPqLHuzXHUon7  
Zx15CUtP3sbHI+XI B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbH34aIVJ  
aN+2AMCb0hpI3IkreYo A8Lk6UM0uIQaMnhYf+RyPXhPOqs01PpIPhKBGTi6p39XMvi  
yRXvSpn5+eIYPhve5jYaEn Ue0nVZRhNCVnruJAYXSLhJApf5iIQr1JiJb/mVt8+zpqc  
CU9HCWQqsMrNF0FrSpcbHu5V4ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYSK70ps8u7BtgpR  
fSRUr7g0LfzhzMuswoDSnB65pkCqI7yZnBeRS0zrUDgHLLRfzwjwmXjmw0bxYfRGMLp4  
=
```

```
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN RSA PUBLIC KEY-----
```

```
MIGHAoGBAMVuFgfJYLbUzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DiitSf  
B2Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQ0voFBYNmbzHc7a+7043wfVmH+  
QOXfTbnRDhIMVrZJGbzI1c9IzGky1I21XmicY0/nwsXDAgEj
```

```
-----END RSA PUBLIC KEY-----
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB  
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg  
MIGfMAoGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY  
00g9XM1Axf0iqlIQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZPOFv38  
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5s04lv0bSN7oaGjFA  
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuYQinJst6hI  
XFDxe7I80d3Uyt3Dmf7KE/AmUVOPif2yUluy/RuxRwKhDp/IGrK12tzLQz+s50x7  
Klft/IcjbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWapuS+gXrIqjW  
WVZdOn1fXhMacoflgnnEmweIzmrqXBs=
```

```
-----END CERTIFICATE-----
```

```
.
```

```
Certificate imported successfully.
```

```
Issued by : C=, ST=, L=, CN=0.0.0.0, O=, OU=
```

```
Valid From: Jan 24 18:41:24 2017 GMT
```

```
Valid to: Jan 24 18:41:24 2017 GMT
```

```
Subject: C=US, ST=, L=, CN=router.gm.com, O= General Motors, OU=
```

```
SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

40.8 show crypto certificate

The show crypto certificate Privileged EXEC mode command displays the device SSL certificates and key-pair for both default and user defined keys.

Syntax

```
show crypto certificate [mycertificate] [number]
```

Parameters

- **number**—Specifies the certificate number. (Range: 1,2)
- **mycertificate**—Specifies that only the certificate will be displayed

Default Configuration

Certificate number 1.

Command Mode

Privileged EXEC mode

Examples

The following example displays SSL certificate # 1 present on the device and the key-pair.

ZEQU0xxxxDL# show crypto certificate 1

Certificate 1:

Certificate Source: Default

-----BEGIN CERTIFICATE-----

dHmUgUm9vdCBDZX0aWZpZXIwX DANBgkqhkiG9w0BAQEFAANLADBI AKEAp4HS
nnH/xQSGA2ffkRBwU2X1xb7n8VPsTm1xyJ1t11a1Ga qchfMqqe0kmfhcoHSWr
yf1FpDOMWOTgDawIDAQABo4IBojC A24wEwYJKwYBBAAGNCxQCBAYeABDAEEw
CwROPBAQDAfGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVRO0BBYEfAf4MT9BRD47
ZvKBAEL9Ggp+6MI IBNgYDVROfBI BLTCCASkgdKg gc+ggcyGgcIsZGfW0i8v
LOVByb3h5JTJwU29mdHdcmUIMjBSB290JTJwQ2VydGlm aWVyLENOPXNlcnZl

-----END CERTIFICATE-----

Issued by: www.verisign.com

Valid From: Jun 9 07:15:30 2017 GMT

Valid to: Jun 9 07:15:30 2018 GMT

Subject: CN= router.gm.com, O= General Motors, C= US

SHA1 Fingerprint: DC789788 DC88A988 127897BC BB789788

41 Spanning-Tree Commands

41.1 spanning-tree

Use the spanning-tree Global Configuration mode command to enable spanning-tree functionality. Use the no form of this command to disable the spanning-tree functionality.

Syntax

spanning-tree state enable

spanning-tree state disable

Parameters

N/A

Default Configuration

Spanning-tree is enabled.

Command Mode

Global Configuration mode

Example

The following example enables spanning-tree functionality.

```
ZEQU0xxxxDL (config) # spanning-tree state enable
```

41.2 spanning-tree mode

Use the spanning-tree mode Global Configuration mode command to select which Spanning Tree Protocol (STP) protocol to run. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree mode {stp| rstp | mst}

no spanning-tree mode

Parameters

- stp—Specifies that STP is enabled.
- rstp—Specifies that the Rapid STP is enabled.
- mst—Specifies that the Multiple STP is enabled.

Default Configuration

The default is RSTP.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

Example

The following example enables MSTP.

```
ZEQU0xxxxDL (config) # spanning-tree mode mst
```

41.3 spanning-tree forward-time

Use the spanning-tree forward-time Global Configuration mode command to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree forward-time seconds

no spanning-tree forward-time

Parameters

seconds—Specifies the spanning-tree forward time in seconds. (Range: 4–30)

Default Configuration

15 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be maintained:

$$2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$$

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
ZEQU0xxxxDL (config) # spanning-tree forward-time 25
```

41.4 spanning-tree hello-time

Use the spanning-tree hello-time Global Configuration mode command to configure how often the device broadcasts Hello messages to other devices. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree hello-time seconds

no spanning-tree hello-time

Parameters

seconds—Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

Default Configuration

2 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the Hello time, the following relationship should be maintained: Max-Age

$$\geq 2 * (\text{Hello-Time} + 1)$$

Example

The following example configures the spanning-tree bridge hello time to 5 seconds.

```
ZEQU0xxxxDL (config)# spanning-tree hello-time 5
```

41.5 spanning-tree max-age

Use the spanning-tree max-age Global Configuration mode command to configure the STP maximum age. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree max-age seconds

no spanning-tree max-age

Parameters

seconds—Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

Default Configuration

The default maximum age is 20 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the maximum age, the following relationships should be maintained:

$$2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$$

$$\text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$$

Example

The following example configures the spanning-tree bridge maximum age to 10 seconds.

```
ZEQU0xxxxDL (conf ig) #spanning-tree max-age 10
```

41.6 spanning-tree priority

Use the spanning-tree priority Global Configuration mode command to configure the device STP priority, which is used to determine which bridge is selected as the root bridge. Use the no form of this command to restore the default device spanning-tree priority.

Syntax

spanning-tree priority priority

no spanning-tree priority

Parameters

priority—Specifies the bridge priority. (Range: 0–61440)

Default Configuration

Default priority = 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree. When more than one switch has the lowest priority, the switch with the lowest MAC address is selected as the root.

Example

The following example configures the spanning-tree priority to 12288.

```
ZEQU0xxxxDL(config)# spanning-tree priority 12288
```

41.7 spanning-tree state

Use the spanning-tree state Interface (Ethernet, Port Channel) Configuration mode command to disable the spanning tree on a specific port. Use the no form of this command to enable the spanning tree on a port.

Syntax

spanning-tree state enable

spanning-tree state disable

Parameters

N/A

Default Configuration

Spanning tree is enabled on all ports.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables the spanning tree on gi1/0/5

```
ZEQU0xxxxDL(config)# interface gi1/0/5
ZEQU0xxxxDL(config-if)# spanning-tree state enable
```

41.8 spanning-tree cost

Use the spanning-tree cost Interface (Ethernet, Port Channel) Configuration mode command to configure the spanning-tree path cost for a port. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree cost cost

no spanning-tree cost

Parameters

cost—Specifies the port path cost. (Range: 1–200000000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below

Interface	Long	Short
Port-channel	Half the default cost based on Port-channel interface	Half the default cost based on Port-channel interface speed
TenGigabit Ethernet (10000 Mbps)	2000	2
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures the spanning-tree cost on gi1/0/15 to 35000.

```
ZEQU0xxxxDL(config)# interface gi1/0/15
ZEQU0xxxxDL(config-if)# spanning-tree cost 35000
```

41.9 spanning-tree port-priority

Use the spanning-tree port-priority Interface (Ethernet, Port Channel) Configuration mode command to configure the port priority. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree port-priority priority

no spanning-tree port-priority

Parameters

priority—Specifies the port priority. (Range: 0–240)

Default Configuration

The default port priority is 128.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on gi1/0/15 to 96

```
ZEQU0xxxxDL(config)# interface gi1/0/15
ZEQU0xxxxDL(config-if)# spanning-tree port-priority 96
```

41.10 spanning-tree portfast

Use the spanning-tree portfast Interface (Ethernet, Port Channel) Configuration mode command to enable the PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay. Use the no form of this command to disable the PortFast mode.

Syntax

spanning-tree portfast [auto]

no spanning-tree portfast

Parameters

auto—Specifies that the software waits for 3 seconds (with no Bridge Protocol Data Units (BPDUs) received on the interface) before putting the interface into the PortFast mode.

Default Configuration

PortFast mode is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables the PortFast mode on gi1/0/15.

```
ZEQU0xxxxDL(config)# interface gi1/0/15
ZEQU0xxxxDL(config-if)# spanning-tree portfast
```

41.11 spanning-tree link-type

Use the spanning-tree link-type Interface (Ethernet, Port Channel) Configuration mode command to override the default link-type setting determined by the port duplex mode, and enable RSTP transitions to the Forwarding state. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree link-type {point-to-point | shared}

no spanning-tree spanning-tree link-type

Parameters

- point-to-point—Specifies that the port link type is point-to-point.
- shared—Specifies that the port link type is shared.

Default Configuration

The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables shared spanning-tree on gi1/0/15.

```
ZEQU0xxxxDL (config) # interface gi1/0/15
ZEQU0xxxxDL (config-if) # spanning-tree link-type shared
```

41.12 spanning-tree pathcost method

Use the spanning-tree pathcost method Global Configuration mode command to set the default path cost method. Use the no form of this command to return to the default configuration.

Syntax

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

Parameters

- long—Specifies that the default port path costs are within the range: 1–200,000,000.
- short—Specifies that the default port path costs are within the range: 1–65,535.

Default Configuration

Long path cost method.

Command Mode

Global Configuration mode

User Guidelines

This command applies to all the spanning tree instances on the switch.

- If the short method is selected, the switch calculates the default cost as 100.
- If the long method is selected, the switch calculates the default cost as 20000.

Example

The following example sets the default path cost method to Long.

```
ZEQU0xxxxDL(config)# spanning-tree pathcost method long
```

41.13 spanning-tree bpdud (Global)

Use the spanning-tree bpdud Global Configuration mode command to define Bridge Protocol Data Unit (BPDU) handling when the spanning tree is disabled globally or on a single interface. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree bpdud { filtering | flooding }

no spanning-tree bpdud

Parameters

- filtering—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- flooding—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to all ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration

The default setting is flooding.

Command Mode

Global Configuration mode

User Guidelines

The filtering and flooding modes are relevant when the spanning tree is disabled globally or on a single interface.

Example

The following example defines the BPDU packet handling mode as flooding when the spanning tree is disabled on an interface.

```
ZEQU0xxxxDL (config) # spanning-tree bpdud flooding
```

41.14 spanning-tree forward-bpdu (Interface)

Use the spanning-tree bpdu Interface (Ethernet, Port Channel) Configuration mode command to define BPDU handling when the spanning tree is disabled on a single interface. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree forward-bpdu

no spanning-tree forward-bpdu

Parameters

Default Configuration

The spanning-tree bpdu (Global) command determines the default configuration.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example defines the BPDU packet when the spanning tree is disabled on ge1/0/3.

```
ZEQU0xxxxDL (config) # interface ge1/0/3
ZEQU0xxxxDL (config-if) # spanning-tree forward-bpdu
```

41.15 spanning-tree guard root

use the spanning-tree guard root Interface (Ethernet, Port Channel) Configuration mode command to enable Root Guard on all spanning-tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the no form of this command to disable the root guard on the interface.

Syntax

spanning-tree guard root

no spanning-tree guard root

Default Configuration

Root guard is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Root Guard can be enabled when the device operates in any mode (STP, RSTP and MSTP).

When Root Guard is enabled, the port changes to the alternate state if the spanning-tree calculations select the port as the root port.

Example

The following example prevents gi1/0/1 from being the root port of the device.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# spanning-tree guard root
```

41.16 clear spanning-tree detected-protocols

Use the clear spanning-tree detected-protocols Privileged EXEC mode command to restart the STP migration process (force renegotiation with neighboring switches) on all interfaces or on the specified interface

Syntax

clear spanning-tree detected-protocols [interface interface-id]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This feature can only be used when working in RSTP or MSTP mode.

Example

This restarts the STP migration process on all interfaces.

```
ZEQU0xxxxDL# clear spanning-tree detected-protocols
```

41.17 spanning-tree mst priority

Use the spanning-tree mst priority Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree mst instance-id priority priority

no spanning-tree mst instance-id priority

Parameters

- instance-id—Specifies the spanning-tree instance ID. (Range:1–15)
- priority—Specifies the device priority for the specified spanning-tree instance. This setting determines the likelihood that the switch is selected

as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0–61440)

Default Configuration

The default priority is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
ZEQU0xxxxDL (config)# spanning-tree mst 1 priority 4096
```

41.18 **spanning-tree mst max-hops**

Use the spanning-tree mst max-hops Global Configuration mode command to configure the number of hops in an MST region before the BDPU is discarded and the port information is aged out. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree mst max-hops hop-count

no spanning-tree mst max-hops

Parameters

max-hops hop-count—Specifies the number of hops in an MST region before the BDPU is discarded. (Range: 1–40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
ZEQU0xxxxDL (config)# spanning-tree mst max-hops 10
```

41.19 spanning-tree mst port-priority

Use the spanning-tree mst port-priority Interface (Ethernet, Port Channel) Configuration mode command to configure the priority of a port. Use the no form of this command to restore the default configuration.

Syntax

spanning-tree mst instance-id port-priority priority

no spanning-tree mst instance-id port-priority

Parameters

- instance-id—Specifies the spanning tree instance ID. (Range: 1–15)
- priority—Specifies the port priority. (Range: 0–240 in multiples of 16)

Default Configuration

The default port priority is 128.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the port priority of gi1/0/1 to 144.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# spanning-tree mst 1 port-priority 144
```

41.20 spanning-tree mst cost

Use the spanning-tree mst cost Interface (Ethernet, Port Channel) Configuration mode command to configure the path cost for MST calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the Forwarding state. Use the no form of this command to restore the default configuration.

Syntax

```
spanning-tree mst instance-id cost cost
```

```
no spanning-tree mst instance-id cost
```

Default Configuration

N/A

Parameters

- instance-id—Specifies the spanning-tree instance ID. (Range: 1–15)
- cost—Specifies the port path cost. (Range: 1–2000000000)

Default Configuration

Default path cost is determined by the port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	Half the default cost based on Port-channel interface	Half the default cost based on Port-channel interface speed
TenGigabit Ethernet (10000 Mbps)	2000	2
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures the MSTP instance 1 path cost for port gi1/0/9 to 4.

```
ZEQU0xxxxDL (config)# interface gi1/0/9  
ZEQU0xxxxDL (config-if)# spanning-tree mst 1 cost 4
```

41.21 spanning-tree mst configuration

Use the spanning-tree mst configuration Global Configuration mode command to enable configuring an MST region by entering the MST mode.

Syntax

spanning-tree mst configuration

Command Mode

Global Configuration mode

User Guidelines

For two or more switches to be in the same MST region, they must contain the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example configures an MST region.

```
ZEQU0xxxxDL (config) # spanning-tree mst configuration
ZEQU0xxxxDL (config-mst) # instance 1 vlan 10-20
ZEQU0xxxxDL (config-mst) # name region1
ZEQU0xxxxDL (config-mst) # revision 1
```

41.22 instance (MST)

Use instance MST Configuration mode command to map VLANs to an MST instance. Use the no form of this command to restore the default mapping.

Syntax

instance instance-id vlan vlan-range

no instance instance-id vlan vlan-range

Parameters

- instance-id—MST instance (Range: 1–15)
- vlan-range—The specified range of VLANs is added to the existing ones. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1–4094)

Default Configuration

All VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Mode

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
ZEQU0xxxxDL (config) # spanning-tree mst configuration
ZEQU0xxxxDL (config-mst) # instance 1 vlan 10-20
```

41.23 **name (MST)**

Use the name MST Configuration mode command to define the MST instance name. Use the no form of this command to restore the default setting.

Syntax name

string no

name

Parameters

string—Specifies the MST instance name. (Length: 1–32 characters)

Default Configuration

The default name is the bridge MAC address.

Command Mode

MST Configuration mode

Example

The following example defines the instance name as Region1.

```
ZEQU0xxxxDL(config)# spanning-tree mst configuration  
ZEQU0xxxxDL(config-mst)# name region1
```

41.24 **revision (MST)**

Use the revision MST Configuration mode command to define the MST configuration revision number. Use the no form of this command to restore the default configuration.

Syntax

revision value

no revision

Parameters

value—Specifies the MST configuration revision number. (Range: 0–65535)

Default Configuration

The default configuration revision number is 0.

Command Mode

MST Configuration mode

Example

The following example sets the configuration revision to 1.

```
ZEQU0xxxxDL (config) # spanning-tree mst configuration  
ZEQU0xxxxDL (config-mst) # revision 1
```

41.25 show (MST)

Use the show MST Configuration mode command to display the current or pending MST region configuration.

Syntax

show {current | pending}

Parameters

- current—Displays the current MST region configuration.
- pending—Displays the pending MST region configuration.

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example displays a pending MST region configuration

```
ZEQU05410DL(config)# spanning-tree mst configuration
ZEQU05410DL(config-mst)# show pending
Gathering information .....
Pending MST configuration
Name: 00:50:40:3c:4c:7b
Revision: 0
Instance  Vlans Mapped                                State
-----  -
0          1
ZEQU05410DL(config-mst)#
```

41.26 **exit (MST)**

Use the exit MST Configuration mode command to exit the MST region Configuration mode and apply all configuration changes.

Syntax

exit

Parameters

N/A

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example exits the MST Configuration mode and saves changes.

```
ZEQU0xxxxDL (config)# spanning-tree mst configuration
ZEQU0xxxxDL (config-mst)# exit
ZEQU0xxxxDL (config)#
```

41.27 **abort (MST)**

Use the abort MST Configuration mode command to exit the MST Configuration mode without applying the configuration changes.

Syntax

abort

Parameters

N/A

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example exits the MST Configuration mode without saving changes.

```
ZEQU0xxxxDL (config) # spanning-tree mst configuration  
ZEQU0xxxxDL (config-mst) # abort
```

41.28 **show spanning-tree**

Use the show spanning-tree Privileged EXEC mode command to display the spanning-tree configuration.

Syntax

```
show spanning-tree [interface-id] [instance instance-id]
```

```
show spanning-tree [detail] [active | blockedports] [instance instance-id]
```

```
show spanning-tree mst-configuration
```

Parameters

- instance instance-id—Specifies the spanning tree instance ID. (Range: 1–15).
- detail—Displays detailed information.
- active—Displays active ports only.
- blockedports—Displays blocked ports only.
- mst-configuration—Displays the MST configuration identifier.
- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

If no interface is specified, the default is all interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This command only works when MST is enabled.

Example

The following examples display spanning-tree information in various configurations

ZEQU0xxxxDL# **show spanning-tree**

Spanning tree enabled mode RSTP

Default port cost method: long

Loopback guard: Disabled

Root ID Priority 32768
 Address 00:50:40:97:e0:00
 Cost 20000
 Port gi1/0/1
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 36864
 Address 00:50:40:29:7a:00
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interfaces

Name	State	Prio. No	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Root	No	P2p (RSTP)
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	Shared (STP)
gi1/0/3	Disabled	128.3	20000	-	-	-	-
gi1/0/4	Enabled	128.4	20000	BLK	Altn	No	Shared (STP)
te1/0/5	Enabled	128.5	20000	DIS	-	-	-

42 SPAN and RSPAN Commands

42.1 monitor session destination

To create a new Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) destination session, use the monitor session destination command in Global Configuration mode. To remove a destination session, use the no form of the command.

Syntax

```
monitor session session_number destination { {interface interface-id [network]} |  
{remote vlan vlan-id reflector-port interface-id} network }
```

```
no monitor session session_number destination
```

Parameters

- session_number—Specify the session number identified with the SPAN, RSPAN or flow mirror session. The range is 1 to 7.
- interface interface-id—Specify the destination interface for the SPAN, RSPAN or flow mirror session (Ethernet port). When the source interface is a RSPAN VLAN the RSPAN VLAN_ID is removed from all frames copied to the interface.
 - network—Specify that the destination port acts also as a network port.
- remote vlan vlan-id—Specify the RSPAN VLAN for an RSPAN destination session. Not more than one RSPAN destination VLAN can be defined. The VLAN must be defined as a RSPAN transit VLAN in the source, intermediate and final switches by the remote-span command.
- reflector-port interface-id—Specify the destination interface for a RSPAN session (Ethernet port). The RSPAN VLAN_ID is added to all frames copied to the interface.

Default Configuration

No SPAN and RSPAN sessions are configured.

Command Mode

Global Configuration mode

User Guidelines

Use the monitor session session_number destination interface interface-id, to create a SPAN, local flow mirror, final RSPAN or final remote flow mirror destination session to copy traffic to a destination port.

Use the monitor session session_number destination remote vlan vlan-id reflector-port interface-id command, to create a start RSPAN destination session to copy traffic to a RSPAN VLAN via a reflector port. The remote VLAN must be configured by the remote-span command before this command.

A destination or reflector port cannot be a source port. A

If the network keyword is not defined only mirrored traffic sent on a destination port and all input traffic is discard and a value of DOWN is advertised as its operational status to all applications running on it.

A port cannot be configured as destination port with the network keyword if one the following conditions is true:

- It belongs to the source VLAN
- It belongs to the remote VLAN

Please, do not add the destination port to the source/remote VLAN.

A port cannot be configured as reflector if it belongs to the remote VLAN. The remote VLAN cannot be configured as a source VLAN.

Only in the final switch the remote VLAN can be configured as a source remote VLAN

A destination port with the network keyword or reflector port cannot be configured on an edge port (a port having the vlan-mapping ssss mode).

Mirrored traffic is sent to queue number 1 of the destination port.

Use the no monitor session session_number destination command to remove one destination session.

Example

Example 1. The following example configures a SPAN session consisting from 3 source and one destination session. The first source session copies traffic for both directions from the source port gi1/0/2, the second source session copies bridges traffic from VLAN 100, and the third source session copies traffic for received on the source port gi1/0/3. The destination session defines port gi1/0/1 as the destination port.

```
ZEQU0xxxxDL (config) # monitor session 1 source interface gi1/0/2 both
ZEQU0xxxxDL (config) # monitor session 1 source vlan 100
ZEQU0xxxxDL (config) # monitor session 1 source interface gi1/0/3 rx
ZEQU0xxxxDL (config) # monitor session 1 destination interface gi1/0/1
```

Example 2. The following example configures a flow mirror session:

```
ZEQU0xxxxDL (config) # ip access-list extended ip1
ZEQU0xxxxDL (config-ip-a1) # permit ip any any
ZEQU0xxxxDL (config-ip-a1) # exit
ZEQU0xxxxDL (config) # class-map c1
ZEQU0xxxxDL (config-cmap) # match access-group ip1
ZEQU0xxxxDL (config-cmap) # exit
ZEQU0xxxxDL (config) # policy-map p1
ZEQU0xxxxDL (config-pmap) # class c1
ZEQU0xxxxDL (config-pmap-c) # mirror 1
ZEQU0xxxxDL (config-pmap-c) # exit
ZEQU0xxxxDL (config-pmap) # exit
```

Example 3. The following example configures a RSPAN start session consisting from 2 source and one destination sessions. The first source session copies traffic for both directions from the source port gi1/0/2 and the second session copies traffic from VLAN 100. The destination session defines VLAN 2 as the RSPAN VLAN and port gi1/0/1 as the reflector port

```
ZEQU0xxxxDL (config) # monitor session 1 source interface gi1/0/2 both
ZEQU0xxxxDL (config) # monitor session 1 source vlan 100
ZEQU0xxxxDL (config) # monitor session 1 destination remote vlan 2 reflector-port gi1/0/1 network
```

Example 4. The following example configures a final RSPAN session that copies traffic from a RSPAN VLAN 2 to destination port gi1/0/1:

```
ZEQU0xxxxDL (config) # vlan 2
ZEQU0xxxxDL (config-vlan) # remote-span
ZEQU0xxxxDL (config-vlan) # exit
ZEQU0xxxxDL (config) # monitor session 1 source remote vlan 2
ZEQU0xxxxDL (config) # monitor session 1 destination interface gi1/0/1
```

42.2 monitor session source

To create a new Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) source session, use the `monitor session source` command in Global Configuration mode. To remove a source session, use the `no` form of the command.

Syntax

```
monitor session session_number source {interface interface-id [both | rx | tx]} | {vlan  
vlan-id} | {remote vlan vlan-id}
```

```
no monitor session [session_number] source [{interface interface-id} | {vlan vlan-id}  
| {remote vlan vlan-id}]
```

Parameters

- `session_number`—Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 7.
- `interface interface-id`—Specify the source interface for a SPAN or RSPAN session (Ethernet port).
- `both, rx, tx`—Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
- `vlan vlan-id`—Specify the SPAN source interface as a VLAN ID. In this case only a value of 1 is allowed for the `session_number` argument.
- `remote vlan vlan-id`—Specify the source RSPAN source VLAN ID. The VLAN must be defined as a RSPAN transit VLAN in the source, intermediate and final switches by the `remote-span` command.

Default Configuration

No SPAN and RSPAN sessions are configured.

Command Mode

Global Configuration mode

User Guidelines

Use the `monitor session session_number source interface interface-id [both | rx | tx]` command, to create a SPAN or RSPAN start source session to monitor traffic that enters or leaves a source port.

Use the `monitor session session_number source vlan vlan-id` command, to create a SPAN or start RSPAN source session to monitor traffic that bridged into a source VLAN.

Use the `monitor session session_number source remote vlan vlan-id` command, to create a final RSPAN source session to monitor traffic that passed via a RSPAN VLAN.

A SPAN or RSPAN session consists from up to 8 sources and one destination with the same session number.

Each monitor session source command defines one source port or VLAN. Different monitor session source commands must define different sources. A new

command with the same session number and the same source overrides the previous defined one.

Up to 8 sources can be defined in one session.

If a packet is mirrored by both the port-based ingress mirroring mechanism, and one of the other ingress mirroring mechanisms, the selected session is the one with the higher session number.

All definitions of different source ports for the same source session must be of the same type: SPAN, start RSPAN start, or RSPAN final.

A source port cannot be a destination port. A

The source interface in a RSPAN source switch can not be a membership of the remote VLAN.

Use the `no monitor session session_number source {interface interface-id} | {vlan vlan-id} | {remote vlan vlan-id}` command to remove one source.

Use the `no monitor session session_number source` command to remove all sources ports of the given source session.

Example

Example 1. The following example configures a SPAN session consisting from 3 source and one destination session. The first source session copies traffic for both directions from the source port gi1/0/2, the second source session copies bridges traffic from VLAN 100, and the third source session copies traffic for received on the source port gi1/0/3. The destination session defines port gi1/0/1 as the destination port.

```
ZEQU0xxxxDL (config) # monitor session 1 source interface gi1/0/2 both
ZEQU0xxxxDL (config) # monitor session 1 source vlan 100
ZEQU0xxxxDL (config) # monitor session 1 source interface gi1/0/3 rx
ZEQU0xxxxDL (config) # monitor session 1 destination interface gi1/0/1
```

Example 2. The following example configures a RSPAN start session consisting from 2 source and one destination sessions. The first source session copies traffic for both directions from the source port gi1/0/2 and the second session copies

traffic from VLAN 100. The destination session defines VLAN 2 as the RSPAN VLAN and port gi1/0/1 as the reflector port

```
ZEQU0xxxxDL (config) # monitor session 1 source interface gi1/0/2 both
ZEQU0xxxxDL (config) # monitor session 1 source vlan 100
ZEQU0xxxxDL (config) # monitor session 1 destination remote vlan 2 reflector-port gi1/0/1
```

Example 3. The following example configures a final RSPAN session that copies traffic from a RSPAN VLAN 2 to destination port gi1/0/1:

```
ZEQU0xxxxDL (config) # vlan 2
ZEQU0xxxxDL (config-vlan) # remote-span
ZEQU0xxxxDL (config-vlan) # exit
ZEQU0xxxxDL (config) # monitor session 1 source remote vlan 2
ZEQU0xxxxDL (config) # monitor session 1 destination interface gi1/0/1
```

42.3 remote-span

To configure a virtual local area network (VLAN) as a RSPAN remote VLAN, use the remote-span command in VLAN Configuration mode. To return to default, use the no form of this command.

Syntax

remote-span

no remote-span

Parameters

This command has no arguments or keywords.

Default Configuration

A VLAN is not a RSPAN remote VLAN.

Command Mode

VLAN Configuration mode

User Guidelines

Use the remote-span command to define a VLAN as a RSPAN remote VLAN. Only one

Remote VLAN can be defined per switch.

The Remote VLAN must be created manually before configuring of the remote-span command.

Guest VLAN cannot be configured as a Remote VLAN.

All traffic into a RSPLAN VLAN is tagged and MAC learning is disabled in a RSPAN VLAN.

The remote-span command verifies that all ports of the configured VLAN are egress tagged ports and disables MAC learning. The no remote-span command resets MAC learning.

Note. The membership of a RSPAN remote VLAN depended where it is defined:

- Source or Start switch—It is recommended that the RSPAN remote VLAN does not have any memberships.

- Intermediate switch—It is recommended to remove the RSPAN remote VLAN from trunk ports not used for passing mirrored traffic to avoid superfluous flooding. Usually, a RSPAN remote VLAN contains two ports.
- Destination or Final switch—The RSPAN remote VLAN should contain memberships on which the mirrored traffic via this VLAN is arrived. The destination interface cannot be a membership of this VLAN.

Example

Example 1. The following example shows how to configure a RSPAN remote VLAN in a source switch:

```

ZEQU0xxxxDL (config) # vlan 2
ZEQU0xxxxDL (config-vlan) # remote-span
ZEQU0xxxxDL (config-vlan) # exit
ZEQU0xxxxDL (config) # monitor session 1 source interface gi1/0/2 both
ZEQU0xxxxDL (config) # monitor session 1 destination remote vlan 2 reflector-port gi1/0/1

```

Example 2. The following example shows how to configure a RSPAN remote VLAN in a final switch:

```

ZEQU0xxxxDL (config) # interface gi1/0/3
ZEQU0xxxxDL (config-if) # switchport mode trunk
ZEQU0xxxxDL (config-if) # switchport trunk allowed none
ZEQU0xxxxDL (config-if) # switchport trunk allowed add 2
ZEQU0xxxxDL (config-if) # exit
ZEQU0xxxxDL (config) # vlan 2
ZEQU0xxxxDL (config-vlan) # remote-span
ZEQU0xxxxDL (config-vlan) # exit
ZEQU0xxxxDL (config) # monitor session 1 source remote vlan 2
ZEQU0xxxxDL (config) # monitor session 1 destination interface gi1/0/1

```

Example 3. The following example shows how to configure a RSPAN remote VLAN in an intermediate switch:

```

ZEQU0xxxxDL (config) # interface range gi1/0/3, 4
ZEQU0xxxxDL (config-if) # switchport mode trunk
ZEQU0xxxxDL (config-if) # switchport trunk allowed none
ZEQU0xxxxDL (config-if) # switchport trunk allowed add 2
ZEQU0xxxxDL (config-if) # exit
ZEQU0xxxxDL (config) # vlan 2
ZEQU0xxxxDL (config-vlan) # remote-span
ZEQU0xxxxDL (config-vlan) # exit

```

42.4 show monitor session

To display information about Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch, use the show monitor command in User EXEC mode.

Syntax

show monitor session [session_number]

Parameters

- session_number—Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 7. If the argument is not defined information about all sessions are displayed.

Default Configuration

This command has no default settings.

Command Mode

User EXEC mode

User Guidelines

Use the show monitor session session_number command to display information about one session.

Use the show monitor session command to display information about all sessions

Example

Example 1. The following example displays information about all SPAN sessions defined into the switch:

```
ZEQU0xxxxDL> show monitor session
Session 1
  Type: SPAN
  Source: gi1/0/2, rx only
  Source: VLAN 100
  Source: flow mirrow, policy-map: alpha class-maps: ip-http, ipv6-http
  Destination: gi1/0/1, network port
```

Example 2. The following example displays information about all start RSPAN sessions defined into the switch:

```
ZEQU0xxxxDL> show monitor session
Session 1
  Type: RSPAN Start
  Source: gi1/0/3, both
  Source: VLAN 100
  Source: flow mirrow, policy-map: alpha class-maps: ip-http, ipv6-http
  Destination: RSPAN VLAN 2, reflector-port gi1/0/1, network port
```

Example 3. The following example displays information about all final RSPAN sessions defined into the switch:

```
ZEQU0xxxxDL> show monitor session
Session 1
  Type: RSPAN Final
  Source: RSPAN VLAN 10
  Source: RSPAN VLAN 20
  Destination: gi1/0/1
```

Field Definitions:

- Type—The type of the session.
- Source—A source of the session. The following options are supported:
 - Source: *interface-id*, *traffic-direction*(rx only,tx only,or both)

The Source is an interface.

- Source: *vlan* *vlan-id*

The Source is a VLAN.

- Source: *remote* *vlan* *vlan-id*

The Source is a RSPAN VLAN (in the RSPAN session final switch).

- Source: *flow mirror*, *policy-map*: *policy-map-name*, *class-maps*:
class-map-name1, *class-map-name2*

The Source is a flow mirror, only attached policy-names are displayed.

- Destination—A destination of the session. The following options are supported:

- Destination: *interface-id*

The Destination is an interface, regular forwarding on the interface is not supported.

- Destination: *interface-id*, network

The Destination is an interface, regular forwarding on the interface is supported.

- Destination: RSPANVLAN*vlan-id*, reflector-port *interface-id*

The switch is the first switch in the RSPAN session, regular forwarding on the interface is not supported.

- Destination: RSPANVLAN*vlan-id*, reflector-port *interface-id*, network

The switch is the first switch in the RSPAN session, regular forwarding on the interface is supported.

42.5 show vlan remote-span

To display a list of remote Switched Port Analyzer (RSPAN) VLANs, use the show vlan remote-span command in User EXEC mode.

Syntax

show vlan remote-span

Parameters

This command has no arguments or keywords

Default Configuration

This command has no default settings.

Command Mode

User EXEC mode

Example

Example. This example shows how to display a list of remote SPAN VLANs:

```
ZEQU0xxxxDL> show vlan remote-span  
Remote SPAN VLAN: 20
```

43 SSH Client Commands

Features in this chapter are not supported.

43.1 ip ssh-client authentication

To define the SSH client authentication method used by the local SSH clients to be authenticated by remote SSH servers, use the `ip ssh-client authentication` command in Global Configuration mode.

To return to default, use the `no` format of the command.

Syntax

```
ip ssh-client authentication {password | public-key {rsa | dsa}}
```

```
no ip ssh-client authentication
```

Parameters

- `password`—Username and password are used for authentication.
- `public-key rsa`—Username and RSA public key are used for authentication.
- `public-key dsa`—Username and DSA public key are used for authentication.

Default Configuration

Username and password are used for authentication by the local SSH clients.

Command Mode

Global Configuration mode

User Guidelines

A user can use the `ip ssh-client key` command to generate/configure RSA/DSA keys if SSH authentication is by public key. Otherwise, the default keys generated by the switch are used.

Example

The following example specifies that, username and public key are used for authentication:

```
ZEQU0xxxxDL (config)# ip ssh-client authentication public-key rsa
```

43.2 ip ssh-client change server password

To change a password of an SSH client on a remote SSH server, use the `ip ssh-client change server password` command in Global Configuration mode.

Syntax

```
ip ssh-client change server password server {host | ip-address | ipv6-address}  
username username old-password old-password new-password new-password
```

Parameters

- `host`—DNS name of a remote SSH server.
- `ip-address`—Specifies the IP address of a remote SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- `username` —Username of the local SSH clients (1 - 70 characters).
- `old-password` —Old password of the local SSH client (1 - 70 characters).
- `new-password`—New password for the local SSH client (1 - 70 characters). The password cannot include the characters "@" and ":".

Default Configuration

None

Command Mode

Global Configuration mode

User Guidelines

Use the command to change a password on a remote SSH server. Use the `ip ssh-client password` command to change the SSH client password of the switch's SSH client so that it matches the new password set on the remote SSH server.

Example

The following example changes a password of the local SSH clients:

```
ZEQU0xxxxDL(config)# ip ssh-client change server password server 10.7.50.155  
username john old-password &&&00@aaaff new-password &&&00@aaee
```

43.3 ip ssh-client key

To create a key pair for SSH client authentication by public key (either by generating a key or by importing a key), use the `ip ssh-client key` command in Global Configuration mode. To remove a key, use the `no` form of the command.

Syntax

```
ip ssh-client key {dsa | rsa} {generate | key-pair privkey pubkey}
```

```
no ip ssh-client key [dsa | rsa]
```

Parameters

- `dsa`—DSA key type.
- `rsa`—RSA key type.
- `key-pair`—Key that is imported to the device.
 - `privkey`—Plaintext private key.
 - `pubkey`—The plaintext public key.

Default Configuration

The application creates a key automatically; this is the default key.

Command Mode

Global Configuration mode

User Guidelines

When using the keyword `generate`, a private key and a public key of the given type (RSA/DSA) are generated for the SSH client. Downloading a configuration file with a Key Generating command is not allowed, and such download will fail.

When using the keyword `key-pair`, the user can import a key-pair created by another device. In this case, the keys must follow the format specified by RFC 4716.

If the specified key already exists, a warning will be issued before replacing the existing key with a new key.

Use the `no ip ssh-client key` command to remove a key pair. Use this command without specifying a key-type to remove both key pairs.

Table 4 describes the expected behavior of keys, default and users within the various operations.

Table 4: Keys, Defaults and Users

From/To	Show	Show (detailed)	Copy/Upload of Running Config	Copy/Upload of Startup Config	Download text-based CLI (TFTP/Backup)
Startup Config	Only user-defined	N/A	All keys (default and user)	N/A	All keys (default and user)
Running Config	Keys are not displayed.	All keys (default and user)	N/A	Only user defined.	Same as user configuration
Text-based CLI (TFTP/Backup)	As it was copied.	N/A	All keys (default and user)	Only user defined.	As a text file.

If no keys are included in text-based configuration file, the device generates its own keys during initialization. If the Running Configuration contains default keys (not user-defined), the same default keys remain.

Examples

Example 1 - In the following example, a key pair of the RSA type is created:

```
ZEQU0xxxxDL(config)# ip ssh-client key rsa generate
```

The SSH service is generating a private RSA key.
This may take a few minutes, depending on the key size.

Example 2 - In the following example, both public and private keys of the RSA type are imported (private key as plaintext):

```
ZEQU0xxxxDL (config) # ip ssh-client key rsa key-pair
```

Please paste the input now, add a period (.) on a separate line after the input

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDH6CU/2KYRl8rYrK5+TlvwS4zvhBmIC4I31m9cR/1iRTFViMRUj++Ter
p9ssqWyI1Ti9d0jzmG0N3jHzp2je5/DUTHZXvYaUzchBDnsPTJo8dyiB14YBqYHQgCjUhk
tXqvloy+1uxRJTAaLVXCBAmuIU/kMLoEox8/zwjB/jsF9wIBIwKBG2xZ5mQmvy0+yo2GU
FwIQ05f0yweuM11J8McTmqDgfVTRrdbroXwbs3exVqsfaUPY9wa8Le6JPX+DPp4XovEfC/
igIZBSC8SeDmI2U7D6HrkAyD9HHf/r32jukB+5Z7B1HPz2Xczs2c100wrnToy+YTzjLUxy
WS7V/IxbB11ipLAkEA/QUVSCfFmdMIzXaEfJVzqP01cF8guovsWLteBf/gqHuvbHuNy0t
OWEp0bKZs1m/mtCWppkgcgrB0oJaYbUFQJBAMo/cCrkyhsiV/+ZsryeD26NbPEKiaK16V
Tz2ayDstidGuuvcm2YF7DjM6n6NYz3+/ZLyc5n82okbld1NhDONsCQQCmSAas+C4HaHqn
zSU+/IWIDI88As4qJN2DMmGJbtsbVHhQxWIIHAG4tBVWa8bV12+RPYuan/jnk8irniGyVza
FPaKEAiQ8oV+1XYxA8V39V/a42d7FvRjMckUmKD14Rmt32+u9i6sFzaWcdgs87+2vS3AZQ
afQDE5U6YSMIGLVewC4YWwJBAOFZmh0+dIlxT81rzf2cUZGggopfnX6Y+L+YI09MuZHbWH
tXaBGj6ayMYvXnloNecApBjGEm37YVwKj02DV2w=
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMfoJT/YphGXytsrns5Mi/BLj0+EGaILgjFwb1xH/WJFMVWixG4n75MSun2yyp
b1jVOL13SPOYbQ3eMfOna7n8NRMdle9hpTNyEE0ew9Mmjx3KIGXhgGpgdCAKNSGS1eq+W
jL7W7FEIMBotVcIECa4hT+QwugSjHz/PCMH+OwX3AgEj
-----END RSA PUBLIC KEY-----
```

Example 3 - In the following example, both public and private keys of the DSA type are imported (private key as encrypted):

```
ZEQU0xxxxDL (config) # encrypted ip ssh-client key rsa key-pair
```

(Need to encrypted SSH client RSA key pair, for example:)

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
gxe0js60zGRtL4qstmQg1B/4gexQbIfa56RdjgHAMEjvUT02eIYmNi+m4aTu6mlyXPHmYP
lXlXny7jZkHRvgg8EzcpeEB003yQzq3kNi756cMg40qbkm7TU0tdqYFEz/h8rJJ0QvUFfh
BsEQ3e16E/OPitWgK43WTzedsuyFeOoMXR9BCuxPUJc2UeqQVM2IjT50M0FbVt0S6oqXhG
sEEEdotIhIDwHWg97FcV7x+bEnPfzFGmrbrUxcx0xIkFsuCNo3/94PHK8zEXyWtrx2KocDQ
qFRuM8uecpjmdh6M02GURUVstctohEWEIVCI0r5SBCbciaxv5oS0jIzXMrJA==
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBALL0eh3css8tBL8ujFt3trcX0XJyJLlxt4sGp8Q3ExISRN25+Mcac6togpIEg
tIzk6t1IEJscuAih9Brwh1ovgMLRaMe25j5Yj04xG6Fp42nhHiRcie+YTS1o309EdZkiXa
QeJtLdnYL/r3uTIRVGBX15nxtfWpWegxxDwfqzHAgEj
-----END RSA PUBLIC KEY-----
```

Example 4 - In the following example, a DSA key pair is removed:

```
ZEQU0xxxxDL(config)# no ip ssh-client key dsa
```

Example 5 - In the following example, all key pairs (RSA and DSA types) are removed.

```
ZEQU0xxxxDL(config)# no ip ssh-client key
```

43.4 ip ssh-client password

To configure the password for SSH client authentication by password, use the `ip ssh-client password` command in Global Configuration mode. To return to default, use the `no` form of the command.

Syntax

`ip ssh-client password string`

`no ip ssh-client password`

Parameters

- `string`—Password for the SSH clients (1 - 70 characters). The password cannot include the characters "@" and ":".

Default Configuration

The default password is anonymous.

Command Mode

Global Configuration mode

User Guidelines

If authentication is configured to use a password (using the command `ip ssh-client authentication`), use the `ip ssh-client password` command to define the password.

Example

The following example specifies a plaintext password for the local SSH clients:

```
ZEQU0xxxxDL(config)# ip ssh-client password &&&111aaff
```

43.5 ip ssh-client server authentication

To enable remote SSH server authentication by the SSH client, use the `ip ssh-client server authentication` command in Global Configuration mode.

To disable remote SSH server authentication, use the `no` form of the command.

Syntax

`ip ssh-client server authentication`

`no ip ssh-client server authentication`

Parameters

This command has no arguments or keywords.

Default Configuration

SSH server authentication is disabled

Command Mode

Global Configuration mode

User Guidelines

When remote SSH server authentication is disabled, any remote SSH server is accepted (even if there is no entry for the remote SSH server in the SSH Trusted Remote Server table).

When remote SSH server authentication is enabled, only trusted SSH servers are accepted. Use the `ip ssh-client server fingerprint` command to configure trusted SSH servers.

Example

The following example enables SSH server authentication:

```
ZEQU0xxxxDL(config)# ip ssh-client server authentication
```

43.6 ip ssh-client server fingerprint

To add a trusted server to the Trusted Remote SSH Server Table, use the `ip ssh-client server fingerprint` command in Global configuration mode. To remove an entry or all entries from the Trusted Remote SSH Server Table, use the `no` form of the command.

Syntax

```
ip ssh-client server fingerprint {host | ip-address} fingerprint
```

```
no ip ssh-client server fingerprint [host | ip-address]
```

Parameters

- `host`—DNS name of an SSH server.
- `ip-address`—Specifies the address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- `fingerprint`—Fingerprint of the SSH server public key (32 Hex characters).

Default Configuration

The Trusted Remote SSH Server table is empty.

Command Mode

Global Configuration mode

User Guidelines

Fingerprints are created by applying a cryptographic hash function to a public key. Fingerprints are shorter than the keys they refer to, making it simpler to use (easier to manually input than the original key). Whenever the switch is required to authenticate an SSH server's public key, it calculates the received key's fingerprint and compares it to the previously-configured fingerprint.

The fingerprint can be obtained from the SSH server (the fingerprint is calculated when the public key is generated on the SSH server).

The `no ip ssh-client server fingerprint` command removes all entries from the Trusted Remote SSH Server table.

Example

In the following example, a trusted server is added to the Trusted Servers table (with and without a separator ":"):

```
ZEQU0xxxxDL(config)# ip ssh-client server fingerprint 1.1.1.1
DC789788DC88A988127897BCBB789788

ZEQU0xxxxDL(config)# ip ssh-client server fingerprint 1.1.1.1
DC:78:97:88:DC:88:A9:88:12:78:97:BC:BB:78:97:88
```

43.7 ip ssh-client source-interface

To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 SSH servers, use the `ip ssh-client source-interface` Global Configuration mode command. To restore the default configuration, use the `no` form of this command.

Syntax

```
ip ssh-client source-interface interface-id
```

```
no ip ssh-client source-interface
```

Parameters

- `interface-id`—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL (config)# ip ssh-client source-interface vlan 10
```

43.8 ipv6 ssh-client source-interface

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 SSH servers, use the `ipv6 ssh-client source-interface` Global Configuration mode command. To restore the default configuration, use the `no` form of this command.

Syntax

`ipv6 ssh-client source-interface interface-id`

`no ipv6 ssh-client source-interface`

Parameters

- `interface-id`—(Optional) Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL(config)# ipv6 ssh-client source-interface vlan 10
```

43.9 ip ssh-client username

To configure the SSH client username of the switch, use the `ip ssh-client username` command in Global Configuration mode.

To return to default, use the `no` form of the command.

Syntax

`ip ssh-client username string`

`no ip ssh-client username`

Parameters

- `string`—Username of the SSH client. The length is 1 - 70 characters. The username cannot include the characters "@" and ":".

Default Configuration

The default username is anonymous

Command Mode

Global Configuration mode

User Guidelines

The configured username is used when SSH client authentication is done both by password or by key.

Example

The following example specifies a username of the SSH client:

```
ZEQU0xxxxDL(config)# ip ssh-client username jeff
```

43.10 show ip ssh-client

To display the SSH client credentials, both default and user-defined keys, use the show ip ssh-client command in Privilege EXEC mode.

Syntax

```
show ip ssh-client
```

```
show ip ssh-client {mypubkey | key} {dsa | rsa}
```

Parameters

- dsa—Specifies displaying the DSA key type.
- rsa—Specifies displaying the RSA key type.
- mypubkey—Specifies that only the public key is selected to be displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Use the command with a specific key-type to display the SSH client key; You can either specify display of public key or private key, or with no parameter to display both private and public keys. The keys are displayed in the format specified by RFC 4716.

Examples

Example 1. The following example displays the authentication method and the RSA public key:

```
ZEQU0xxxxDL# show ip ssh-client mypubkey rsa
```

```
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
```

```
----- BEGIN SSH2 PUBLIC KEY ----- Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAudGEIaPARsKoVJVjs8XALAKqBN1WmXnY
kUf5oZjGY3QoMGDvNipQvdN3YmwLUBiKk31WvVwFB3N2K5a7fUBjoblkdjns
QKTKZiu4V+IL5rds/bD6LOEkJbjUz0jmp9hIikh9uc0ceZ3ZxMtKhNORLrXL
aRyxYsz05FuirTo6xW8=
----- END SSH2 PUBLIC KEY -----
```

```
Public Key Fingerprint: 84:f8:24:db:74:9c:2d:51:06:0a:61:ef:82:13:88:88
```

Example 2. The following example displays the authentication method and DSA private key in encrypted format:

```
ZEQU0xxxxDL# show ip ssh-client key DSA
```

```
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:      DSA key
Username:                   john
Key Source:                 User Defined
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
```

```
----- BEGIN SSH2 PUBLIC KEY ----- Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxahvx5wOJ0rzZdzoS0XxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnD1aBDHtbIQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI140m1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfXOD2s9Rd7NBvQAAAIEA1N92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
JO/RHd+NjB4eo1D+Odix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKW0ocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1v0+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnFOGDI B3VVmxHLMxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
----- END SSH2 PUBLIC KEY -----
```

```
----- BEGIN SSH2 PRIVATE KEY ----- Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxahvx5wOJ0rzZdzoS0XxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnD1aBDHtbIQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI140m1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfXOD2s9Rd7NBvQAAAIEA1N92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
JO/RHd+NjB4eo1D+Odix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKW0ocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1v0+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnFOGDI B3VVmxHLMxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
----- END SSH2 PRIVATE KEY -----
```

Example 3. The following example displays the SSH client authentication method, the username and the password:

```
ZEQU0xxxxDL# show ip ssh-client
```

```
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:      DSA key
Username:                   anonymous (default)
Password:                   anonymous (default)
password (Encrypted):       KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5nsxSxwic=
```

43.11 show ip ssh-client server

To display the SSH remote server authentication method and the Trusted Remote SSH Server table, use the `show ip ssh-client server` command in Privilege EXEC Configuration mode.

Syntax

```
show ip ssh-client server [host | ip-address]
```

Parameters

- `host`—(Optional) DNS name of an SSH server.
- `ip-address`—(Optional) IP Address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

Default Configuration

None

Command Mode

Privileged EXEC mode

User Guidelines

If a specific SSH server is specified, only the fingerprint of this SSH server is displayed. Otherwise, all known servers are displayed.

Examples

Example 1 - In the following example, the SSH remote server authentication method and all trusted remote SSH servers are displayed:

```
ZEQUOxxxxDL# show ip ssh-client server SSH Server
Authentication is enabled server address: 11.1.0.1
  Server Key Fingerprint: 5a:8d:1d:b5:37:a4:16:46:23:59:eb:44:13:b9:33:e9 server
address: 192.165.204.111
  Server Key Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9 server
address: 4002:0011::12
  Server Key Fingerprint: a5:34:44:44:27:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

Example 2 - The following example displays the authentication method and DSA private key in encrypted format:

```
ZEQU0xxxxDL# show ip ssh-client key DSA
```

```
Authentication method:    DSA key
Username:                  john
Key Source:                Default
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
```

```
----- BEGIN SSH2 PUBLIC KEY ----- Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaeHvx5w0J0rzZdzoS0XxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnD1aBDHtbIQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI140m1eg9e4NnCRleaQoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfXOD2s9Rd7NBvQAAAIEA1N92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
JO/RHd+NjB4eo1D+OdiX6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetZrtOKW0ocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1v0+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjKEb11juqnFOGDI B3VVmxHLMxnAz643WK4Z27dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
----- END SSH2 PUBLIC KEY -----
```

```
----- BEGIN SSH2 PRIVATE KEY ----- Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaeHvx5w0J0rzZdzoS0XxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnD1aBDHtbIQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI140m1eg9e4NnCRleaQoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfXOD2s9Rd7NBvQAAAIEA1N92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
JO/RHd+NjB4eo1D+OdiX6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetZrtOKW0ocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1v0+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjKEb11juqnFOGDI B3VVmxHLMxnAz643WK4Z27dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
----- END SSH2 PRIVATE KEY -----
```

Example 3 - The following example displays the SSH client authentication method, the username and the password:

```
ZEQU0xxxxDL# show ip ssh-client Authentication
method: password (default) Username: anonymous
(default)
password (Encrypted) : KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5
```

44 Stack Commands

44.1 stack unit

To place the user in the context of the specified stack unit or all stack units, use the stack unit Global Configuration command.

Syntax

stack unit {unit-id | all}

Parameters

- unit-id— Select a specific unit. All commands after this command refer to this unit. Unit must be member in the stack. (Range: 1–2).
- all—Select all the units in the stack.

Default Configuration

None

Command Mode

GlobalConfiguration mode

Examples

Example 1—The following example sets the unit context to 2, all following stack command will apply to unit 2.

```
ZEQU0xxxxDL (config) # stack unit 2
```

Example 2—The following example sets the unit context to all units in the stack, all following stack command will apply to all the units.

```
ZEQU0xxxxDL (config) # stack unit all
```

44.2 stack

To configure the ports and unit id after reboot, use the stack command.

Syntax

```
stack {[links ports-list] [unit-id {unit-id | auto}] }
```

no stack

Parameters

- links— Select port list to be used as stack links after reload.
- ports-list - a list of one or more stack ports separated by comma, or a range of sequential ports marked by dash.
- unit-id— Select the unit id to be used after reload. (Range: 1–2). Use auto to enable stack auto numbering feature.

Default Configuration

None

Command Mode

GlobalConfiguration mode

StackUnitmode.

User Guidelines

- Running the command in GlobalConfiguration mode will configure the current stack master unit.
- The no stack is used to return the stack to factory default after reload (use the reload command to reboot unit).
- Running the command in stack unit all context and configuration of the unit-id parameter not to auto generate an error (to avoid setting several units to the same Id).
- Optional parameters not provided in the command will not be changed.
-
- Setting the unit-id not to auto require the links to configured to a non empty port list.

Examples

Example 1—The following example sets the master unit to stack factory default.

```
ZEQU0xxxxDL (config) # no stack
```

Example 2—The following example sets the unit 1 to have stack links (ports) gi15-16 with unit ID auto.

```
ZEQU0xxxxDL (config) # stack unit 1  
ZEQU0xxxxDLunit# stack links te 15-16 unit-id auto
```

44.3 show stack configuration

To display the stack configuration (including configuration that is configured after reboot) parameters, use the show stack configuration EXEC mode command.

Syntax

show stack configuration

Parameters

N/A

Default Configuration

N/A.

Command Mode

User EXEC mode

Examples

Display the stack configuration information for an entire stack.

ZEQU0xxxxDL# **show stack configuration**

Unit Id After Reboot Configuration		
	Unit Id	Stack Links

1	1	te15-16
2	2	te15-16

44.4 show stack

To display the stack operational status, use the show stack EXEC mode command.

Syntax

show stack

Parameters

N/A

Default Configuration

N/A.

Command Mode

User EXEC mode

Examples

Display the stack information for an entire stack.

ZEQU0xxxxDL# show stack

Units stack mode: Native

Unit Id	MAC Address	Role	Network Port Type	Uplink Port Type
1	00:50:40:00:10:00	master	te	te
2	00:50:40:00:20:00	backup	te	te

44.5 show stack links

To display the stack links operational status, use the show stack links EXEC mode command.

Syntax

show stack links [details]

Parameters

N/A

Default Configuration

N/A.

Command Mode

User EXEC mode

Examples

Example 1—Display the stack links information for an entire stack.

ZEQU0xxxxDL# show stack links

Topology is Chain

Unit Id	Active Links	Neighbor Links	Operational Link Speed	Down/Standby Links
1	te1/0/28	te2/0/28	10G	te1/0/27
2	te1/0/28	te2/0/28	10G	te2/0/27

Example 2—Display the stack links information for an entire stack with details.

ZEQU0xxxxDL# show stack links details

Topology is Chain

UNIT ID	Link	Status	Speed	Neighbor Unit ID	Neighbor Link	Neighbor MAC Address
1	te27	Active	10G	2	te27	00:50:40:3b:c4:a4
1	te28	Active	10G	2	te28	00:50:40:3b:20:a4
2	te27	Active	10G	1	te27	00:50:40:3b:10:88
2	te28	Active	10G	1	te28	00:50:40:3b:10:88

44.6 snmp-server enable traps stack

Configure Stacking trap state.

Syntax

snmp-server enable traps stack

Parameters

N/A

Default Configuration

Enabled

Command Mode

GlobalConfiguration mode

Examples

```
ZEQU0xxxxDL (config)# snmp-server enable traps stack
ZEQU0xxxxDL#
```

45 SYSLOG Commands

45.1 clear logging

To clear messages from the internal logging buffer, use the clear logging Privileged EXEC mode command.

Syntax

clear logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the internal logging buffer.

```
ZEQU0xxxxDL# clear logging  
Clear Logging Buffer ? (Y/N) [N]
```

45.2 clear logging file

To clear messages from the logging file, use the clear logging file Privileged EXEC mode command.

Syntax

clear logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the logging file.

```
ZEQU0xxxxDL# clear logging file
Clear Logging File [y/n]
```

45.3 file-system logging

To enable logging file system events, use the file-system logging Global Configuration mode command. To disable logging file system events, use the no form of this command.

Syntax

file-system logging {copy | delete-rename}

no file-system logging {copy | delete-rename}

Parameters

- copy—Specifies logging messages related to file copy operations.
- delete-rename—Specifies logging messages related to file deletion and renaming operations.

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

The following example enables logging messages related to file copy operations.

```
ZEQU0xxxxDL (config) # file-system logging copy
```

45.4 logging buffered

To limit the SYSLOG message display to messages with a specific severity level, and to define the buffer size (number of messages that can be stored), use the logging buffered Global Configuration mode command. To cancel displaying the SYSLOG messages, and to return the buffer size to default, use the no form of this command.

Syntax

logging buffered [buffer-size] [severity-level | severity-level-name]

no logging buffered

Parameters

- **buffer-size**—(Optional) Specifies the maximum number of messages stored in buffer. (Range: 20–1000)
- **severity-level**—(Optional) Specifies the severity level of messages logged in the buffer. The possible values are: 1-7.
- **severity-level-name**—(Optional) Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is informational. The default buffer size is 1000.

Command Mode

Global Configuration mode

User Guidelines

All the SYSLOG messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example shows two ways of limiting the SYSLOG message display from an internal buffer to messages with severity level debugging. In the second example, the buffer size is set to 100 and severity level informational.

```
ZEQU0xxxxDL (config) # logging buffered debugging
ZEQU0xxxxDL (config) # logging buffered 100 informational
```

45.5 logging console

To limit messages logged to the console to messages to a specific severity level, use the logging console Global Configuration mode command. To restore the default, use the no form of this command.

Syntax

logging console level

no logging console

Parameters

level—Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

Informational.

Command Mode

Global Configuration mode

Example

The following example limits logging messages displayed on the console to messages with severity level errors.

```
ZEQU0xxxxDL(config)# logging console errors
```

45.6 logging file

To limit SYSLOG messages sent to the logging file to messages with a specific severity level, use the logging file Global Configuration mode command. To cancel sending messages to the file, use the no form of this command.

Syntax

logging file level

no logging file

Parameters

level—Specifies the severity level of SYSLOG messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is errors.

Command Mode

Global Configuration mode

Example

The following example limits SYSLOG messages sent to the logging file to messages with severity level alerts.

```
ZEQU0xxxxDL (config) # logging file alerts
```

45.7 logging server

To log messages to the specified SYSLOG server, use the logging server Global Configuration command. To delete the SYSLOG server with the specified address from the list of SYSLOG servers, use the no form of this command.

Syntax

```
logging server {ip-address | ipv6-address | hostname} [port port] [severity level]
[facility facility] [description text]
```

```
no logging server {ipv4-address | ipv6-address | hostname}
```

Parameters

- **ip-address**—IP address of the host to be used as a SYSLOG server. The IP address can be an IPv4, IPv6 or Ipv6z address. See IPv6z Address Conventions.
- **hostname**—Hostname of the host to be used as a SYSLOG server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size for each part of the host name: 63)
- **port port**—(Optional) Port number for SYSLOG messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- **severity level**—(Optional) Limits the logging of messages to the SYSLOG servers to a specified level: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, Debugging.
- **facility facility**—(Optional) The facility that is indicated in the message. It can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7. If unspecified, the port number defaults to local7.
- **description text**—(Optional) Description of the SYSLOG server. (Range: Up to 64 characters)

Default Configuration

No messages are logged to a SYSLOG server.

If unspecified, the severity level defaults to Informational.

Command Mode

Global Configuration mode

User Guidelines

You can use multiple SYSLOG servers.

Examples

```
ZEQU0xxxxDL (config) # logging server 1.1.1.121
```

```
ZEQU0xxxxDL (config) # logging server 3000::100/SYSLOG1
```

45.8 logging on

To enable message logging, use the logging on Global Configuration mode command. This command sends debug or error messages asynchronously to designated locations. To disable the logging, use the no form of this command.

Syntax

logging on

no logging on

Parameters

This command has no arguments or keywords.

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the logging messages distribution at various destinations, such as the logging buffer, logging file or SYSLOG server. Logging on and off at these destinations can be individually configured using the clear logging file, logging console, Global Configuration mode commands.

Example

The following example enables logging error messages.

```
ZEQU0xxxxDL(config)# logging on
```

45.9 logging source-interface

To specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SYSLOG servers, use the logging source-interface Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

logging source-interface interface-id

no logging source-interface

Parameters

interface-id—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to the next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the lowest IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SYSLOG server.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL (config)# logging source-interface vlan 100
```

45.10 logging source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 SYSLOG servers, use the logging source-interface-ipv6 Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

logging source-interface-ipv6 interface-id

no logging source-interface-ipv6

Parameters

interface-id—Specifies the source interface.

Default Configuration

The IPv6 source address is the defined IPv6 address of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SYSLOG server.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL (config)# logging source-interface-ipv6 vlan 100
```

45.11 logging aggregation on

To control aggregation of SYSLOG messages, use the logging aggregation on Global Configuration mode command. If aggregation is enabled, logging messages are displayed every time interval (according to the aging time specified by logging aggregation aging-time). To disable aggregation of SYSLOG messages, use the no form of this command.

Syntax

logging aggregation on

no logging aggregation on

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

Example

To turn off aggregation of SYSLOG messages:

```
ZEQU0xxxxDL (config)# no logging aggregation on
```

45.12 logging aggregation aging-time

To configure the aging time of the aggregated SYSLOG messages, use the logging aggregation aging-time Global Configuration mode command. The SYSLOG messages are aggregated during the time interval set by the aging-time parameter. To return to the default, use the no form of this command.

Syntax

logging aggregation aging-time sec

no logging aggregation aging-time

Parameters

aging-time sec—Aging time in seconds (Range: 15–3600)

Default Configuration

300 seconds.

Command Mode

Global Configuration mode

Example

```
ZEQU0xxxxDL (config)# logging aggregation aging-time 300
```

45.13 logging origin-id

To configure the origin field of the SYSLOG message packet headers sent to the SYSLOG server, use the logging origin-id Global Configuration mode command. To return to the default, use the no form of this command.

Syntax

logging origin-id {hostname | IP | IPv6 | string user-defined-id}

no logging origin-id

Parameters

- hostname—The system hostname will be used as the message origin identifier.
- IP—IP address of the sending interface that is used as the message origin identifier.
- IPv6—IPv6 address of the sending interface that is used as the message origin identifier. If the sending interface is IPv4, the IPv4 address will be used instead.
- string user-defined-id—Specifies an identifying description chosen by the user. The user-defined-id argument is the identifying description string.

Default Configuration

No header is sent apart from the PRI field.

Command Mode

Global Configuration mode

Example

```
ZEQU0xxxxDL(config)# logging origin-id string "Domain 1, router B"
```

45.14 **show logging**

To display the logging status and SYSLOG messages stored in the internal buffer, use the show logging Privileged EXEC mode command.

Syntax

show logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the internal buffer.

ZEQU0xxxxDL# **show logging**

2001/01/01 05:25:03 :%AAA-I-CONNECT: User CLI session for user manager over console , source 0.0.0.0
destination 0.0.0.0 ACCEPTED

45.15 **show logging file**

To display the logging status and the SYSLOG messages stored in the logging file, use the show logging file Privileged EXEC mode command.

Syntax

show logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the logging file.

```
ZEQU0xxxxDL# show logging file
```

```
2001/01/04 05:05:31 :%UNQ-C-UNQ-CDB-Error: Function UNQP_cdb_config_finished_hook:
UNQP_voiceVlan_MIB_config Failed
```

```
2001/01/04 05:05:31 :%MNG_DIAG-E-DIAGATINIT: Init: Entry already exists
```

```
2001/01/01 00:02:01 :%UNQ-C-UNQ-CDB-Error: Function UNQP_cdb_config_finished_hook:
UNQP_voiceVlan_MIB_config Failed
```

45.16 **show syslog-servers**

To display the SYSLOG server settings, use the show syslog-servers Privileged EXEC mode command.

Syntax

show syslog-servers

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example provides information about the SYSLOG servers.

ZEQU0xxxxDL# **show syslog-servers**

Source IPv4 interface: vlan 1

Source IPv6 interface: vlan 10

Device Configuration

IP address	Port	Facility	Severity	Description
1.1.1.121	514	local7	info	
3000::100	514	local7	info	

46 System Management Commands

46.1 disable ports leds

To turn off the LEDs on all ports on a device, use the disable ports leds Global Configuration mode command.

To set the LEDs of all the ports on the device to their current operational status of the port, use the no disable ports leds command.

Syntax

disable ports leds

no disable ports leds

Parameters

This command has no arguments or keywords.

Default Configuration

The default is no disable port leds; that is the LEDs of all the ports reflect their current status.

Command Mode

Global Configuration mode

Examples

The following example turns off the port LEDs.

```
ZEQU0xxxxDL (conf ig) # disable ports leds
```

46.2 hostname

To specify or modify the device host name, use the hostname Global Configuration mode command. To remove the existing host name, use the no form of the command.

Syntax hostname

name no hostname

Parameters

Name—Specifies the device host name. (Length: 1-58 characters). The hostname must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens.

Default Configuration

No host name is defined.

Command Mode

Global Configuration mode

Example

The following example specifies the device host name as 'enterprise'.

```
ZEQU0xxxxDL (config)#hostname enterprise
enterprise (config)#
```

46.3 resume

To enable switching to another open Telnet session, use the resume EXEC mode command.

Syntax

resume [connection]

Parameters

connection—(Optional) Specifies the connection number. (Range: 1-4 connections.)

Default Configuration

The default connection number is that of the most recent connection.

Command Mode

Privileged EXEC mode

Example

The following command switches to open Telnet session number 1.

```
ZEQU0xxxxDL> resume 1
```

46.4 service cpu-utilization

To enable measuring CPU utilization, use the service cpu-utilization Global Configuration mode command. To restore the default configuration, use the no form of this command.

Syntax

service cpu-utilization

no service cpu-utilization

Parameters

This command has no arguments or keywords.

Default Configuration

Measuring CPU utilization is enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the service cpu utilization command to measure information on CPU utilization.

Example

The following example enables measuring CPU utilization.

```
ZEQU0xxxxDL (config) # service cpu-utilization
```

46.5 show cpu input rate

To display the rate of input frames to the CPU in packets per seconds (pps), use the show cpu input rate Privileged EXEC mode command.

Syntax

```
show cpu input rate
```

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays CPU input rate information.

```
ZEQU0xxxxDL# show cpu input rate  
Input Rate to CPU is 1030 pps.
```

46.6 show cpu utilization

To display information about CPU utilization, use the show cpu utilization Privileged EXEC mode command.

Syntax

show cpu utilization

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

Privileged EXEC mode

User Guidelines

Use the show cpu-utilization command to enable measuring CPU utilization.

Example

The following example displays CPU utilization information.

```
ZEQU0xxxxDL# show cpu utilization
CPU utilization service is on. CPU utilization
-----
five seconds: 5%; one minute: 3%; five minutes: 3%
```

46.7 show environment

To display environment information, use the show environment EXEC mode command.

Syntax

show environment {all | power | fan | temperature {status} | stack [switch-number]}

Parameters

- all—Displays the fan and temperature general status
- power - Display the power supply status
- fan—Displays the fan status
- temperature status—Displays the temperature status
- stack switch-number—(Optional) Displays detailed environment status of a stack. If the switch-number is specified, the environment status of the selected device number is displayed. (Range: 1 – 2)

Command Mode

User EXEC mode

User Guidelines

The power parameters displays power supply information.

Main Power supply statuses:

- Power Supply1 : Connected or Not Connected.
- Power Supply2 : Connected or Not Connected.

The fan and temperature status parameters are available only on devices on which FAN and/or temperature sensor are installed. Fan

status can be one of:

- Fans OK, redundant fan Ready - The fan/s functions correctly.
- Fans OK, redundant fan Active - One of the fans failed and is backed-up by the redundant fan.
- Fail - Several fans failed.
- N/A - No fan installed.

Sensor status can be one of:

- OK - The sensor/s functions correctly.
- Failure - The sensor/s failed.
- NA - No sensor is installed.

Temperature can be one of:

- OK - The temperature is below the warning threshold.
- Warning- The temperature is between the warning threshold to the critical threshold.
- Critical - the temperature is above the critical threshold.

Examples

Example 1 - The following example displays the general environment status of a device or a stack.

```
ZEQU0xxxxDL> show environment all
```

```
Power Supply1 Not Connected.  
Power Supply2 Connected.
```

```
FANs OK  
TEMPERATURE is OK
```

Example 2 - The following example displays the general FAN status of a device or a stack.

```
ZEQU0xxxxDL> show environment fan
```

```
FANs OK
```

Example 3 - The following example displays the detailed temperature status of a device or a stack.

```
ZEQU0xxxxDL> show environment temperature status
```

```
TEMPERATURE is Warning
```

Example 4 - The following example displays the detailed environment status of a stack.

```
ZEQU0xxxxDL> show environment stack
```

Unit	FAN	Status

1		FANs OK
Unit	Sensor	Temperature
	Status	

1	OK	OK

46.8show inventory

To display system information, use the show inventory EXEC mode command.

Syntax

show inventory [entity]

Parameters

entity—Specifies the entity to be displayed. It can be a number (1 - 8) for a specific unit number, or an interface (Ethernet) name.

Command Mode

User EXEC mode

Examples

Example 1 - The following example displays all the entities in a standalone system.

```
ZEQU0xxxxDL> show inventory
```

```
NAME: "1"   DESCR: "ZEQUO 4500DL 24G+4XG Stackable Switch"  
PID: ZEQUO 4500DL   VID: 000001   SN: 71P12345678
```

Example 2 - The following example displays a specific entity in a standalone system.

```
ZEQU0xxxxDL> show inventory gigabitethernet1/0/25
```

```
NAME: "TenGigabitEthernet1/0/25" DESCR: "Panasonic 10G LR Module"  
PID: PN59023   VID: V01   SN: 71C12345678
```

46.9 show reboot

To display whether there is a pending reload for status of the device, use the show reload Privileged EXEC mode command.

Syntax

show reload

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

Privileged EXEC mode

User Guidelines

You can use this command to display a pending software reload. To cancel a pending reload, use this command with the cancel parameter.

Example

The following example displays that reboot is scheduled for 00:00 on Saturday, April-20.

```
ZEQU0xxxxDL> show reboot
```

```
Reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
```

46.10 show sessions

To display open Telnet sessions, use the show sessions EXEC mode command.

Syntax

show sessions

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

User Guidelines

The show sessions command displays Telnet sessions to remote hosts opened by the current Telnet session to the local device. It does not display Telnet sessions to remote hosts opened by other Telnet sessions to the local device.

Example

The following example displays open Telnet sessions.

```
ZEQU0xxxxDL> show sessions
```

Connection	Host	Address	Port	Byte
1	Remote router	172. 16. 1. 1	23	89
2	172. 16. 1. 2	172. 16. 1. 2	23	8

The following table describes significant fields shown above.

Field	Description
Connection	The connection number.
Host	The remote host to which the device is connected through a Telnet session.
Address	The remote host IP address.
Port	The Telnet TCP port number.
Byte	The number of unread bytes for the user to see on the connection.

46.11 **show system**

The show system EXEC mode command displays system information.

Syntax

show system unit unit-id

Parameters

unit-id—Specifies the unit number. (Range: 1 – 2)

Command Mode

User EXEC mode

Example

```
ZEQU0xxxxDL# show system
System Description:           ZEQU0 xxxxDL
System Up Time (days, hour:min:sec): 01, 02:51:52
System Contact:
System Name:                  ZEQU0xxxxDL
System Location:
System MAC Address:           00:50:40:xx:xx:xx
System Object ID:             1.3.6.1.4.1.396.5.4.1.44
```

Unit	Type
1	ZEQU0 5410DL

Unit	Power Supply1	Power Supply2
1	Not Connected	Connected

Unit	Fans Status
1	FANs OK

Unit	Temperature (Celsius)	Status
1	48	OK

46.12 show system languages

To display the list of supported languages, use the show system languages EXEC mode command.

Syntax

show system languages

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays the languages configured on the device. Number of Sections indicates the number of languages permitted on the device.

```
ZEQU0xxxxDL# show system languages
*accepted language(s) :
```

language Name	Unicode Name	Code	NumOfSections
English	English	en-US	2
Japanese	μ ùÑ μ &%F-P	ja-JP	2

46.13 show system tcam utilization

To display the Ternary Content Addressable Memory (TCAM) utilization, use the show system tcam utilization EXEC mode command.

Syntax

show system tcam utilization [unit unit-id]

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays TCAM utilization information.

ZEQU0xxxxDL> show system tcam utilization	
System: 3%	
Unit	TCAM utilization[%]
-----	-----
1	3
2	3

46.14 how services tcp-udp

To display information about the active TCP and UDP services, use the show services tcp-udp Privileged EXEC mode command.

Syntax

show services tcp-udp

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

The output does not show sessions where the device is a TCP/UDP client.

Examples

ZEQU0xxxxDL> show services tcp-udp

Type	Local IP Address	Remote IP address	Service Name	State
TCP	All:22		SSH	LISTEN
TCP	All:23		Telnet	LISTEN
TCP	All:80		HTTP	LISTEN
TCP	All:443		HTTPS	LISTEN
TCP	172. 16. 1. 1:23	172. 16. 1. 18:8789	Telnet	ESTABLISHED
TCP6	All-23		Telnet	LISTEN
TCP6	fe80::200:b0ff:fe00:0-23		Telnet	
	fe80::200:b0ff:fe00:0-8999			ESTABLISHED
UDP	All:161		SNMP	
UDP6A	II-161		SNMP	

46.15 **debug show tech-support**

To display system and configuration information that can be provided to the Technical Assistance Center when reporting a problem, use the debug show tech-support EXEC mode command.

Syntax

debug show tech-support [config | memory]

Parameters

- memory—(Optional) Displays memory and processor state data.
- config—(Optional) Displays switch configuration within the CLI commands supported on the device.

Default Configuration

By default, this command displays the output of technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

Command Types

Switch command.

Command Mode

User EXEC mode

User Guidelines

Caution: Avoid running multiple debug show tech-support commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

The debug show tech-support command may time out if the configuration file output takes longer to display than the configured session time out time. If this happens, enter a set logout timeout value of 0 to disable automatic disconnection of idle sessions or enter a longer timeout value.

The debug show tech-support command output is continuous, meaning that it does not display one screen at a time. To interrupt the output, press Esc.

If the user specifies the memory keyword, the debug show tech-support command displays the following output:

- Flash info (dir if exists, or flash mapping)
- Output of command show bootvar
- Buffers info (like print os buff)
- Memory info (like print os mem)
- Proc info (like print OS tasks)
- Versions of software components
- Output of command show cpu utilization

46.16 show system fans

To view the status of the fans on the device, use the show system fans EXEC mode command.

Syntax

show system fans [unit-id]

Parameters

unit-id—(Optional) Specifies the unit number to be reloaded. (Range: 1 – 2). If unspecified, displays information for all the units.

Command Mode

User EXEC mode

Examples

Example 1: For devices whose hardware supports variable fan speed.

ZEQU0xxxxDL> **show system fans**

Unit	State
1	FANs OK

46.17 **show system sensors**

To view the temperature sensor status, use the show system sensors EXEC mode command.

Syntax

show system sensors

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Examples

For systems with a single sensor status

ZEQU0xxxxDL> **show system sensors**

Unit	Sensor	Status	Temperature (C)	Warning Alarm Temp(C)	Critical Alarm Temp(C)
1		OK	46	89	93

46.18 **show system power-supply**

To view the power-supply status, use the show system power-supply EXEC mode command.

Syntax

show system power-supply

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

User Guidelines

Power supply supported:

- Main (internal power supply).

Main Power supply statuses:

- Power Supply1 : Connected or Not Connected.
- Power Supply2 : Connected or Not Connected.

Examples

ZEQU0xxxxDL> **show system power-supply**

Unit	Power Supply	Status
1	Power Supply1	Not Connected
1	Power Supply2	Connected:

46.19 show system id

To display the system identity information, use the show system id EXEC mode command.

Syntax

show system id [unit unit-id]

Parameters

unit unit-id—(Optional) Unit number or all. If unspecified, defaults to all. (Range: 1 – 2)

Command Mode

User EXEC mode

Example

The following example displays the system identity information.

ZEQU0xxxxDL> **show system id**

Unit	Serial number
-----	-----
1	79P12345678

46.20 **show ports leds configuration**

To display whether the LEDs of the ports are enabled or disabled, use the show port leds configuration EXEC mode command.

Syntax

```
show ports leds configuration
```

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

Examples

Example 1: The following example displays the status of the port's LEDs when they are turned on.

```
ZEQU0xxxxDL> show ports leds configuration
```

```
Port leds are not disabled
```

Example 2: The following example displays the status of the port LEDs when they are turned off.

```
ZEQU0xxxxDL> show port leds configuration
```

```
Port leds are disabled
```

46.21 show users

To display information about the active users, use the show users EXEC mode command.

Syntax

show users

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays information about the active users.

```
ZEQU0xxxxDL> show users
```

Username	Protocol	Location
-----	-----	-----
Bob	Serial	
John	SSH	172. 16. 0. 1
Robert	HTTP	172. 16. 0. 8
Betty	Telnet	172. 16. 1. 7
Sam		172. 16. 1. 6

46.22 **show hardware version**

To display hardware version information, use the show hardware version EXEC mode command.

Syntax

show hardware version[unit unit-id]

Parameters

- unit—(Optional) Specifies the unit number. (Range: 1 – 2)

Default Usage

Show hardware version on all units if no unit is specified.

Command Mode

User EXEC mode

Example

The following example displays hardware version information.

ZEQU0xxxxDL> **show hardware version**

Unit	HW version
1	000001

46.23 **system recovery**

To set the system to automatically recover from temperature that reached the critical threshold, use the system recovery Global Configuration command.

To return to disable automatic recovery, use the no form of the command.

Syntax

system recovery

no system recovery

Parameters

This command has no arguments or keywords.

Default Configuration

System recovery is enabled by default.

Command Mode

Global Configuration mode

Example

```
ZEQU0xxxxDL (config) # no system recovery
```

47 TACACS+Commands

47.1 tacacs-server host

To specify a TACACS+ host, use the tacacs-server host Global Configuration mode command. To delete the specified TACACS+ host, use the no form of this command.

Syntax

```
tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [priority priority]
```

```
no tacacs-server host {ip-address | hostname}
```

Parameters

- host ip-address—Specifies the TACACS+ server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.
- host hostname—Specifies the TACACS+ server host name. (Length: 1-158 characters. Maximum label length of each part of the host name: 63 characters)
- single-connection—(Optional) Specifies that a single open connection is maintained between the device and the daemon, instead of the device opening and closing a TCP connection to the daemon each time it communicates.
- port port-number—(Optional) Specifies the TACACS server TCP port number. If the port number is 0, the host is not used for authentication. (Range: 0-65535)
- timeout timeout—(Optional) Specifies the timeout value in seconds. (Range: 1-30)
- key key-string—(Optional) Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Length: 0-128 characters). If this parameter is omitted, the globally-defined key (set in the tacacs-server key command tacacs-server host source-interface command) will be used.
- priority priority—(Optional) Specifies the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

Default Configuration

No TACACS+ host is specified. The default port-number is 1812.

If timeout is not specified, the global value (set in the tacacs-server timeout command) is used.

If key-string is not specified, the global value (set in the tacacs-server key command) is used.

Command Mode

Global Configuration mode

User Guidelines

Multiple tacacs-server host commands can be used to specify multiple hosts.

Example

The following example specifies a TACACS+ host.

```
ZEQU0xxxxDL (config) # tacacs-server host 172.16.1.1
```

47.2 tacacs-server host source-interface

To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 TACACS+ servers, use the `tacacs-server host source-interface` Global Configuration mode command. To restore the default configuration, use the `no` form of this command.

Syntax

`tacacs-server host source-interface interface-id`

`no tacacs-server host source-interface`

Parameters

- `interface-id`—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 TACACS+ server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL (config)# tacacs-server host source-interface vlan 100
```

47.3 tacacs-server host source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 TACACS+ servers, use the `tacacs-server host source-interface-ipv6` Global Configuration mode command. To restore the default configuration, use the `no` form of this command.

Syntax

`tacacs-server host source-interface-ipv6 interface-id`

`no tacacs-server host source-interface-ipv6`

Parameters

- `interface-id`—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 TACACS+ server.

Example

The following example configures the VLAN 10 as the source interface.

```
ZEQU0xxxxDL (config)# tacacs-server host source-interface-ipv6 vlan 10
```

47.4 tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon, use the `tacacs-server key` Global Configuration mode command. To disable the key, use the `no` form of this command.

Syntax

`tacacs-server key key-string`

`no tacacs-server key`

Parameters

- `key-string`—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Length: 0–128 characters)
- `encrypted-key-string`—Same as `key-string`, but the key is in encrypted format.

Default Configuration

The default key is an empty string.

Command Mode

Global Configuration mode

Example

The following example sets Enterprise as the authentication key for all TACACS+ servers.

```
ZEQU0xxxxDL (config)# tacacs-server key enterprise
```

47.5 tacacs-server timeout

To set the interval during which the device waits for a TACACS+ server to reply, use the `tacacs-server timeout` Global Configuration mode command. To restore the default configuration, use the `no` form of this command.

Syntax

`tacacs-server timeout timeout`

`no tacacs-server timeout`

Parameters

- `timeout`—Specifies the timeout value in seconds. (Range: 1-30).

Default Configuration

The default timeout value is 5 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout value to 30 for all TACACS+ servers.

```
ZEQU0xxxxDL(config)# tacacs-server timeout 30
```

47.6 show tacacs

To display configuration and statistical information for a TACACS+ server, use the show tacacs Privileged EXEC mode command.

Syntax

show tacacs [ip-address]

Parameters

- ip-address—Specifies the TACACS+ server name, IPv4 or IPv6 address.

Default Configuration

If ip-address is not specified, information for all TACACS+ servers is displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays configuration and statistical information for all TACACS+ servers

```
ZEQU0xxxxDL# show tacacs
```

Device Configuration

```
-----  
  
      IP address      Status  Port  Single      TimeOut  Priority  
                        Connection  
-----  
172. 16. 1. 1      Connected  49    No          Global    1
```

Global values

```
-----  
  
TimeOut : 5  
Source IPv4 interface : vlan120  
Source IPv6 interface :vlan10
```

47.7 show tacacs key

To display the configured key of the TACACS+ server, use the show tacacs key Privileged EXEC mode command.

Syntax

show tacacs key [ip-address]

Parameters

- ip-address—Specifies the TACACS+ server name or IP address.

Default Configuration

If ip-address is not specified, information for all TACACS+ servers is displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays configuration and statistical information for all TACACS+ servers

ZEQU0xxxxDL# **show tacacs key**

Device Configuration

IP address	key

172. 16. 1. 1	Sharon123
172. 16. 1. 2	Bruce123
Global key	

Alice456	

48 Telnet, Secure Shell (SSH) and Secure Login(Slogin) Commands

48.1 ip telnet server

Use the ip telnet server Global Configuration mode command to enable the device as a Telnet server that accepts connection requests from remote Telnet clients. Remote Telnet clients can configure the device through the Telnet connections.

Use the no form of this command to disable the Telnet server functionality on the device.

To Login Privileged EXEC mode, use enable password command or set Privileged LEVEL to 15 by username command.

Syntax

ip telnet server

no ip telnet server

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The device can be enabled to accept connection requests from both remote SSH and Telnet clients. It is recommended that the remote client connects to the device using SSH (as opposed to Telnet), since SSH is a secure protocol and Telnet is not. To enable the device to be an SSH server, use the ip ssh server command.

Example

The following example enables the device to be configured from a Telnet server.

```
ZEQU0xxxxDL (config) # ip telnet server
```

48.2 ip ssh server

The ip ssh server Global Configuration mode command enables the device to be an SSH server and so to accept connection requests from remote SSH clients. Remote SSH clients can manage the device through the SSH connection.

Use the no form of this command to disable the SSH server functionality from the device.

To Login Privileged EXEC mode, use enable password command or set Privileged LEVEL to 15 by username command.

Syntax

ip ssh server

no ip ssh server

Default Configuration

The SSH server functionality is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The device, as an SSH server, generates the encryption keys automatically.

To generate new SSH server keys, use the crypto key generate dsa and crypto key generate rsa commands.

Example

The following example enables configuring the device to be an SSH server.

```
ZEQU0xxxxDL (config)# ip ssh server
```

48.3 ip ssh port

The `ip ssh port` Global Configuration mode command specifies the TCP port used by the SSH server. Use the `no` form of this command to restore the default configuration.

Syntax

`ip ssh port port-number`

`no ip ssh port`

Parameters

- `port-number`—Specifies the TCP port number to be used by the SSH server. (Range: 1–65535).

Default Configuration

The default TCP port number is 22.

Command Mode

Global Configuration mode

Example

The following example specifies that TCP port number 8080 is used by the SSH server.

```
ZEQU0xxxxDL (config)# ip ssh port 8080
```

48.4 ip ssh password-auth

Use the `ip ssh password-auth` Global Configuration mode command to enable password authentication of incoming SSH sessions.

Use the `no` form of this command to disable this function.

Syntax

`ip ssh password-auth`

`no ip ssh password-auth`

Default Configuration

Password authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables password key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

Example

The following example enables password authentication of the SSH client.

```
ZEQU0xxxxDL(config)# ip ssh password-auth
```

48.5 ip ssh pubkey-auth

Use the `ip ssh pubkey-auth` Global Configuration mode command to enable public key authentication of incoming SSH sessions.

Use the `no` form of this command to disable this function.

Syntax

```
ip ssh pubkey-auth [auto-login]
```

```
no ip ssh pubkey-auth
```

Parameters

- `auto-login`—Specifies that the device management AAA authentication (CLI login) is not needed. By default, the login is required after the SSH authentication.

Default Configuration

Public key authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables public key authentication by a local SSH server or remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device, except if the `auto-login` parameter was specified.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

If the `auto-login` keyword is specified for SSH authentication by public key management access is granted if SSH authentication succeeds and the name of SSH used is found in the local user database. The device management AAA authentication is transparent to the user. If the user name is not in the local user database, then the user receives a warning message, and the user will need to pass the device management AAA authentication independently of the SSH authentication.

if the auto-login keyword is not specified, management access is granted only if the user engages and passes both SSH authentication and device management AAA authentication independently. If no SSH authentication method is enabled management access is granted only if the user is AAA authenticated by the device management. No SSH authentication method means SSH is enabled and neither SSH authentication by public key nor password is enabled.

Example

The following example enables authentication of the SSH client.

```
ZEQU0xxxxDL (config) # ip ssh pubkey-auth
```

48.6 crypto key pubkey-chain ssh

The crypto key pubkey-chain ssh Global Configuration mode command enters the SSH Public Key-chain Configuration mode. This mode is used to manually specify device public keys, such as SSH client public keys.

Syntax

crypto key pubkey-chain ssh

Default Configuration

Keys do not exist.

Command Mode

Global Configuration mode

User Guidelines

Use this command when you want to manually specify SSH client's public keys.

Example

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain to the user 'bob'.

```
ZEQU0xxxxDL (config)# crypto key pubkey-chain ssh
ZEQU0xxxxDL (config-keychain)# user-key bob rsa
ZEQU0xxxxDL (config-keychain-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWI
Al4kpqIw9GBRonZQZxjHKcqKL6rMIQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJk67IOU/zfw0l1g
kTwmI75QR9gHujS6KwGN2QWXgh3ub8gdjTSq
muSn/Wd05iDX2lExQWu08licgIk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY

OZCkON/W9a/tnkm1shRE7Di71+w3fNiOA

6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdaTn/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

48.7 user-key

The user-key SSH Public Key-string Configuration mode command associates a username with a manually-configured SSH public key.

Use the no user-key command to remove an SSH user and the associated public key.

Syntax

```
user-key username {rsa | dsa}
```

```
no user-key username
```

Parameters

- username—Specifies the remote SSH client username. (Length: 1–48 characters)
- rsa—Specifies that the RSA key pair is manually configured.
- dsa—Specifies that the DSA key pair is manually configured.

Default Configuration

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

After entering this command, the existing key, if any, associated with the user will be deleted. You must follow this command with the key-string command to configure the key to the user.

Example

The following example enables manually configuring an SSH public key for SSH public key-chain bob.

```
ZEQU0xxxxDL (config)# crypto key pubkey-chain ssh  
ZEQU0xxxxDL (config-keychain)# user-key bob rsa  
ZEQU0xxxxDL (config-keychain-key)# key-string row AAAAB3NzaC1yc2EAAAADAQABAAQCVtnRwPWI
```

48.8 key-string

The key-string SSH Public Key-string Configuration mode command manually specifies an SSH public key.

Syntax

key-string [row key-string]

Parameters

- row—Specifies the SSH public key row by row. The maximum length of a row is 160 characters.
- key-string—Specifies the key in UU-encoded DER format. UU-encoded DER format is the same format as in the `authorized_keys` file used by OpenSSH.

Default Configuration

Keys do not exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Use the key-string SSH Public Key-string Configuration mode command without the row parameter to specify which SSH public key is to be interactively configured next. Enter a row with no characters to complete the command.

Use the key-string row SSH Public Key-string Configuration mode command to specify the SSH public key, row by row. Each row must begin with a key-string row command.

The UU-encoded DER format is the same format as in the `authorized_keys` file used by OpenSSH.

Example

The following example enters public key strings for SSH public key client ‘bob’.

```
ZEQU0xxxxDL(config)# crypto key pubkey-chain ssh
ZEQU0xxxxDL(config-keychain)# user-key bob rsa
ZEQU0xxxxDL(config-keychain-key)# key-string
```

AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMIQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJk67IOU/zfw0lIg
kTwmI75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08IicgIk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY

OZCkON/W9a/tnkm1shRE7Di71+w3fNiOA

6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdaTn/4oJfce166DqVX1gWmN
zNR4DYDvSzg0IDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

ZEQU0xxxxDL (config) # **crypto key pubkey-chain ssh**

ZEQU0xxxxDL (config-keychain) # **user-key bob rsa**

ZEQU0xxxxDL (config-keychain-key) # **key-string row AAAAB3Nza**

ZEQU0xxxxDL (config-keychain-key) # **key-string row C1yc2**

48.9 show ip ssh

The show ip ssh Privileged EXEC mode command displays the SSH server configuration.

Syntax

show ip ssh

Command Mode

Privileged EXEC mode

Example

The following example displays the SSH server configuration.

```
ZEQU05410DL#show ip ssh
```

```
SSH Server disabled. Port: 22
```

```
RSA key was generated.
```

```
DSA(DSS) key was generated.
```

```
SSH Public Key Authentication is disabled.
```

```
SSH Password Authentication is disabled.
```

```
Active incoming sessions:
```

IP address	SSH username	Version	Cipher	Auth Code
172.16.0.1	John Brown	1.5	3DES	HMAC-SHA1
172.20.0.2	Bob Smith	1.5	3DES	Password

The following table describes the significant fields shown in the display.

Field	Description
IP Address	The client address
SSH Username	The user name
Version	The SSH version number
Cipher	The encryption type (3DES, Blowfish, RC4)
Auth Code	The authentication Code (HMAC-MD5, HMAC-SHA1) or Password

48.10 show crypto key pubkey-chain ssh

The show crypto key pubkey-chain ssh Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

```
show crypto key pubkey-chain ssh [username username] [fingerprint  
{bubble-babble | hex}]
```

Parameters

- username username—Specifies the remote SSH client username. (Length: 1–48 characters)
- fingerprint {bubble-babble | hex}—Specifies the fingerprint display format. The possible values are:
 - bubble-babble—Specifies that the fingerprint is displayed in Bubble Babble format.
 - hex—Specifies that the fingerprint is displayed in hexadecimal format.

Default Configuration

The default fingerprint format is hexadecimal.

Command Mode

Privileged EXEC mode

Example

The following examples display SSH public keys stored on the device.

```
ZEQU0xxxxDL# show crypto key pubkey-chain ssh
```

Username	Fingerprint
-----	-----
bob	9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
john	98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8

```
ZEQU0xxxxDL# show crypto key pubkey-chain ssh username bob
```

Username	Fingerprint
-----	-----
bob	9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86

49 User Interface Commands

49.1 banner exec

To specify and enable a message to be displayed after a successful logon, use the banner exec Global Configuration mode command. This banner is applied automatically on all the user interfaces: console, Telnet and SSH. To delete the existing EXEC banner, use the no form of this command.

Syntax

banner exec d message-text d

no banner exec

Parameters

- d—Delimiting character of user's choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
- message-text—The message must start in a new line. You can enter multi-line messages. You can include tokens in the form of \$(token) in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 1000 characters (after every 510 characters, press <Enter> to continue).

Default Configuration

Disabled (no EXEC banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of \$(token) in the message text to customize the banner. The tokens are described in the table below:

Token	Information Displayed in the Banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.
\$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.
\$(location)	Displays the system location string.
\$(mac-address s)	Displays the base MAC address of the device.

Use the no banner exec Line Configuration command to disable the Exec banner on a particular line or lines.

Example

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the \$(token) syntax is replaced by the corresponding configuration variable.

```
ZEQU0xxxxDL (config)# banner exec %
```

Enter TEXT message. End with the character '% '.

```
$(bold)Session activated.$(bold) Enter commands at the prompt.
```

%

When a user logs on to the system, the following output is displayed: Session activated.
Enter commands at the prompt.

49.2 banner login

To specify a message to be displayed before the username and password login prompts, use the banner login command in Global Configuration mode. This banner is applied automatically on all the user interfaces: Console, Telnet and SSH. To delete the existing login banner, use the no form of this command

Syntax

banner login d message-text d

no banner login

Parameters

- d—Delimiting character of user's choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
- message-text—Message text. The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of \$(token) in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 1000 characters (after every 510 characters, you must press <Enter> to continue).

Default Configuration

Disabled (no Login banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of \$(token) in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.
\$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.

Token	Information displayed in the banner
\$(location)	Displays the system location string.
\$(mac-address)	Displays the base MAC address of the device.

Use the no banner login Line Configuration command to disable the Login banner on a particular line or lines.

Example

The following example sets a Login banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the \$(token) syntax is replaced by the corresponding configuration variable.

```
ZEQU0xxxxDL (config)# banner login %
```

```
Enter TEXT message. End with the character '%'. You have
entered $(hostname).$(domain)
%
```

```
When the login banner is executed, the user will see the following banner: You have entered
host123.ourdomain.com
```

49.3 configure

To enter the Global Configuration mode, use the configure Privileged EXEC mode command.

Syntax

configure [terminal]

Parameters

terminal—(Optional) Enter the Global Configuration mode with or without the keyword terminal.

Command Mode

Privileged EXEC mode

Example

The following example enters Global Configuration mode.

```
ZEQU0xxxxDL# configure
ZEQU0xxxxDL (conf ig)#
```

49.4 disable

To leave the Privileged EXEC mode and return to the User EXEC mode, use the disable Privileged EXEC mode command.

Syntax

disable [privilege-level]

Parameters

privilege-level—(Optional) Reduces the privilege level to the specified privileged level. If privilege level is left blank, the level is reduce to the minimal privilege level.

Default Configuration

The default privilege level is 15.

Command Mode

Privileged EXEC mode

Example

The following example returns the user to user level 1.

```
ZEQU0xxxxDL# disable 1
```

```
ZEQU0xxxxDL#
```

49.5 do

To execute an EXEC-level command from Global Configuration mode or any configuration submode, use the do command.

Syntax

do command

Parameters

command—Specifies the EXEC-level command to execute.

Command Mode

All configuration modes

Example

The following example executes the show vlan Privileged EXEC mode command from Global Configuration mode.

Example

ZEQU0xxxxDL# do show vlan

Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN

Vlan	Name	Tagged Ports	UnTagged Ports	Created by
1	Default		gi1/0/1	D
10	Marketing	gi1/0/2	gi1/0/2	S
91	11	gi1/0/2-4	gi1/0/2	SGR
92	11	gi1/0/3-4		G
93	11	gi1/0/3-4		GR

49.6 enable

To enter the Privileged EXEC mode, use the enable User EXEC mode command.

Syntax

enable [privilege-level]

Parameters

privilege-level—(Optional) Specifies the privilege level at which to enter the system.(Range: 1,7,15)

Default Configuration

The default privilege level is 15.

Command Mode

User EXEC mode

Example

The following example enters privilege level 15.

```
ZEQU0xxxxDL# enable
enter password:*****
ZEQU0xxxxDL# Accepted
```

49.7 end

To end the current configuration session and return to the Privileged EXEC mode, use the end command.

Syntax

end

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Example

The following example ends the Global Configuration mode session and returns to the Privileged EXEC mode.

```
ZEQU0xxxxDL (config)# end  
ZEQU0xxxxDL#
```

49.8 exit (Configuration)

To exit any mode and bring the user to the next higher mode in the CLI mode hierarchy, use the exit command.

Syntax

exit

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Examples

The following examples change the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
ZEQU0xxxxDL(config-if)# exit  
ZEQU0xxxxDL(config)# exit
```

49.9 exit (EXEC)

To close an active terminal session by logging off the device, use the exit User EXEC mode command.

Syntax

exit

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

Example

The following example closes an active terminal session.

```
ZEQU0xxxxDL# exit
```

49.10 **help**

To display a brief description of the Help system, use the help command.

Syntax

help

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Example

The following example describes the Help system.

ZEQU0xxxxDL# **help**

Help may be requested at any point in a command by entering a question mark

'?'. If nothing matches the currently entered incomplete command, the help list is empty. This indicates that there is no command matching the input as it currently appears. If the request is within a command, press the Backspace key and erase the entered characters to a point where the request results in a match.

Help is provided when:

1. There is a valid command and a help request is made for entering a parameter or argument (e. g. 'show ?'). All possible parameters or arguments for the entered command are then displayed.
 2. An abbreviated argument is entered and a help request is made for arguments matching the input (e. g. 'show pr?').
-

49.11 history

To enable saving commands that have been entered, use the history Line Configuration Mode command. To disable the command, use the no form of this command.

Syntax

history

no history

Parameters

This command has no arguments or keywords

Default Configuration

Enabled.

Command Mode

Line Configuration Mode

User Guidelines

This command enables saving user-entered commands for a specified line. You can return to previous lines by using the up or down arrows.

It is effective from the next time that the user logs in via console/telnet/ssh. The following are related commands:

- Use the terminal history size User EXEC mode command to enable or disable this command for the current terminal session.
- Use the history size Line Configuration Mode command to set the size of the command history buffer.

Example

The following example enables the command for Telnet.

```
ZEQU0xxxxDL (config)# line telnet
ZEQU0xxxxDL (config-line)# history
```

49.12 history size

To change the maximum number of user commands that are saved in the history buffer for a particular line, use the history size Line Configuration Mode command.

To reset the command history buffer size to the default value, use the no form of this command.

Syntax

history size number-of-commands

no history size

Parameters

number-of-commands—Specifies the number of commands the system records in its history buffer.

Default Configuration

The default command history buffer size is 10 commands.

Command Mode

Line Configuration Mode

User Guidelines

This command configures the command history buffer size for a particular line. It is effective from the next time that the user logs in via console/telnet/ssh.

Use the terminal history size User EXEC mode command to configure the command history buffer size for the current terminal session.

The allocated command history buffer is per terminal user, and is taken from a shared buffer. If there is not enough space available in the shared buffer, the command history buffer size cannot be increased above the default size.

Example

The following example changes the command history buffer size to 100 entries for Telnet.

```
ZEQU0xxxxDL (config)# line telnet
ZEQU0xxxxDL (config-line)# history size 100
```

49.13 **logout**

To Logout, use the logout User EXEC mode command.

Syntax

login

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

Example

The following example is to logou console.

ZEQU0xxxxDL# **logout**

ZEQU0xxxxDL
Command Line Interface

Product Number: PNxxxxxx
Firmware Version: 1.0.0.00
MAC Address: 00:50:40:xx:xx:xx
Serial Number: 79P12345678

UserName:

49.14 terminal datadump

To enable dumping all the output of a show command without prompting, use the terminal datadump User EXEC mode command. To disable dumping, use the no form of this command.

Syntax

terminal datadump

terminal no datadump

Parameters

This command has no arguments or keywords

Default Configuration

When printing, dumping is disabled and printing is paused every 24 lines.

Command Mode

User EXEC mode

User Guidelines

By default, a More prompt is displayed when the output contains more than 24 lines. Pressing the Enter key displays the next line; pressing the Spacebar displays the next screen of output.

The terminal datadump command enables dumping all output immediately after entering the show command by removing the pause.

The width is not limited, and the width of the line being printed on the terminal is based on the terminal itself.

This command is relevant only for the current session.

Example

The following example dumps all output immediately after entering a show command.

```
ZEQU0xxxxDL# terminal datadump
```

49.15 terminal history

To enable the command history function for the current terminal session, meaning that it will not be stored in the Running Configuration file, use the terminal history User EXEC mode command. To disable the command, use the no form of this command.

Syntax

terminal history

terminal no history

Parameters

This command has no arguments or keywords

Default Configuration

The default configuration for all terminal sessions is defined by the history Line Configuration Mode command.

Command Mode

User EXEC mode

User Guidelines

The command enables the command history for the current session. The default is determined by the history Line Configuration Mode command.

This command is effective immediately.

Example

The following example disables the command history function for the current terminal session.

```
ZEQU0xxxxDL# terminal no history
```

49.16 terminal history size

To change the command history buffer size for the current terminal session, meaning it will not be stored in the Running Configuration file, use the terminal history size User EXEC mode command. , use the no form of this command to reset the command history buffer size to the default value.

Syntax

terminal history size number-of-commands

terminal no history size

Parameters

number-of-commands—Specifies the number of commands the system maintains in its history buffer. (Range: 10–206)

Default Configuration

The default configuration for all terminal sessions is defined by the history size Line Configuration Mode command.

Command Mode

User EXEC mode

User Guidelines

The terminal history size EXEC command changes the command history buffer size for the current terminal session. Use the history Line Configuration Mode command to change the default history buffer size.

The maximum number of commands in all buffers is 207.

Example

The following example sets the command history buffer size to 20 commands for the current terminal session.

```
ZEQU0xxxxDL# terminal history size 20
```

49.17 terminal prompt

To enable the terminal prompts, use the terminal prompt User EXEC mode command. To disable the terminal prompts, use terminal no prompt command.

The command is per session and will not be saved in the configuration database.

Syntax

terminal prompt

terminal no prompt

Parameters

This command has no arguments or keywords

Default Configuration

The default configuration is prompts enabled.

Command Mode

Privileged EXEC mode

Example

The following example disables the terminal prompts

```
ZEQU0xxxxDL# terminal no prompt
```

49.18 terminal width

To determine the width of the display for the echo input to CLI sessions, use the terminal width User EXEC mode command. To return to the default, use terminal no width.

The command is per session and will not be saved in the configuration database.

Syntax

terminal width number-of-characters

terminal no width

Parameters

number-of-characters - Specifies the number of characters to be displayed for the echo output of the CLI commands and the configuration file,'0' means endless number of characters on a screen line. (Range: 0, 70-512)

Default Configuration

The default number of characters is 77.

Command Mode

Privileged EXEC mode

Example

The following example sets the terminal width to 100 characters

```
ZEQU0xxxxDL# terminal width 100
```

49.19 **show banner**

To display the banners that have been defined, use the show banner commands in User EXEC mode.

Syntax

show banner login

show banner exec

Parameters

This command has no arguments or keywords

Command Mode

User EXEC mode

Examples

```
ZEQU0xxxxDL# show banner login  
Banner: Login  
Line SSH: Enabled  
Line Telnet: Enabled  
Line Console: Enabled
```

```
ZEQU0xxxxDL# show banner exec  
Banner: EXEC  
Line SSH: Enabled  
Line Telnet: Enabled  
Line Console: Enabled
```

49.20 **show history**

To list the commands entered in the current session, use the show history User EXEC mode command.

Syntax

show history

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

User Guidelines

The buffer includes executed and unexecuted commands. Commands are

listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

Example

The following example displays all the commands entered while in the current Privileged EXEC mode.

```
ZEQU0xxxxDL# show clock
```

```
*18:58:05 UTC Jan 2 2019  
Time source is sntp  
Time from Browser is disabled
```

```
ZEQU0xxxxDL# show history
```

```
show clock  
show history  
2 commands were logged (buffer size is 10)
```

49.21 **show privilege**

To display the current privilege level, use the show privilege User EXEC mode command.

Syntax

show privilege

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

User EXEC mode

Example

The following example displays the privilege level for the user logged on.

```
ZEQU0xxxxDL# show privilege  
Current privilege level is 15
```

50 Virtual Local Area Network (VLAN) Commands

50.1 vlan database

Use the vlan database Global Configuration mode command to enter the VLAN Configuration mode. This mode is used to create VLAN(s) and define the default VLAN.

Use the exit command to return to Global Configuration mode.

Syntax

vlan database

Parameters

N/A

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

Example

The following example enters the VLAN Configuration mode, creates VLAN 1972 and exits VLAN Configuration mode.

```
ZEQU0xxxxDL (config) # vlan database
ZEQU0xxxxDL (config-vlan) # vlan 1972
ZEQU0xxxxDL (config-vlan) # exit
```

50.2 vlan

Use the `vlan` VLAN Configuration mode or Global Configuration mode command to create a VLAN and assign it a name (if only a single VLAN is being created). Use the `no` form of this command to delete the VLAN(s).

Syntax

`vlan vlan-range | {vlan-id [name vlan-name]} [media ethernet] [state active]`

`no vlan vlan-range`

Parameters

- `vlan-range`—Specifies a list of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs (range: 2-4094).
- `vlan-id`—Specifies a VLAN ID. (range: 2-4094).
- `vlan-name`—Specifies the VLAN name. (range: 1–32 characters).
- `media`—Specifies the media type of the VLAN. Valid values are `ethernet`.
- `state`—Specifies whether the state of the VLAN. Valid values are `active`.

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

VLAN Database Configuration mode

User Guidelines

If the VLAN does not exist, it is created. If the VLAN cannot be created then the command is finished with error and the current context is not changed.

Example

The following example creates a few VLANs. VLAN 1972 is assigned the name Marketing.

```
ZEQU0xxxxDL(config)# vlan database
ZEQU0xxxxDL(config-vlan)# vlan 19-23
ZEQU0xxxxDL(config-vlan)# vlan 100
ZEQU0xxxxDL(config-vlan)# vlan 1972 name Marketing
ZEQU0xxxxDL(config-vlan)# exit
```

50.3 show vlan

Use the show vlan Privileged EXEC mode command to display the following VLAN information.

Syntax

show vlan [tag vlan-id | name vlan-name]

Parameters

- tag vlan-id—Specifies a VLAN ID.
- name vlan-name—Specifies a VLAN name string (length: 1–32 characters)

Default Configuration

All VLANs are displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example displays information for all VLANs:

ZEQU0xxxxDL# show vlan

Created by: S-Static, G-GVRP

VLAN	Name	Tagged Ports	UnTagged Ports	Created by
1	Default		gi1/0/1	D
10	Marketing	gi1/0/2	gi1/0/2	S
91	11	gi1/0/3-4	gi1/0/2	SGR
92	11	gi1/0/3-4		G
93	11	gi1/0/3-4		GR

50.4 interface vlan

Use the interface vlan Global Configuration mode command to enter the Interface Configuration (VLAN) mode for a specific VLAN. After this command is entered, all commands configure this VLAN.

Syntax

interface vlan vlan-id

Parameters

- vlan-id—Specifies the VLAN to be configured.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

If the VLAN does not exist, the VLAN is created. If the VLAN cannot be created, this command is finished with an error and the current context is not changed.

Example

The following example configures VLAN 1 with IP address 192.168.0.1 and subnet mask 255.255.255.0.

```
ZEQU0xxxxDL(config)# interface vlan 1
ZEQU0xxxxDL(config-if)# ip address 192. 168. 0. 1 255. 255. 255. 0
```

50.5 interface range vlan

Use the interface range vlan Global Configuration mode command to configure multiple VLANs simultaneously.

Syntax

interface range vlan vlan-range

Parameters

- **vlan-range**—Specifies a list of VLANs. Separate nonconsecutive VLANs with a comma and no spaces. Use a hyphen to designate a range of VLANs.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface VLAN range context are executed independently on each VLAN in the range. If the command returns an error on one of the VLANs, an error message is displayed, and the system attempts to configure the remaining VLANs.

Example

The following example groups VLANs 221 through 228 and 889 to receive the same command(s).

```
ZEQU0xxxxDL (config) # interface range vlan 221-228, vlan 889
```

50.6 name

Use the name Interface Configuration (VLAN) mode command to name a VLAN. Use the no form of this command to remove the VLAN name.

Syntax name

string no

name

Parameters

- string—Specifies a unique name associated with this VLAN. (Length: 1–32 characters).

Default Configuration

No name is defined.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

The VLAN name must be unique.

Example

The following example assigns VLAN 19 the name Marketing.

```
ZEQU0xxxxDL (config) # interface vlan 19  
ZEQU0xxxxDL (config-if) # name Marketing
```

50.7 switchport protected-port

Use the switchport protected-port Interface Configuration mode command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports on the same switch. Use the no form of this command to disable protection on the port.

Syntax

switchport protected-port

no switchport protected-port

Parameters

N/A

Default Configuration

Unprotected

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Note that packets are subject to all filtering rules and Filtering Database (FDB) decisions.

Use this command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports (that are not associated with the same community as the ingress interface) on the same switch. Please note that the packet is still subject to FDB decision and to all filtering rules.

Example

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# switchport protected-port
```

50.8 show interfaces protected-ports

Use the show interfaces protected-ports EXEC mode command to display protected ports configuration.

Syntax

show interfaces protected-ports [interface-id | detailed]

Parameters

- interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- detailed—Displays information for non-present ports in addition to present ports.

Default Configuration

Show all protected interfaces. If detailed is not used, only present ports are displayed.

Command Mode

User EXEC mode

Example

ZEQU0xxxxDL# show interfaces protected-ports		
Interface	State	Community
-----	-----	-----
gi1/0/1	Protected	1
gi1/0/2	Protected	Isolated
	.	
	.	
te1/0/27	Unprotected	20
te1/0/28	Unprotected	Isolated
Po1	Unprotected	Isolated
Po2	Unprotected	Isolated
	.	
	.	
Po31	Unprotected	Isolated
Po32	Unprotected	Isolated

50.9 switchport

Use the switchport Interface Configuration mode command to put an interface that is in Layer 3 mode into Layer 2 mode. Use the no form of this command to put an interface in Layer 3 mode.

Syntax

switchport

no switchport

Parameters

N/A

Default Configuration

Layer 2 mode

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the no switchport command to set the interface as a Layer 3 interface.

Examples

Example 1 - The following example puts the port gi1/0/1 into Layer 2 mode.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# switchport
```

Example 2 - The following example puts the port gi1/0/1 into Layer 3 mode.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# no switchport
```

50.10 **switchport mode**

Use the switchport mode Interface Configuration mode command to configure the VLAN membership mode. Use the no form of this command to restore the default configuration.

Syntax

```
switchport mode access | trunk | hybrid | private-vlan {promiscuous | host}  
vlan-mapping {tunnel | one-to-one }
```

```
no switchport mode
```

Parameters

- access—Specifies an untagged layer 2 VLAN port.
- trunk—Specifies a trunking layer 2 VLAN port.
- hybrid—Specifies a full 802-1q-supported VLAN port.
- private-vlan promiscuous—Private-VLAN promiscuous port.
- private-vlan host—Private-VLAN host port.
- vlan-mapping tunnel—VLAN Mapping tunnel edge port.
- vlan-mapping one-to-one—VLAN Mapping one-to-one edge port.

Default Configuration

Access mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When the port's mode is changed, it receives the configuration corresponding to the mode.

If the port mode is changed to access and the access VLAN does not exist, then the port does not belong to any VLAN.

Examples

Example 1 - The following example configures gi1/0/1 as an access port (untagged layer 2) VLAN port.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# switchport mode access
ZEQU0xxxxDL(config-if)# switchport access vlan 2
```

Example 2 - The following example puts the port gi1/0/2 into private-vlan mode.

```
ZEQU0xxxxDL(config)# interface gi1/0/2
ZEQU0xxxxDL(config-if)# switchport mode private-vlan
```

50.11 switchport access vlan

A port in access mode can be an untagged member of at most a single VLAN. The switchport access vlan Interface Configuration command reassigns an interface

to a different VLAN than it currently belongs or assigns it to none, in which case it is not a member of any VLAN.

The no form of this command to restore the default configuration.

Syntax

```
switchport access vlan {vlan-id | none}
```

```
no switchport access vlan
```

Parameters

- **vlan-id**—Specifies the VLAN to which the port is configured.
- **none**—Specifies that the access port cannot belong to any VLAN.

Default Configuration

The interface belongs to the Default VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When the port is assigned to a different VLAN, it is automatically removed from its previous VLAN and added it to the new VLAN. If the port is assigned to none, it is removed from the previous VLAN and not assigned to any other VLAN.

A non-existent VLAN can be assigned as an Access VLAN. If the Access VLAN does not exist the show interfaces switchport command adds text "(Inactive)" after VLAN ID.

Example

The following example assigns access port gi1/0/1 to VLAN2 (and removes it from its previous VLAN).

```
ZEQU0xxxxDL(config)# interface gi1/0/2  
ZEQU0xxxxDL(config-if)# switchport mode access  
ZEQU0xxxxDL(config-if)# switchport access vlan 2
```

50.12 **switchport trunk allowed vlan**

A trunk interface is an untagged member of a single VLAN, and, in addition, it may be an tagged member of one or more VLANs. Use the `switchport trunk allowed vlan` Interface Configuration mode command to add/remove VLAN(s) to/from a trunk port. Use the `no` form of the command to return to the default.

Syntax

`switchport trunk allowed vlan {all | none | add vlan-list | remove vlan-list | except vlan-list}`

`no switchport trunk allowed vlan`

Parameters

- `all`—Specifies all VLANs from 1 to 4094. At any time, the port belongs to all VLANs existing at the time. (range: 1–4094).
- `none`—Specifies an empty VLAN list The port does not belong to any VLAN.
- `add vlan-list`—List of VLAN IDs to add to the port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- `remove vlan-list`—List of VLAN IDs to remove from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- `except vlan-list`—List of VLAN IDs including all VLANs from range 1-4094 except VLANs belonging to `vlan-list`.

Default Configuration

By default, trunk ports belongs to all created VLANs.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the `switchport trunk allowed vlan` command to specify which VLANs the port belongs to when its mode is configured as trunk.

Non-existent VLANs can be configured. When a non-existent VLAN is created the port will add to it automatically.

Forbidden VLANs can be configured.

Example

To add VLANs 2,3 and 100 to trunk ports 1 to 13

```
ZEQU0xxxxDL(config)# interface range gi1/0/1-3
ZEQU0xxxxDL(config-if)# switchport mode trunk
ZEQU0xxxxDL(config-if)# switchport trunk allowed vlan add 2-3,100
ZEQU0xxxxDL(config-if)# exit
```

50.13 switchport trunk native vlan

If an untagged packet arrives on a trunk port, it is directed to the port's native VLAN. Use the `switchport trunk native vlan` Interface Configuration mode command to define the native VLAN for a trunk interface. Use the `no` form of this command to restore the default native VLAN.

Syntax

```
switchport trunk native vlan {vlan-id | none}
```

```
no switchport trunk native vlan
```

Parameters

- `vlan-id`—Specifies the native VLAN ID.
- `none`—Specifies the access port cannot belong to any VLAN.

Default Configuration

The default native VLAN is the Default VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

A value of the interface PVID is set to this VLAN ID. When the interface belongs to the Native VLAN it is set as VLAN untagged egress interface.

The configuration is applied only when the port mode is trunk.

Examples

The following example defines VLAN 2 as native VLAN for port `gi1/0/1`:

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# switchport trunk native vlan 2
ZEQU0xxxxDL(config-if)# exit
```

50.14 switchport hybrid allowed vlan

General ports can receive tagged or untagged packets. Use the switchport hybrid allowed vlan Interface Configuration mode command to add/remove VLANs to/from a hybrid port and configure whether packets on the egress are tagged or untagged. Use the no form of this command to reset to the default.

Syntax

```
switchport hybrid allowed vlan add vlan-list [tagged | untagged]
```

```
switchport hybrid allowed vlan remove vlan-list
```

```
no switchport hybrid allowed vlan
```

Parameters

- add vlan-list—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. (range: 1–4094)
- remove vlan-list—List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- tagged—Specify that packets are transmitted tagged for the configured VLANs
- untagged—Specify that packets are transmitted untagged for the configured VLANs (this is the default)

Default Configuration

The port is not a member of any VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. There will be an error message in this case ("An interface cannot become a member of a forbidden VLAN. This message will only be displayed once.") and the command continues to execute in case if there are more VLANs in the vlan-list.

A non-existed VLAN cannot be configured. When a VLAN is removed it is deleted from the vlan-list.

The configuration is applied only when the port mode is general.

Example

The example adds gi1/0/1 and to VLAN 2 and 3. Packets are tagged on the egress:

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# switchport hybrid allowed vlan add 2-3 tagged
```

50.15 switchport hybrid native vlan

Use the switchport hybrid native vlan Interface Configuration mode command to define the native VLAN for a hybrid interface. Use the no form of this command to restore the default native VLAN.

Syntax

switchport hybrid native vlan vlan-id

no switchport hybrid native vlan vlan-id

Parameters

- vlan-id—Specifies the Port VLAN ID (PVID).

Default Configuration

The default native VLAN is the Default VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Examples

Example 1 - The following example sets the gi1/0/2 PVID to 234.

```
ZEQU0xxxxDL(config)# interface gi1/0/2
ZEQU0xxxxDL(config-if)# switchport hybrid native vlan 234
```

Example 2 - The following example performs the following:

- Adds VLANs 2&3 as tagged, and VLAN 100 as untagged to gi1/0/4
- Defines VID 100 as the PVID

```
ZEQU0xxxxDL(config)# interface gi1/0/4
ZEQU0xxxxDL(config-if)# switchport mode hybrid
ZEQU0xxxxDL(config-if)# switchport hybrid allowed vlan add 2-3 tagged
ZEQU0xxxxDL(config-if)# switchport hybrid allowed vlan add 100 untagged
ZEQU0xxxxDL(config-if)# switchport hybrid native vlan 100
ZEQU0xxxxDL(config-if)# exit
```

50.16 **no ingress-checking**

Use the no ingress-check Interface Configuration mode command to disable port ingress filtering (no packets are discarded at the ingress) on a general port. Use the no form of this command to restore the default configuration.

Syntax

no ingress-checking

ingress-checking

Parameters

N/A

Default Configuration

Ingress filtering is enabled. (ingress-checking)

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables port ingress filtering on gi1/0/1.

```
ZEQU0xxxxDL(config)# interface gi1/0/1
ZEQU0xxxxDL(config-if)# switchport mode hybrid
ZEQU0xxxxDL(config-if)# no ingress-checking
```

50.17 acceptable-frame-type

The acceptable-frame-type Interface Configuration mode command configures the types of packets (tagged/untagged) that are filtered (discarded) on the interface. Use the no form of this command to return ingress filtering to the default.

Syntax

acceptable-frame-type { tagged-only | untagged-only | all }

no acceptable-frame-type

Parameters

- tagged-only—Ignore (discard) untagged packets and priority-tagged packets.
- untagged-only—Ignore (discard) VLAN-tagged packets (not including priority-tagged packets)
 - all—Do not discard packets untagged or priority-tagged packets.

Default Configuration

All frame types are accepted at ingress (all).

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures port gi1/0/3 to be in general mode and to discard untagged frames at ingress.

```
ZEQU0xxxxDL(config)# interface gi1/0/3
ZEQU0xxxxDL(config-if)# switchport mode hybrid
ZEQU0xxxxDL(config-if)# acceptable-frame-type tagged-only
```

50.18 switchport hybrid forbidden vlan

Use the switchport hybrid forbidden vlan Interface Configuration mode command to forbid adding/removing specific VLANs to/from a port.

Syntax

switchport hybrid forbidden vlan {add vlan-list | remove vlan-list}

no switchport hybrid forbidden vlan

Parameters

- add vlan-list—Specifies a list of VLAN IDs to add to interface. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- remove vlan-list—Specifies a list of VLAN IDs to remove from interface. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The forbidden VLAN cannot be one that does not exist on the system, or one that is already defined on the port.

Example

The following example defines gi1/0/4 as a forbidden membership in VLANs 5-7:

```
ZEQU0xxxxDL(config)# interface gi1/0/28
ZEQU0xxxxDL(config-if)# switchport hybrid forbidden vlan add 5-7
ZEQU0xxxxDL(config-if)# exit
```

50.19 map protocol protocols-group

Use the map protocol protocols-group VLAN Configuration mode command to map a protocol to a group of protocols. This protocol group can then be used in switchport general map protocols-group vlan. Use the no form of this command to delete a protocol from a group.

Syntax

map protocol protocol [encapsulation-value] protocols-group group

no map protocol protocol [encapsulation]

Parameters

- protocol—Specifies a 16-bit protocol number or one of the reserved names listed in the User Guidelines. (range: 0x0600–0xFFFF)
- encapsulation-value—Specifies one of the following values: Ethernet, rfc1042, llcOther.
- protocols-group group—Specifies the group number of the group of protocols (range: 1–2147483647).

Default Configuration

The default encapsulation value is Ethernet.

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their protocol requires setting up groups of protocols and then mapping these groups to VLANs.

The value 0x8100 is not valid as the protocol number for Ethernet encapsulation.

The following protocol names are reserved for Ethernet Encapsulation:

- ip
- arp
- ipv6
- ipx

Example

The following example maps the IP protocol to protocol group number 213.

```
ZEQU0xxxxDL(config)# vlan database  
ZEQU0xxxxDL(config-vlan)# map protocol ip protocols-group 213
```

50.20 show vlan protocols-groups

Use the show vlan protocols-groups EXEC mode command to display the protocols that belong to the defined protocols-groups.

Syntax

show vlan protocols-groups

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays protocols-groups information.

ZEQU0xxxxDL# show vlan protocols-groups		
Encapsulation	Protocol	Group Id
-----	-----	-----
Ethernet	0x800 (IP)	1
Ethernet	0x806 (ARP)	1
Ethernet	0x86dd (IPv6)	2
Ethernet	0x8898	3

50.21 **map mac macs-group**

Use the `map mac macs-group` VLAN Configuration mode command to map a MAC address or range of MAC addresses to a group of MAC addresses. Use the `no` form of this command to delete the mapping.

Syntax

```
map mac mac-address {prefix-mask | host} macs-group group
```

```
no map mac mac-address {prefix-mask | host}
```

Parameters

- `mac-address`—Specifies the MAC address to be mapped to the group of MAC addresses.
- `prefix-mask`—Specifies the number of ones in the mask.
- `host`—Specifies that the mask is comprised of all 1s.
- `group`—Specifies the group number (range: 1–2147483647)

Default Configuration

N/A

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their MAC address requires setting up groups of MAC addresses and then mapping these groups to VLANs.

Up to 256 MAC addresses (host or range) can be mapped to one or many MAC-based VLAN groups.

Example

The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
ZEQU0xxxxDL(config)# vlan database
ZEQU0xxxxDL(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
ZEQU0xxxxDL(config-vlan)# map mac 0000.0000.2222 host macs-group 2
ZEQU0xxxxDL(config-vlan)# exit
ZEQU0xxxxDL(config)# interface gi1/0/4
ZEQU0xxxxDL(config-if)# switchport mode hybrid
ZEQU0xxxxDL(config-if)# switchport hybrid map macs-group 1 vlan 2
ZEQU0xxxxDL(config-if)# switchport hybrid map macs-group 2 vlan 3
```

50.22 switchport hybrid map macs-group vlan

Use the switchport hybrid map macs-group vlan Interface Configuration mode command to set a MAC-based classification rule. Use the no form of this command to delete a classification rule.

Syntax

```
switchport hybrid map macs-group group vlan vlan-id
```

```
no switchport hybrid map macs-group group
```

Parameters

- group—Specifies the group number (range: 1–2147483647)
- vlan-id—Defines the VLAN ID associated with the rule.

Default Configuration

N/A

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

MAC-based VLAN rules cannot contain overlapping ranges on the same interface. The VLAN classification rule priorities are:

- MAC-based VLAN (best match among the rules)
- Subnet-based VLAN (best match among the rules)
- Protocol-based VLAN
- PVID

User Guidelines

After groups of MAC addresses have been created (see the map mac macs-group command), they can be mapped to specific VLANs.

Each MAC address (host or range) in the MAC-based group assigned to an interface consumes a single TCAM entry.

Example

The following example creates two groups of MAC addresses, sets a port to hybrid mode and maps the groups of MAC addresses to specific VLANs.

```
ZEQU0xxxxDL(config)# vlan database
ZEQU0xxxxDL(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
ZEQU0xxxxDL(config-vlan)# map mac 0000.0000.2222 host macs-group 2
ZEQU0xxxxDL(config-vlan)# exit
ZEQU0xxxxDL(config)# interface gi1/0/4
ZEQU0xxxxDL(config-if)# switchport mode hybrid
ZEQU0xxxxDL(config-if)# switchport hybrid map macs-group 1 vlan 2
ZEQU0xxxxDL(config-if)# switchport hybrid map macs-group 2 vlan 3
```

50.23 show vlan macs-groups

Use the show vlan macs-groups EXEC mode command to display the MAC addresses that belong to the defined MAC-based classification rules.

Syntax

show vlan macs-groups

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays defined MAC-based classification rules.

ZEQU0xxxxDL# show vlan macs-groups

MAC Address	Mask	Group ID
00:12:34:56:78:90	20	22
00:50:40:4c:73:ff	40	1

50.24 map subnet subnets-group

Use the map subnet subnets-group VLAN Configuration mode command to map an IP subnet to a group of IP subnets. Use the no form of this command to delete the map.

Syntax

map subnet ip-address prefix-mask subnets-group group

no map subnet ip-address prefix-mask

Parameters

- ip-address—Specifies the IP address prefix of the subnet to be mapped to the group.
- prefix-mask—Specifies the number of 1s in the mask.
- group—Specifies the group number. (range: 1–2147483647)

Default Configuration

N/A

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their IP subnet requires setting up groups of IP subnets and then mapping these groups to VLANs.

Example

The following example maps an IP subnet to the group of IP subnets 4. It then maps this group of IP subnets to VLAN 8

```
ZEQU0xxxxDL(config)# vlan database
ZEQU0xxxxDL(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
ZEQU0xxxxDL(config-vlan)# switchport hybrid map subnets-group 4 vlan 8
```

50.25 switchport hybrid map subnets-group vlan

Use the switchport hybrid map subnets-group vlan Interface Configuration mode command to set a subnet-based classification rule. Use the no form of this command to delete a subnet-based classification rule.

Syntax

switchport hybrid map subnets-group group vlan vlan-id

no switchport hybrid map subnets-group group

Parameters

- group—Specifies the group number. (range: 1–2147483647)
- vlan-id—Defines the VLAN ID associated with the rule.

Default Configuration

N/A

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The VLAN classification rule priorities are:

- MAC-based VLAN (Best match among the rules)
- Subnet-based VLAN (Best match among the rules)
- Protocol-based VLAN
- PVID

Example

The following example maps an IP subnet to the group of IP subnets 4. It then maps this group of IP subnets to VLAN 8

```
ZEQU0xxxxDL(config)# vlan database
ZEQU0xxxxDL(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
ZEQU0xxxxDL(config-vlan)# switchport hybrid map subnets-group 4 vlan 8
```

50.26 show vlan subnets-groups

Use the show vlan subnets-groups EXEC mode command to display subnets-groups information.

Syntax

show vlan subnets-groups

Parameters

N/A

Default Configuration

N/A

Command Mode

User EXEC mode

Example

The following example displays subnets-groups information.

ZEQU0xxxxDL#

show vlan subnets-groups

IP Subnet Address	Mask	Group Id
-----	-----	-----
1. 1. 1. 1	32	1
172. 16. 2. 0	24	2

50.27 **show interfaces switchport**

Use the show interfaces switchport Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

Syntax

show interfaces switchport [interface-id]

Parameters

- Interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Default

Displays the status of all interfaces.

User Guidelines

Each port mode has its own private configuration. The show interfaces switchport command displays all these configurations, but only the port mode configuration that corresponds to the current port mode displayed in "Administrative Mode" is active.

Example

```
ZEQU0xxxxDL# show interfaces switchport gi1/0/1
```

Gathering information...

S-VLAN Ethernet Type: 0x8100 (802.1q)

Name: gi1/0/1

Switchport: enable

Administrative Mode: access

Operational Mode: down

Access Mode VLAN: 1

Trunking Native Mode VLAN: 1

Trunking VLANs: 1
2-4094 (Inactive)

Hybrid PVID: 1

Hybrid VLANs: none

Hybrid Egress Tagged VLANs: none

Hybrid Forbidden VLANs: none

Hybrid Ingress Filtering: enabled

Hybrid Acceptable Frame Type: all
 Hybrid GVRP status: Enabled
 Customer Mode VLAN: none
 Private-vlan promiscuous-association primary VLAN: none
 Private-vlan promiscuous-association Secondary VLANs: none
 Private-vlan host-association primary VLAN: none
 Private-vlan host-association Secondary VLAN: none

VLAN Mapping Tunnel:

C-VLANs	Outer S-VLANs
-----	-----

VLAN Mapping One-to-one:

C-VLANs	Translated S-VLANs
-----	-----

Classification rules:

Classification type	Group ID	VLAN ID
Protocol	1	19
Protocol	1	20
Protocol	2	72
Subnet	1	15
MAC	1	77

50.28 private-vlan

Use the private-vlan Interface VLAN Configuration mode command to configure a private VLAN. Use the no form of this command to return the VLAN to normal VLAN configuration.

Syntax

```
private-vlan {primary | community | isolated}
```

```
no private-vlan
```

Parameters

- **primary**—Designate the VLAN as a primary VLAN.
- **community**—Designate the VLAN as a community VLAN.
- **isolated**—Designate the VLAN as an isolated VLAN.

Default Configuration

No private VLANs are configured.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

- The VLAN type cannot be changed if there is a private VLAN port that is a member in the VLAN.
- The VLAN type cannot be changed if it is associated with other private VLANs.
- The VLAN type is not kept as a property of the VLAN when the VLAN is deleted.

Example

The following example set vlan 2 to be primary vlan:

```
ZEQU0xxxxDL(config)# interface vlan 2  
ZEQU0xxxxDL(config-if)# private-vlan primary
```

50.29 private-vlan association

Use the private-vlan association Interface VLAN Configuration mode command to configure the association between the primary VLAN and secondary VLANs. Use the no form of this command to remove the association.

Syntax

private-vlan association [add | remove] secondary-vlan-list

no private-vlan association

Parameters

- add secondary-vlan-list—List of VLAN IDs of type secondary to add to a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. This is the default action.
- remove secondary-vlan-list—List of VLAN IDs of type secondary to remove association from a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

No private VLANs are configured.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

- The command can only be executed in the context of the primary VLAN.
- A private VLAN cannot be removed or have its type changed, if it is associated with other private VLANs.
- A primary VLAN can be associated with only a single, isolated VLAN.
- A secondary VLAN can be associated with only one primary VLAN.
- The association of secondary VLANs with a primary VLAN cannot be removed if there are private VLAN ports that are members in the secondary VLAN.
- In MSTP mode, all the VLANs that are associated with a private VLAN must be mapped to the same instance.

Example

The following example associate secondary VLAN 20,21,22 and 24 to primary VLAN 2.

```
ZEQU0xxxxDL(config)# interface vlan 2  
ZEQU0xxxxDL(config-if)# private-vlan association add 20-22, 24
```

50.30 switchport private-vlan mapping

Use the switchport private-vlan mapping Interface Configuration mode command to configure the VLANs of the private VLAN promiscuous port. Use the no form of this command to reset to default.

Syntax

```
switchport private-vlan mapping primary-vlan-id [add | remove]  
secondary-vlan-list
```

```
no switchport private-vlan mapping
```

Parameters

- primary-vlan-id —The VLAN ID of the primary VLAN.
- add secondary-vlan-list—Specifies one or more secondary VLANs to be added to the port.
- remove secondary-vlan-list—Specifies one or more secondary VLANs to be removed from the port.

Default Configuration

No VLAN is configured.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The secondary VLANs should be associated with the primary VLANs, otherwise the configuration is not accepted.

Example

The following example add promiscuous port gi1/0/4 to primary VLAN 10 and to secondary VLAN 20.

```
ZEQU0xxxxDL(config)# interface gi1/0/4  
ZEQU0xxxxDL(config-if)# switchport private-vlan mapping 10 add 20
```

50.31 **switchport private-vlan host-association**

Use the switchport private-vlan host-association Interface Configuration mode command to configure the association of a host port with primary and secondary VLANs of the private VLAN. Use the no form of this command to reset to default.

Syntax

```
switchport private-vlan host-association primary-vlan-id secondary-vlan-id
```

```
no switchport private-vlan host-association
```

Parameters

- primary-vlan-id—The VLAN ID of the primary VLAN.
- secondary-vlan-id—Specifies the secondary VLAN.

Default Configuration

No association.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The secondary VLAN must be associated with the primary VLAN, otherwise the configuration is not accepted. See the private-vlan association command.

The port association configuration depends on the type of the secondary VLAN. The port association configuration for a community secondary VLAN includes:

- The port is added as untagged to the primary VLAN and to the secondary VLAN.
- The PVID is set to the VLAN-ID of the secondary VLAN.
- The port ingress filtering is enabled.

The port association configuration for an isolated secondary VLAN includes:

- The port is added as untagged only to the primary VLAN and is not added to the secondary VLAN.
- The PVID is set to the VLAN-ID of the secondary VLAN.
- The port ingress filtering is disabled.

Example

The following example set port gi1/0/4 to secondary VLAN 20 in primary VLAN 10.

```
ZEQU0xxxxDL(config)# interface gi1/0/4  
ZEQU0xxxxDL(config-if)# switchport private-vlan host-association 10 20
```

50.32 **show vlan private-vlan**

Use the show vlan private-vlan EXEC mode command to display private VLAN information.

Syntax

show vlan private-vlan [tag vlan-id]

Parameters

- tag vlan-id—Primary VLAN that represent the private VLAN to be displayed.

Default Configuration

All private VLANs are displayed.

Command Mode

User EXEC mode

User Guidelines

The show vlan private-vlan command does not include non-private VLAN ports that are members in private VLANs. Tag parameters of non-primary VLAN will result in an empty show output.

Example

ZEQU0xxxxDL# **show vlan private-vlan**

Primary	Secondary	Type	Ports
150		primary	gi1/0/1
150	151	isolated	gi1/0/2
160		primary	gi1/0/3
160	161	community	gi1/0/4

ZEQU0xxxxDL# **show vlan private-vlan 150**

Primary	Secondary	Type	Ports
150		primary	gi1/0/1
150	151	isolated	gi1/0/4

50.33 **vlan prohibit-internal-usage**

Use the `vlan prohibit-internal-usage` command in Global configuration mode to specify VLANs that cannot be used by the switch as internal VLANs.

Syntax

`vlan prohibit-internal-usage none | {add | except | remove} vlan-list`

Parameters

- `none`—The Prohibit Internal Usage VLAN list is empty: any VLAN can be used by the switch as internal.
- `except`—The Prohibit Internal Usage VLAN list includes all VLANs except the VLANs specified by the `vlan-list` argument: only the VLANs specified by the `vlan-list` argument can be used by the switch as internal.
- `add`—Add the given VLANs to the Prohibit Internal Usage VLAN list.
- `remove`—Remove the given VLANs from the Prohibit Internal Usage VLAN list.
- `vlan-list`—List of VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. The VLAN ID that can be used is from 1 through 4094.

Default Configuration

The Prohibit Internal usage VLAN list is empty.

Command Mode

Global Configuration mode

User Guidelines

The switch requires an internal VLAN in the following cases:

- One VLAN for each IP interface is defined directly on an Ethernet port or on a Port channel.
- One VLAN for each IPv6 tunnel.

When a switch needs an internal VLAN it takes a free VLAN with the highest VLAN ID.

Use the `vlan prohibit-internal-usage` command to define a list of VLANs that cannot be used as internal VLANs after reload.

If a VLAN was chosen by the software for internal usage, but you want to use that VLAN for a static or dynamic VLAN, do one of the following

- Add the VLAN to the Prohibited User Reserved VLAN list.
- Copy the Running Configuration file to the Startup Configuration file
- Reload the switch
- Create the VLAN

Examples

Example 1—The following example specifies that VLANs 4010, 4012, and 4090-4094 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage add 4010, 4012, 4090-4094
```

Example 2—The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage all  
vlan prohibit-internal-usage remove 4000-4107
```

Example 3—The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage 4000-4107
```

50.34 **show vlan internal usage**

Use the show vlan internal usage Privileged EXEC mode command to display a list of VLANs used internally by the device (defined by the user).

Syntax

show vlan internal usage

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays VLANs used internally by the switch:

ZEQU0xxxxDL# **show vlan internal usage**

Prohibit Internal Usage VLAN list after reset:

Current Prohibit Internal Usage VLAN list:

VLAN	Usage
-----	-----
4093	gi1/0/1
4094	802.1x

51 VRRP Commands

51.1 clear vrrp counters

To clear the VRRP counters, use the clear vrrp counters command in Privileged EXEC mode.

Syntax

clear vrrp counters [interface-id]

Parameters

- interface-id—(Optional) Interface Identifier.

Default Configuration

No description.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command without the identifier-id argument to clear the VRRP counters of all interfaces where Virtual routers are running.

Use this command with the identifier-id argument to clear the VRRP counters of the specified interface.

Example

The following example shows how to clear the counters of all VRRP virtual routers running on VLAN 10:

```
ZEQU0xxxxDL# clear vrrp counters vlan10
```

51.2 show vrrp

To display a brief or detailed status of one or all configured VRRP virtual routers, use the `show vrrp` command in Privileged EXEC mode.

Syntax

`show vrrp [all | brief | interface interface-id]`

Parameters

- `all`—(Optional) Provides VRRP virtual router information about all VRRP virtual routers, including virtual routers in disable status. If no keyword is configured, the `all` keyword is applied.
- `brief`—(Optional) Provides a summary view of the VRRP virtual router information
- `interface interface-id`—(Optional) Interface identifier

Command Mode

Privileged EXEC mode

User Guidelines

Use this command with the `all` keyword or without keywords to display the VRRP status of all configured VRRP virtual routers.

Use this command with the `interface-id` argument to clear the VRRP counters of the specified interface.

Examples

Example 1. The following example displays a detailed VRRP status of all configured VRRP virtual routers:

```
ZEQU0xxxxDL# show vrrp
```

```
Interface: VLAN 10
```

```
Virtual Router 1
```

```
Virtual Router name CLUSTER1 Supported version is VRRPv3 State is Master
```

```
Virtual IP addresses are 10.2.0.10, 10.3.0.10(down)
```

```
Source IP address is 10.3.0.20 is down: a default Source IP address of  
10.2.0.10 is applied
```

```
Virtual MAC address is 00:00:5e:00:01:01 Advertisement interval is 3.000 sec Preemption enabled  
Priority is 100
```

```
Master Router is 10.3.0.20 (local), priority is 100 Master Advertisement interval is 3.000 sec  
Master Down Interval is 10.828 sec
```

```
Interface: VLAN 10
```

```
Virtual Router 2
```

```
Supported version is VRRPv3 State is Master
```

```
Virtual Router name CLUSTER2
```

```
Virtual IP addresses are 10.4.0.20, 10.5.0.20 Source IP address is 10.4.0.20(default) Virtual MAC  
address is 00:00:5e:00:01:02 Advertisement interval is 1.000 sec Preemption enabled
```

```
Priority is 255
```

```
Master Router is 10.4.0.20 (local), priority is 255 Master Advertisement interval is 1.000 sec  
Master Down Interval is 3.629 sec Skew Time is 1.000 sec
```

```
Interface: VLAN 50
```

```
Virtual Router 1
```

```
Supported version is VRRPv3 State is Backup
```

```
Virtual Router name CLUSTER3 Virtual IP addresses are 10.6.0.10
```

```
Source IP address is 10.6.0.20(default) Virtual MAC address is 00:00:5e:00:01:01 Advertisement  
interval is 1.000 sec Preemption enabled
```

```
Priority is 95
```

```
Master Router is 10.6.0.10, priority is 255 Master Advertisement interval is 1.000 sec Master Down  
Interval is 3.629 sec
```

```
Skew Time is 0.628 sec
```

```
Interface VLAN 400
```

```
Virtual Router 4
```

```
Supported version is VRRPv3 State is Initializing Virtual Router name CLUSTER4
```

```
Virtual IP addresses are 10.7.0.10 Source IP address is 10.7.0.20
```

```
Virtual MAC address is 00:00:5e:00:01:03 Advertisement interval is 1.000 sec Preemption enabled  
Priority is 150
```

Example 2. The following example displays a detailed VRRP status of VRRP virtual routers running on VLAN 10:

```
ZEQU0xxxxDL# show vrrp interface vlan10
Interface: VLAN 10
Virtual Router 1
Virtual Router name CLUSTER1 Supported version is VRRPv3 State is Master
Virtual IP addresses are 10.2.0.10, 10.3.0.10 Source IP address is 10.3.0.20
Virtual MAC address is 00:00:5e:00:01:01 Advertisement interval is 3.000 sec Preemption enabled
Priority is 100
Master Router is 10.3.0.10 (local), priority is 100 Master Advertisement interval is 3.000 sec
Master Down Interval is 10.828 sec Interface: VLAN 10
Virtual Router 2
Supported version is VRRPv3 State is Master
Virtual Router name CLUSTER2
Virtual IP addresses are 10.4.0.10, 10.5.0.10 Source IP address is 10.4.0.10
Virtual MAC address is 00:00:5e:00:01:02 Advertisement interval is 1.000 sec Preemption enabled
Priority is 95
Master Router is 10.4.0.10 (local), priority is 95 Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
```

Example 3. The following example displays a brief VRRP status of all configured VRRP virtual routers:

```
ZEQU0xxxxDL# show vrrp brief
```

Priority: Current/Configured

State (St): I - Initialize; M - Master; B - Backup

Preempt (P) : Y - Yes; N - No

Interface	VR	Virtual Address	Pri	Timer	P	St	Ver	Source Address	Master Address
VLAN 10	1	10.2.0.10	100	3000	Y	M	3	10.3.0.10	10.3.0.10
VLAN 10	2	10.4.0.10	255	1000	Y	M	3	10.4.0.10	10.4.0.10
VLAN 50	1	10.6.0.10	95	1000	Y	B	3	10.6.0.10	10.6.0.60

51.3 show vrrp counters

To display the VRRP counters, use the `show vrrp counters` command in Privileged EXEC mode.

Syntax

`show vrrp counters [interface-id]`

Parameters

- `interface-id`—(Optional) Interface Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

Use the `show vrrp counters` command without the `identifier-id` argument to display the VRRP counters of all interfaces where Virtual routers are running.

Use the `show vrrp counters` command with the `identifier-id` argument to display the VRRP counters of the specified interface.

Example

The following example display the counters of all virtual routers defined on VLAN 100:

```
ZEQU0xxxxDL# show vrrp counters vlan 100
vlan 100
Invalid checksum: 0 Invalid Packet Length: 0 Invalid TTL: 0
Invalid VRRP Packet Type: 0 Invalid VRRP ID: 0
Invalid Protocol Number: 0 Invalid IP List: 0
Invalid Interval: 0
Invalid Authentication: 0
```

51.4 vrrp description

To assign a description to the VRRP virtual router, use the `vrrp description` command in Interface Configuration mode. To return to the default, use the `no` format of the command.

Syntax

`vrrp vrid description text`

`no vrrp vrid description`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- `text`—Text that describes the purpose or use of the virtual router. The parameter may contain 0-160 characters.

Default Configuration

No description.

Command Mode

Interface Configuration mode

Example

The following example shows how to assign a VRRP description to the specified VRRP virtual router:

```
ZEQU0xxxxDL(config)# interface vlan 10
ZEQU0xxxxDL(config-if)# vrrp 1 description router1
ZEQU0xxxxDL(config-if)# exit
```

51.5 vrrp ip

To define an IP address of a virtual router, use the `vrrp ip` command in Interface Configuration mode. To remove the IP address, use the `no` format of the command.

Syntax

`vrrp vrid ip ip-address`

`no vrrp vrid ip [ip-address]`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- `ip-address`—Virtual router's IP address.

Command Mode

Interface Configuration mode

User Guidelines

A virtual router comes into existence when it has one or more participating VRRP routers. To participate in a specific virtual router as a VRRP router, use `vrrp ip` to configure an existing IP interface with the identifier and the IP address(es) of the virtual router. The IP interface of the VRRP router and the virtual router must be in the same IP subnet.

A VRRP router that is the owner of the virtual router's IP address(es) is also the VRRP router real IP address at the IP interface. There is only one owner for all virtual router's IP address(es). A VRRP router participates in a virtual router when it is configured with the first virtual router's IP address and does not participate when the virtual router IP address is removed.

A virtual router entity in a VRRP router is created in the shutdown state. Use the `no vrrp shutdown` command to enable it.

To defined more than one virtual router's IP address, the command should be applied for each configured IP address.

Each VRRP router in the virtual router should be configured with the same set of IP addresses.

If the `ip-address` parameter is omitted in the `no` format of the CLI command, all the IP addresses of the virtual router are removed, leading to the virtual router entity in the VRRP router being removed too.

The switch supports up to 255 VRRP routers.

Example

The following example shows how to define a VRRP virtual router:

```
ZEQU0xxxxDL(config)# interface vlan 10  
ZEQU0xxxxDL(config-if)# vrrp 1 ip 192.168.2.1  
ZEQU0xxxxDL(config-if)# exit
```

51.6 vrrp preempt

To enable Virtual Router Redundancy Protocol (VRRP) preemption, use the `vrrp preempt` command in Interface Configuration mode. To return to the default, use the `no` format of the command.

Syntax

`vrrp vrid preempt`

`no vrrp vrid preempt`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.

Command Mode

Interface Configuration mode

Default Configuration

Preemption is enabled by default.

User Guidelines

By default, the VRRP router being configured with this command will take over as Master virtual router for the group if it has a higher priority than the current master virtual router.

Note: The router that is the IP address owner will preempt, regardless of the setting of this command.

Example

The following example shows how to disable VRRP preemption to the specified VRRP virtual router:

```
ZEQU0xxxxDL(config)# interface vlan 10
ZEQU0xxxxDL(config-if)# no vrrp 1 preempt
ZEQU0xxxxDL(config-if)# exit
```

51.7 vrrp priority

To define Virtual Router Redundancy Protocol (VRRP) priority, use the `vrrp priority` command in Interface Configuration mode. To return to the default, use the `no` format of the command.

Syntax

`vrrp vrid priority priority`

`no vrrp vrid priority`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- `priority`—Virtual router priority. The range is 1-254.

Command Mode

Interface Configuration mode

Default Configuration

The default for owner is 255 and for non-owner it is 100.

User Guidelines

The priority of the owner cannot be changed. It is always 255.

Example

The following example shows how to set VRRP priority:

```
ZEQU0xxxxDL (config) # interface vlan 10
ZEQU0xxxxDL (config-if) # vrrp 1 priority 110
ZEQU0xxxxDL (config-if) # exit
```

51.8 vrrp shutdown

To disable the VRRP virtual router on the interface (meaning that it changes its status to Initialize), use the `vrrp shutdown` command in Interface Configuration mode. To return to the default, use the `no` format of the command.

Syntax

`vrrp vrid shutdown`

`no vrrp vrid shutdown`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.

Default Configuration

Disabled.

Command Mode

Interface Configuration mode

User Guidelines

When a VRRP virtual router is disabled on an interface, its configuration is not removed.

Example

The following example shows how to enable a specified virtual router:

```
ZEQU0xxxxDL(config)# interface vlan 10
ZEQU0xxxxDL(config-if)# no vrrp 1 shutdown
ZEQU0xxxxDL(config-if)# exit
```

51.9 vrrp source-ip

To define a real VRRP address that will be used as the source IP address of VRRP messages, use the `vrrp source-ip` command in Interface Configuration mode. To return to the default, use the `no` format of the command.

Syntax

`vrrp vrid source-ip ip-address`

`no vrrp vrid source-ip`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- `ip-address`—VRRP router's IP address: one of IP addresses of VRRP router defined on the same interface.

Default Configuration

Lowest VRRP router's IP address defined on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Example

The following example shows how to define a source ip address to the specified VRRP virtual router:

```
ZEQU0xxxxDL(config)# interface vlan 10
ZEQU0xxxxDL(config-if)# vrrp 1 source-ip 192.168.2.1
ZEQU0xxxxDL(config-if)# exit
```

51.10 vrrp timers advertise

To define the interval between successive advertisements by the Master VRRP virtual router, use the `vrrp timers advertise` command in Interface Configuration mode. To return to the default, use the `no` format of the command.

Syntax

`vrrp vrid timers advertise [msec] interval`

`no vrrp vrid timers advertise`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- `msec`—(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without the keyword, the advertisement interval is in seconds.
- `interval`—Time interval between successive advertisements. If keyword `msec` is present then the valid range is 50 to 40950 milliseconds. If keyword `msec` is omitted then the valid range is 1 to 40 seconds.

Command Mode

Interface Configuration mode

Default Configuration

1 second

User Guidelines

If the advertisement interval is configured in msec, the operation advertisement interval will be the configured advertisement interval round down to the nearest seconds for VRRP v2 and to the nearest centiseconds (10ms) for VRRP v3.

Example

The following example shows how to set VRRP timer advertise of 500 msec to specified VRRP virtual router:

```
ZEQU0xxxxDL (config)# interface vlan 10
ZEQU0xxxxDL (config-if)# vrrp 1 timers advertise msec 500
ZEQU0xxxxDL (config-if)# exit
```

51.11 vrrp version

To define the supported VRRP version, use the `vrrp version` command in Interface Configuration mode. To return to the default, use the `no` format of the command.

Syntax

`vrrp vrid version 2 | 3 | 2&3`

`no vrrp vrid version`

Parameters

- `vrid`—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- `2`—VRRPv2 specified by RFC3768 is supported. Received VRRPv3 messages are dropped by the VRRP virtual router. Only VRRPv2 advertisements are sent.
- `3`—VRRPv3 specified by RFC5798 is supported without VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are dropped by the VRRP virtual router. Only VRRPv3 advertisements are sent.
- `2&3`—VRRPv3 specified by RFC5798 is supported with VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are treated by the VRRP virtual router. VRRPv3 and VRRPv2 advertisements are sent.

Default Configuration

Version 2.

Command Mode

Interface Configuration mode

User Guidelines

Version 2&3 is intended for upgrade scenarios and is not for permanent deployment. Please refer to VRRP 3 standard for version 2 and version 3 interoperability.

Example

The following example shows how to define VRRP version to specified VRRP virtual router:

```
ZEQU0xxxxDL(config)# interface vlan 10
ZEQU0xxxxDL(config-if)# vrrp 1 version 2
ZEQU0xxxxDL(config-if)# exit
```

51.12 vrrp non-owner-ping response

This command is used to enable the virtual router in the master state to respond to ICMP echo requests for an IP address not owned but associated with this virtual router. Use the no form of this command to disable the response.

Syntax

vrrp non-owner-ping response

no vrrp non-owner-ping response

Parameters

N/A

Default Configuration

Version 2.

Command Mode

Global Configuration mode

User Guidelines

The virtual router in Master state will accept packets addressed to the address owner's address as its own if it is not the address owner.

Example

The following example shows how to define vrrp non-owner-ping response:

```
ZEQU0xxxxDL (config)# vrrp non-owner-ping response
```

This image shows a full page of blank, lined paper. It features approximately 28 evenly spaced horizontal black lines across its entire width, typical of notebook or legal stationery. The background is a uniform off-white color, and there are no margins, text, or other markings present.

[illegible]

© Panasonic Electric Works Networks Co., Ltd. 2019-2022

Panasonic Electric Works Networks Co., Ltd.

2-12-7, Higashi-Shimbashi, Minato-ku, Tokyo Japan, 105-0021
URL: <https://panasonic.co.jp/ew/pewnw/english/index.html>

P0919-1042